

DrayTek

Vigor2830n v2

ADSL2+ Security Firewall

DrayTek



Your reliable networking solutions partner

User's Guide

V1.1

Vigor2830n V2 ADSL2+ Security Firewall User's Guide

Version: 1.2

Firmware Version: V3.8.1

(For future update, please visit DrayTek web site)

Date: July 20, 2016

Intellectual Property Rights (IPR) Information

Copyrights

© 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, 7 and Explorer are trademarks of Microsoft Corp.
- Apple and Mac OS are registered trademarks of Apple Inc.
- Other products may be trademarks or registered trademarks of their respective manufacturers.

Safety Instructions and Approval

Safety Instructions

- Read the installation guide thoroughly before you set up the router.
- The router is a complicated electronic unit that may be repaired only 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: Vigor2830 Series Router

DrayTek Corp. declares that Vigor2830n Series of routers are in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EC.

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.

This product is designed for the DSL, 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.

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.

The antenna/transmitter should be kept at least 20 cm away from human body.



Please visit <http://www.draytek.com> for more detailed information.

Table of Contents

1

Introduction	1
1.1 LED Indicators and Connectors	2
1.2 Hardware Installation	4
1.3 Printer Installation	5
1.4 Accessing Web Page	12
1.5 Changing Password	13
1.6 Online Status	14
1.6.1 Physical Connection	14
1.6.2 Virtual WAN	16
1.7 Saving Configuration.....	16

2

Quick Setup	17
2.1 Quick Start Wizard	17
2.1.1 For WAN1 (ADSL)	18
2.1.2 For WAN2 (Ethernet)	24
2.1.3 For WAN3 (USB)	34
2.2 Service Activation Wizard.....	36
2.3 VPN Client Wizard	40
2.4 VPN Server Wizard	46
2.5 Wireless Wizard	51
2.6 Registering Vigor Router.....	54

3

Advanced Configuration.....	57
3.1 WAN	57
3.1.1 Basics of Internet Protocol (IP) Network.....	57
3.1.2 General Setup.....	59
3.1.3 Internet Access	65
3.1.4 Multi-PVC/VLAN	95
3.2 LAN	100
3.2.1 Basics of LAN	100
3.2.2 General Setup.....	102
3.2.3 Static Route	114
3.2.4 VLAN (Multi-Subnet).....	119
3.2.5 Bind IP to MAC	122
3.2.6 LAN Port Mirror	123
3.2.7 Wired 802.1x.....	124
3.2.8 Web Portal Setup.....	125

3.3 Load-Balance /Route Policy.....	128
3.3.1 General Setup.....	129
3.3.2 Diagnose.....	134
3.4 NAT	136
3.4.1 Port Redirection	136
3.4.2 DMZ Host.....	140
3.4.3 Open Ports.....	144
3.4.4 Port Triggering	146
3.5 Firewall.....	149
3.5.1 Basics for Firewall.....	149
3.5.2 General Setup.....	151
3.5.3 Filter Setup.....	155
3.5.4 DoS Defense.....	163
3.6 User Management.....	166
3.6.1 General Setup.....	167
3.6.2 User Profile	168
3.6.3 User Group	172
3.6.4 User Online Status.....	174
3.7 Objects Setting.....	175
3.7.1 IP Object	175
3.7.2 IP Group.....	178
3.7.3 IPv6 Object	180
3.7.4 IPv6 Group.....	182
3.7.5 Service Type Object	184
3.7.6 Service Type Group.....	186
3.7.7 Keyword Object	188
3.7.8 Keyword Group.....	190
3.7.9 File Extension Object.....	192
3.7.10 SMS/Mail Service Object.....	194
3.7.11 Notification Object.....	199
3.8 CSM Profile	201
3.8.1 APP Enforcement Profile	202
3.8.2 URL Content Filter Profile.....	206
3.8.3 Web Content Filter Profile.....	210
3.8.4 DNS Filter Profile	214
3.8.5 APPE Support List	216
3.9 Bandwidth Management	217
3.9.1 Sessions Limit.....	217
3.9.2 Bandwidth Limit	219
3.9.3 Quality of Service.....	221
3.10 Applications	230
3.10.1 Dynamic DNS	230
3.10.2 LAN DNS / DNS Forwarding.....	233
3.10.3 Schedule	236
3.10.4 RADIUS	239
3.10.5 Active Directory/LDAP	240
3.10.6 UPnP.....	243
3.10.7 IGMP	244
3.10.8 Wake on LAN.....	245
3.10.9 SMS/Mail Alert Service	246
3.11 VPN and Remote Access.....	248

3.11.1 Remote Access Control	249
3.11.2 PPP General Setup	249
3.11.3 IPSec General Setup	252
3.11.4 IPSec Peer Identity	254
3.11.5 Remote Dial-in User	256
3.11.6 LAN to LAN	260
3.11.7 VPN TRUNK Management	271
3.11.8 Connection Management	276
3.12 Certificate Management	277
3.12.1 Local Certificate	277
3.12.2 Trusted CA Certificate	281
3.12.3 Certificate Backup	283
3.13 Wireless LAN	283
3.13.1 Basic Concepts	283
3.13.2 General Setup	286
3.13.3 Security	288
3.13.4 Access Control	291
3.13.5 WPS	292
3.13.6 WDS	295
3.13.7 Advanced Setting	299
3.13.8 AP Discovery	302
3.13.9 Station List	303
3.14 SSL VPN	304
3.14.1 General Setup	304
3.14.2 SSL Web Proxy	305
3.14.3 SSL Application	306
3.14.4 User Account	309
3.14.5 User Group	313
3.14.6 Online User Status	315
3.15 USB Application	316
3.15.1 USB General Settings	316
3.15.2 USB User Management	317
3.15.3 File Explorer	320
3.15.4 USB Device Status	321
3.15.5 Modem Support List	322
3.15.6 SMB Client Support List	323
3.16 System Maintenance	323
3.16.1 System Status	324
3.16.2 TR-069	326
3.16.3 Admin Setting	328
3.16.4 User Password	330
3.16.5 Login Page Greeting	333
3.16.6 Configuration Backup	334
3.16.7 Syslog/Mail Alert	337
3.16.8 Time and Date	339
3.16.9 SNMP	341
3.16.10 Management	343
3.16.11 Reboot System	346
3.16.12 Firmware Upgrade	347
3.16.13 Modem Code Upgrade	347
3.16.14 Activation	348
3.17 Diagnostics	350
3.17.1 Dial-out Triggering	350
3.17.2 Routing Table	351

3.17.3 ARP Cache Table	352
3.17.4 IPv6 Neighbour Table	353
3.17.5 DHCP Table	353
3.17.6 NAT Sessions Table	354
3.17.7 DNS Cache Table	356
3.17.8 Ping Diagnosis	357
3.17.9 Data Flow Monitor	358
3.17.10 Traffic Graph	360
3.17.11 Trace Route	361
3.17.12 Syslog Explorer	362
3.17.13 IPv6 TSPC Status	364
3.17.14 DoS Flood Table	364
3.18 External Devices	365

4

Application and Examples.....367

4.1 How to Configure Multi-Subnet in Vigor2830.....	367
4.2 How Can I Use FTP to Get the Files from USB Storage Device Connecting to Vigor Router?	374
4.3 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection.....	376
4.4 Web Portal Log-In Application for Wireless Client	380
4.5 How to Customize Your Login Page	384
4.6 Create a LAN-to-LAN Connection Between Remote Office and Headquarter	387
4.7 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter.....	395
4.8 QoS Setting Example.....	399
4.9 Upgrade Firmware for Your Router	404
4.10 Request a certificate from a CA server on Windows CA Server	407
4.11 Request a CA Certificate and Set as Trusted on Windows CA Server	411
4.12 Creating an Account for MyVigor	413
4.12.1 Creating an Account via Vigor Router	413
4.12.2 Creating an Account via MyVigor Web Site.....	417
4.13 How to Implement the LDAP/AD Authentication for User Management?.....	421
4.14 How to Implement the LDAP/AD Authentication for VPN?	425
4.15 How to Setup Address Mapping.....	428
4.16 How to setup Load Balance for Packets?	432

5

Trouble Shooting.....435

5.1 Checking If the Hardware Status Is OK or Not.....	435
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	436
5.3 Pinging the Router from Your Computer	439
5.4 Checking If the ISP Settings are OK or Not	440

5.5 Problems for 3G/4G Network Connection.....	440
5.6 Backing to Factory Default Setting If Necessary	441
5.7 Contacting DrayTek.....	442
Appendix I: VLAN Applications on Vigor Router	443

1

Introduction

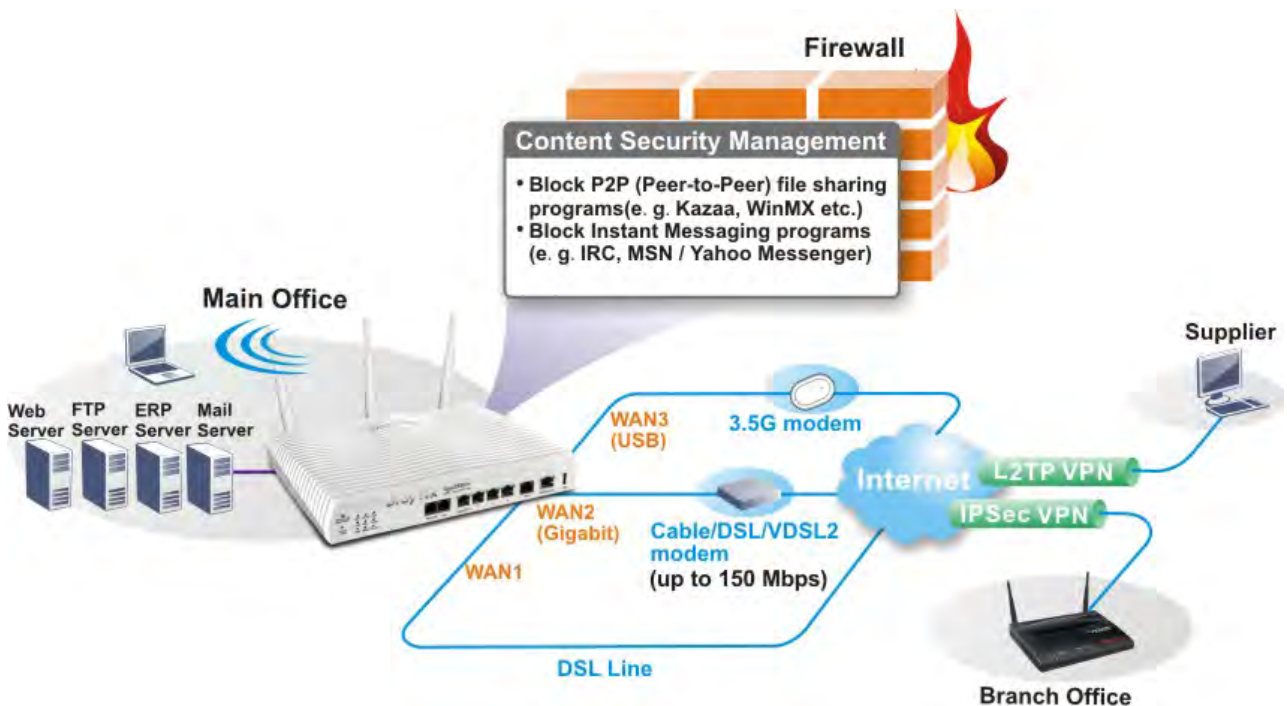
Vigor2830 series is an ADSL2+ router. It integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

By adopting hardware-based VPN platform and hardware encryption of AES/DES/3DES, the router increases the performance of VPN greatly, and offers several protocols (such as IPSec/PPTP/L2TP) with up to 32 VPN tunnels.

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

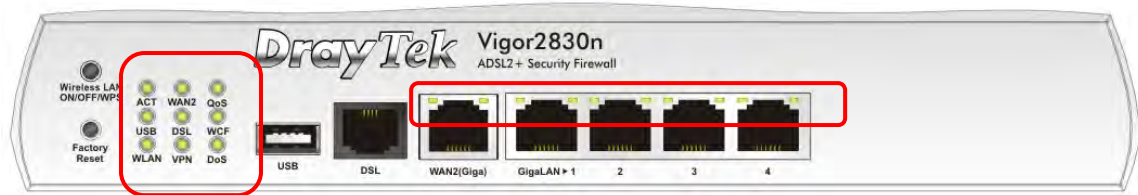
Object-based firewall is flexible and allows your network be safe. In addition, Vigor2830 series supports USB interface for connecting USB printer to share printer or USB storage device for sharing files.

Vigor2830 series provides two-level management to simplify the configuration of network connection. The user mode allows user accessing into WEB interface via simple configuration. However, if users want to have advanced configurations, they can access into WEB interface through admin mode.



1.1 LED Indicators and Connectors

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



LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
USB	On	USB device is connected and ready for use.
	Blinking	The data is transmitting.
CSM	On	The profile(s) of CSM (Content Security Management) for IM/P2P, URL/Web Content Filter application is enabled from Firewall >>General Setup . (Such profile must be established under CSM menu).
WLAN	On	Wireless access point is ready.
	Blinking	It will blink slowly while wireless traffic goes through. If ACT and WLAN LEDs blink quickly and simultaneously when WPS is working, and it will return to normal condition after two minutes. (You need to setup WPS within 2 minutes.)
DSL	On	The router is ready to access Internet through DSL link.
	Blinking	Slowly: The DSL connection is ready. Quickly: The data is transmitting.
WAN2	On	The WAN2 connection is ready.
	Blinking	It will blink while transmitting data.
DoS	On	The DoS/DDoS function is active.
	Blinking	It will blink while an attack is detected.
VPN	On	The VPN tunnel is active.
QoS	On	The QoS function is active.

LED on Connector

GigaLAN 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.
WAN 2 (Giga)	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.

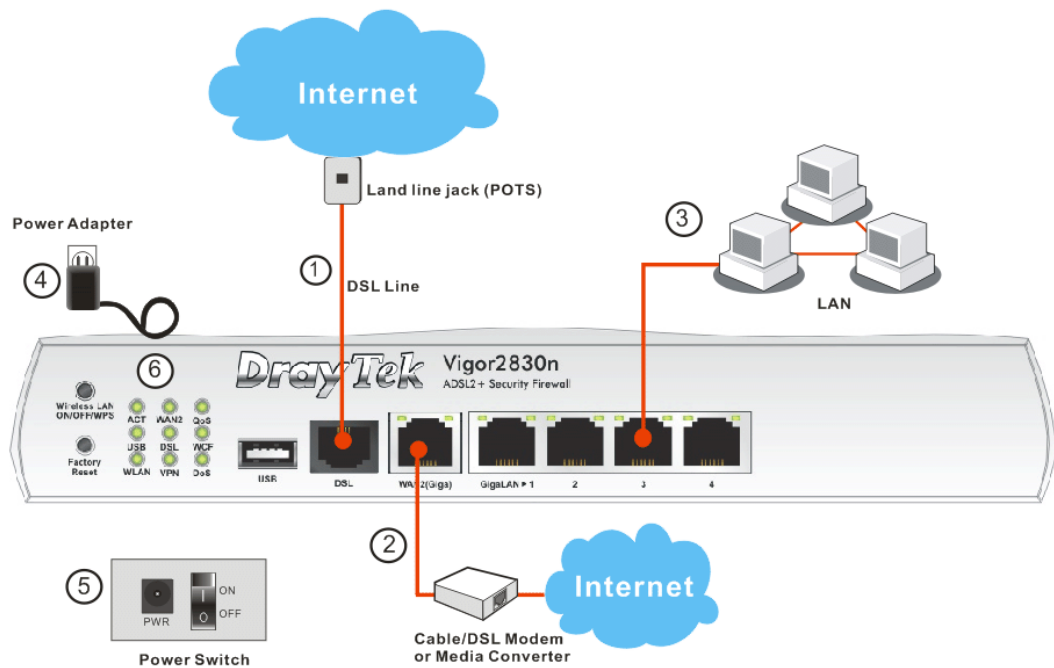


Interface	Description
Wireless LAN ON/OFF/WPS	Press "Wireless LAN ON/OFF/WPS" button once to wait for client device making network connection through WPS. Press "Wireless LAN ON/OFF/WPS" button twice to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
Factory Reset	Restore the default 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.
USB	Connector for a USB device (for 3G USB Modem or printer).
DSL	Connector for accessing the Internet through ADSL2/2+.
WAN2(Giga)	Connectors for remote networked devices.
GigaLAN (1-4)	Connectors for local network devices.
PWR	Connector for a power adapter.
ON/OFF	Power Switch.

1.2 Hardware Installation

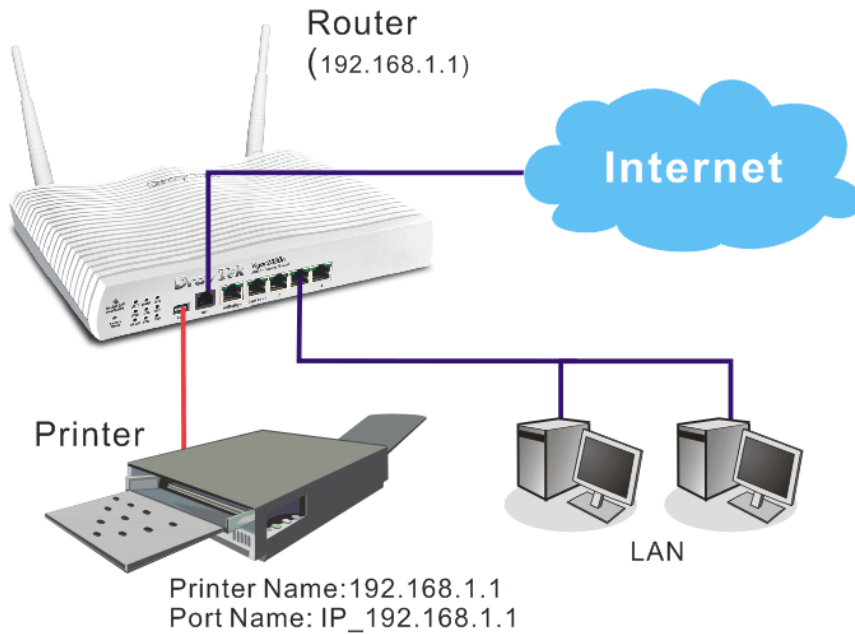
Before starting to configure the router, you have to connect your devices correctly.

1. Use one end of the DSL line cable to DSL port on the router to the land line jack on the wall for accessing Internet.
2. Or, you can connect the WAN1 interface to the Cable/DSL Modem or media converter for accessing Internet.
3. Connect one end of an Ethernet cable (RJ-45) to one of the **LAN** ports of the router and the other end of the cable (RJ-45) into the Ethernet port on your computer.
4. 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.
5. Power on the device by pressing down the power switch on the rear panel.
6. The system starts to initiate. After completing the system test, the **ACT** LED will light up and start blinking.



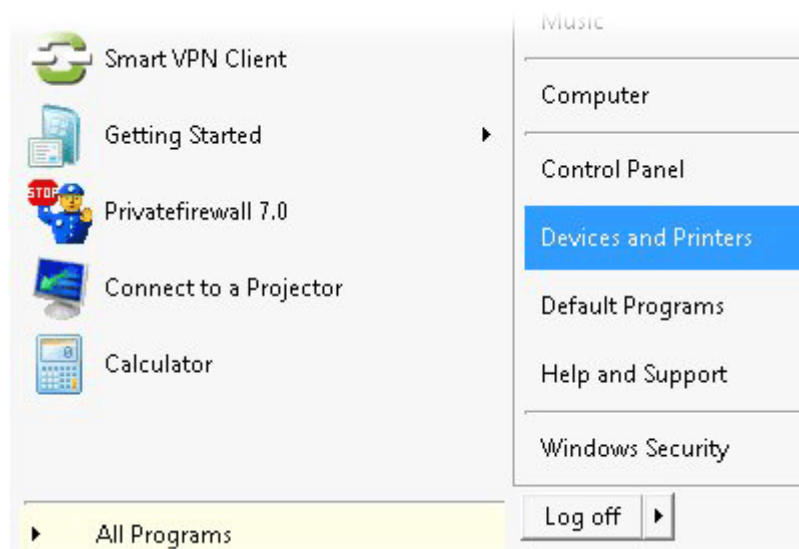
1.3 Printer Installation

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 installation on other Windows systems, please visit www.DrayTek.com.

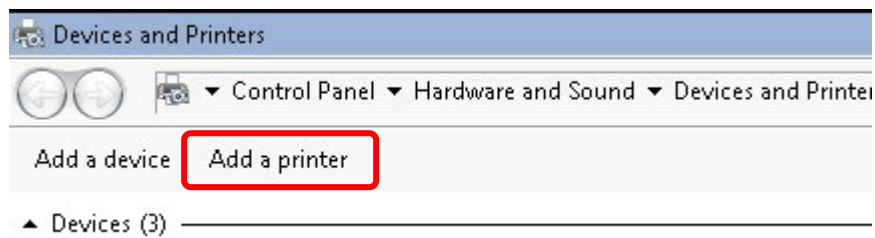


Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

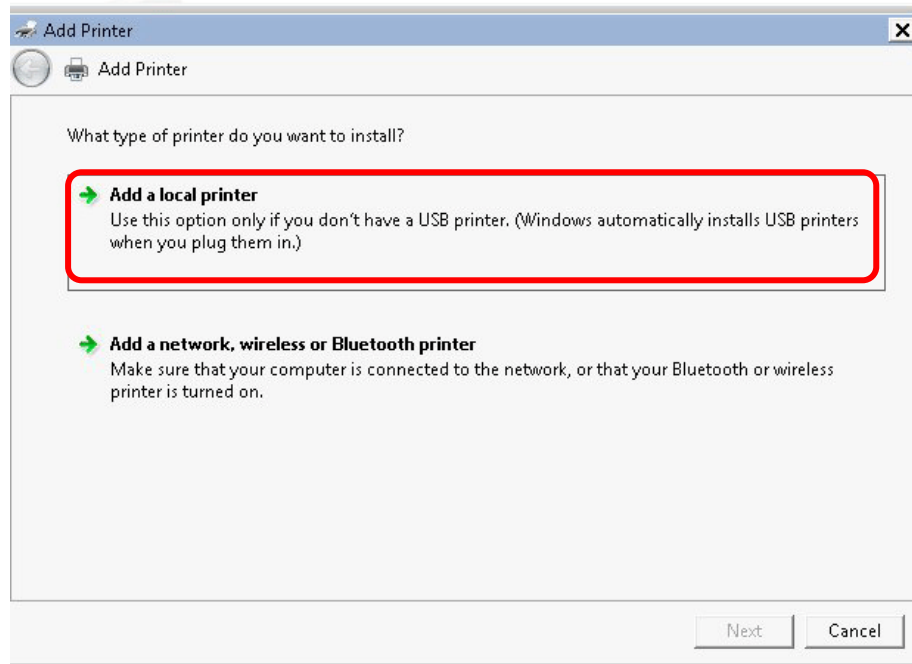
1. Connect the printer with the router through USB/parallel port.
2. Open **All Programs>>Getting Started>>Devices and Printers**.



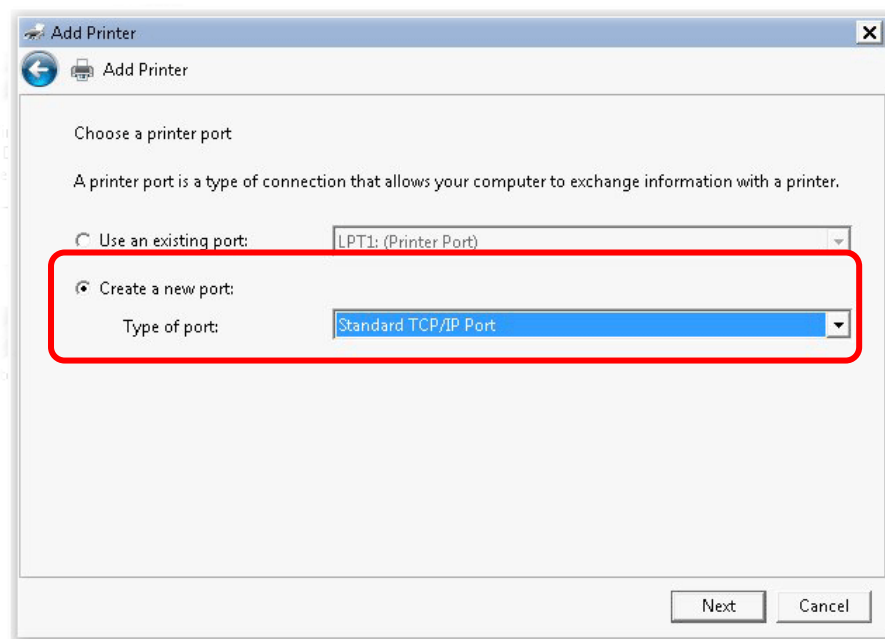
3. Click **Add a printer**.



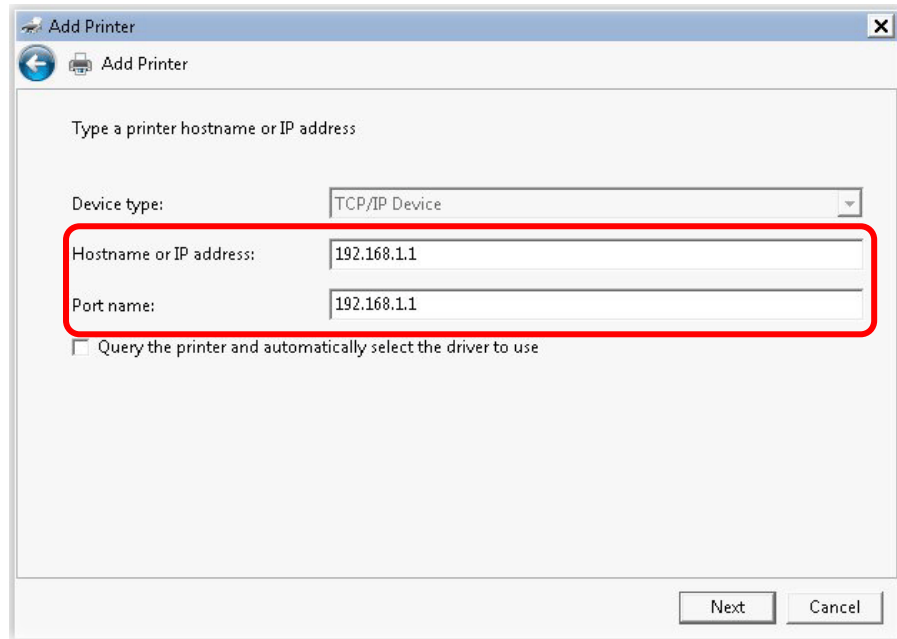
4. A dialog will appear. Click **Add a local printer** and click **Next**.



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**.

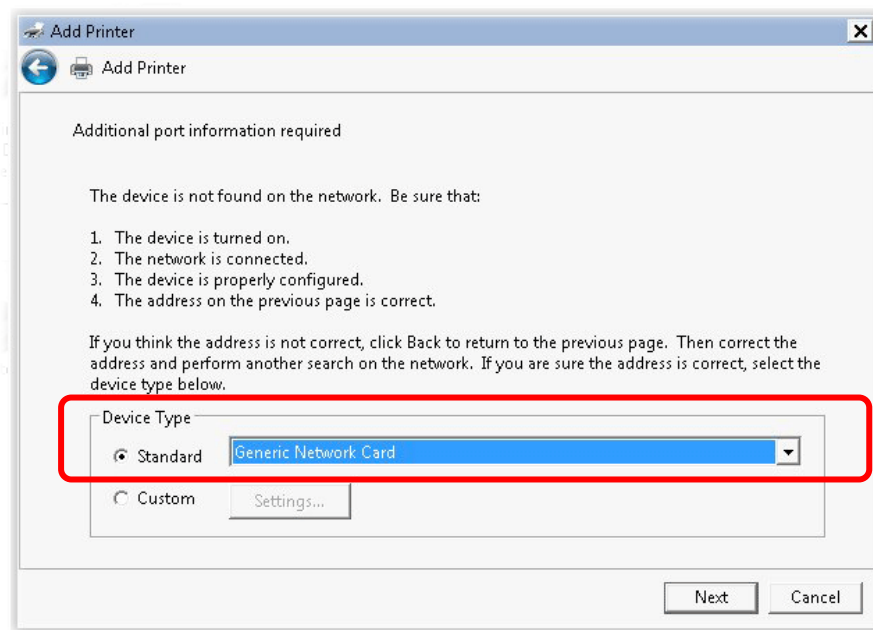


6. In the following dialog, type **192.168.1.1** (router's LAN IP) in the field of **Hostname or IP Address** and type **192.168.1.1** as the **Port name**. Then, click **Next**.



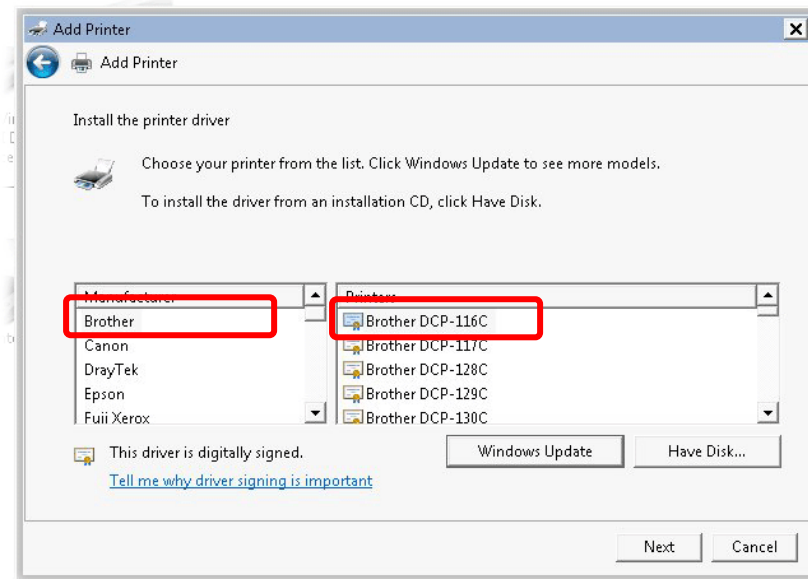
The screenshot shows the 'Add Printer' dialog box with the title bar 'Add Printer'. Below the title bar is a navigation bar with a back arrow and a printer icon. The main area is titled 'Type a printer hostname or IP address'. It contains a 'Device type:' dropdown menu set to 'TCP/IP Device'. Below this are two text input fields: 'Hostname or IP address:' and 'Port name:', both containing the text '192.168.1.1'. These two fields are highlighted with a red rectangular box. Below the input fields is a checkbox labeled 'Query the printer and automatically select the driver to use'. At the bottom right are 'Next' and 'Cancel' buttons.

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

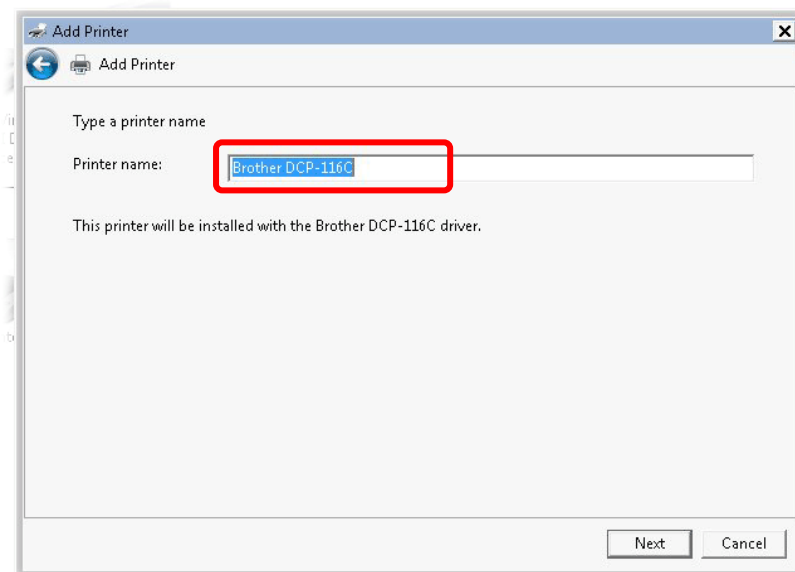


The screenshot shows the 'Add Printer' dialog box with the title bar 'Add Printer'. Below the title bar is a navigation bar with a back arrow and a printer icon. The main area is titled 'Additional port information required'. It contains a message: 'The device is not found on the network. Be sure that:' followed by a list of four items: 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. Below this is a paragraph: '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.' Below this text is a 'Device Type' section with a radio button labeled 'Standard' selected, and a dropdown menu showing 'Generic Network Card'. This section is highlighted with a red rectangular box. Below the 'Standard' radio button is a 'Custom' radio button and a 'Settings...' button. At the bottom right are 'Next' and 'Cancel' buttons.

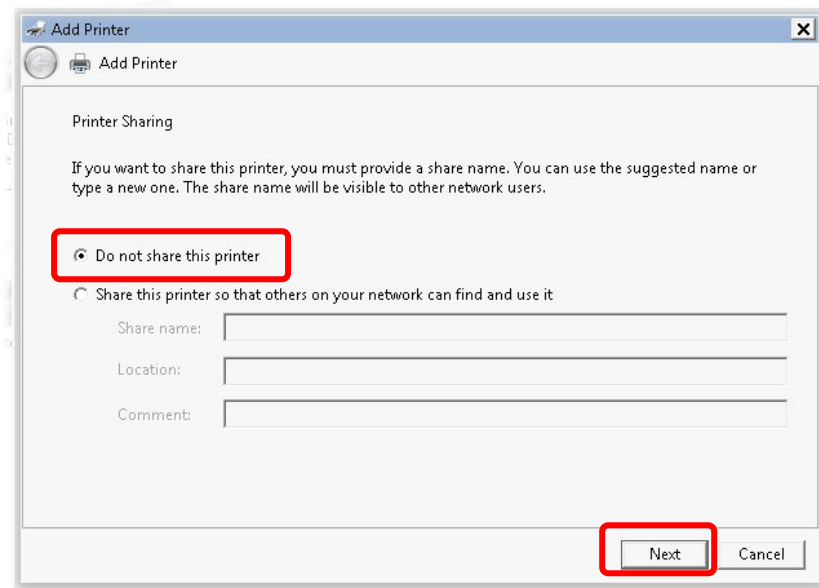
8. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.



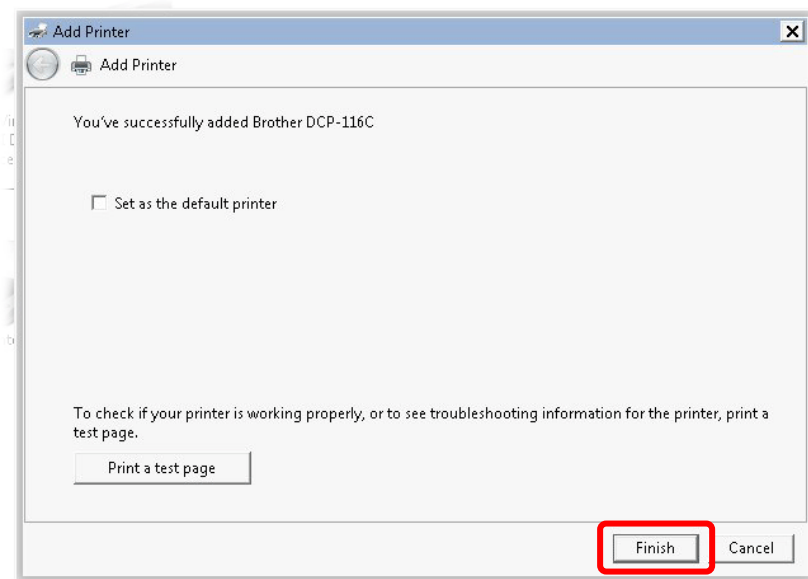
9. Type a name for the chosen printer. Click **Next**.



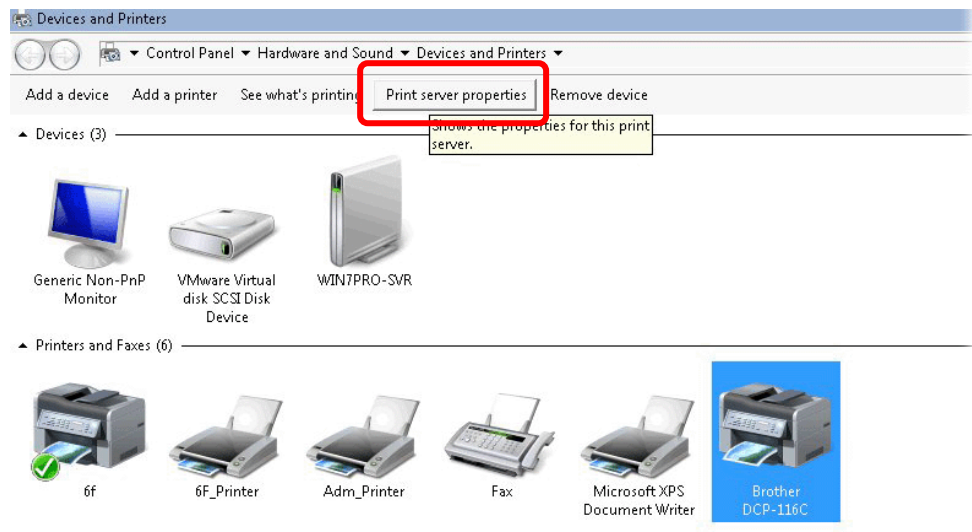
10. Choose **Do not share this printer** and click **Next**.



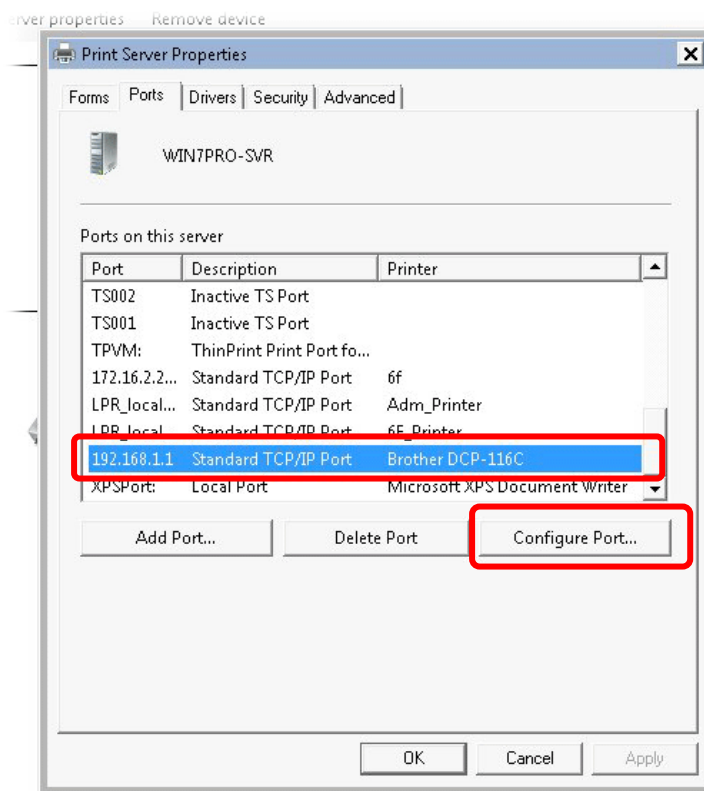
11. Then, in the following dialog, click **Finish**.



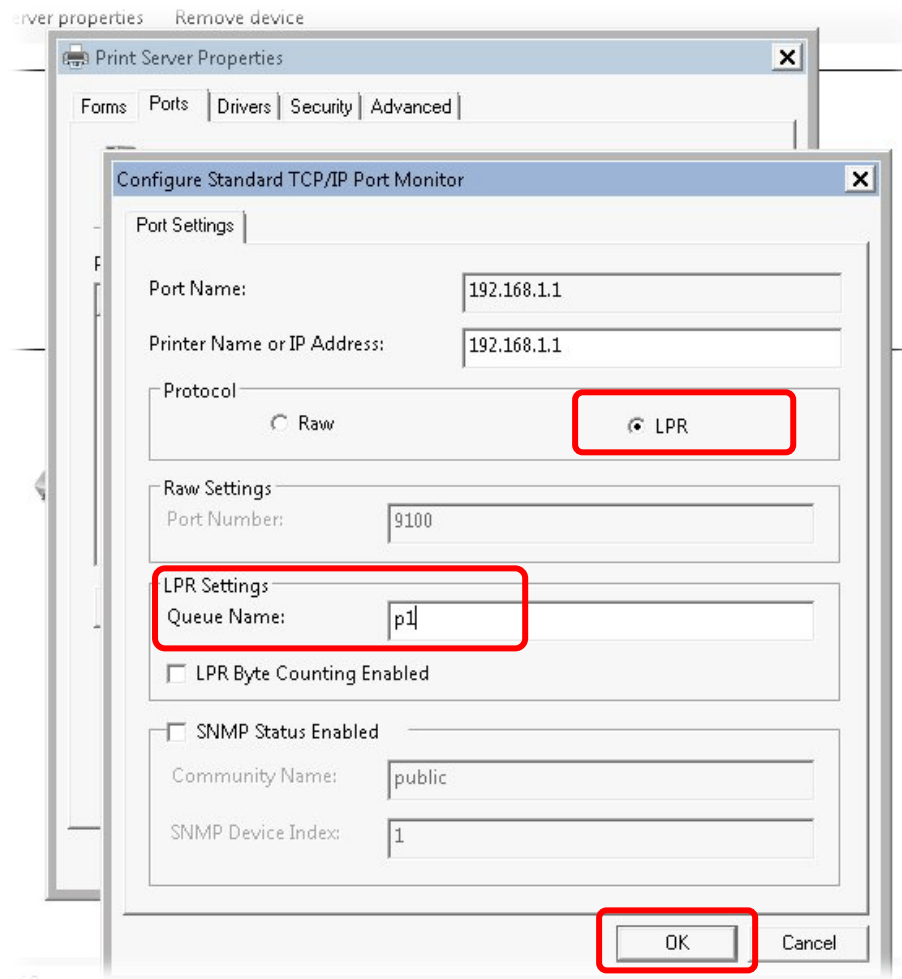
12. The new printer has been added and displayed under **Printers and Faxes**. Click the new printer icon and click **Printer server properties**.



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.

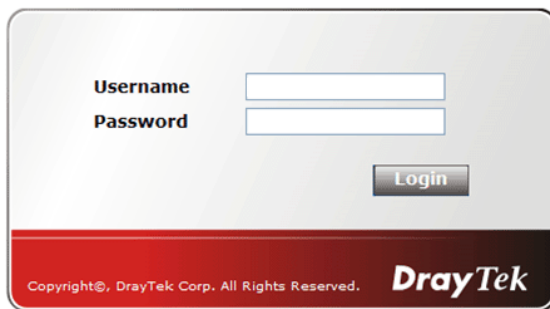
Note 2: Vigor router supports printing request from computers via LAN ports but not WAN port.

1.4 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.



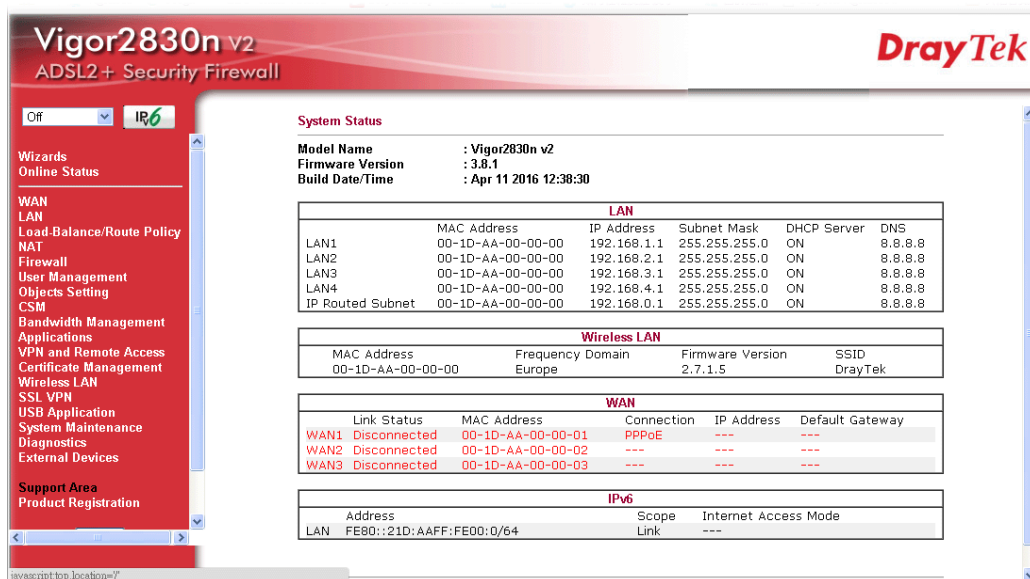
A login window for the Vigor router. It has a light gray background with a red footer. The footer contains the text "Copyright©, DrayTek Corp. All Rights Reserved." and the "DrayTek" logo. The main area has two input fields: "Username" and "Password". Below these fields is a "Login" button.

3. Please type "admin/admin" as the Username/Password and click **Login**.



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

4. Now, the **Main Screen** will appear.



The main configuration screen for the Vigor2830n v2 router. The title bar says "Vigor2830n v2 ADSL2+ Security Firewall" and "DrayTek". On the left is a red sidebar with a menu. The main area shows system status and configuration tables.

System Status

Model Name : Vigor2830n v2
Firmware Version : 3.8.1
Build Date/Time : Apr 11 2016 12:38:30

LAN						
	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS	
LAN1	00-1D-AA-00-00-00	192.168.1.1	255.255.255.0	ON	8.8.8.8	
LAN2	00-1D-AA-00-00-00	192.168.2.1	255.255.255.0	ON	8.8.8.8	
LAN3	00-1D-AA-00-00-00	192.168.3.1	255.255.255.0	ON	8.8.8.8	
LAN4	00-1D-AA-00-00-00	192.168.4.1	255.255.255.0	ON	8.8.8.8	
IP Routed Subnet	00-1D-AA-00-00-00	192.168.0.1	255.255.255.0	ON	8.8.8.8	

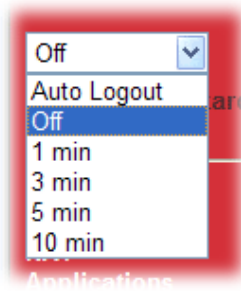
Wireless LAN			
MAC Address	Frequency Domain	Firmware Version	SSID
00-1D-AA-00-00-00	Europe	2.7.1.5	DrayTek

WAN					
	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Disconnected	00-1D-AA-00-00-01	PPPoE	---	---
WAN2	Disconnected	00-1D-AA-00-00-02	---	---	---
WAN3	Disconnected	00-1D-AA-00-00-03	---	---	---

IPv6		
Address	Scope	Internet Access Mode
LAN FE80::21D:AAFF:FE00:0/64	Link	---

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

- 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.



1.5 Changing Password

Please change the password for the original security of the router.

- 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.
- Please type “admin/admin” as the Username/Password and click **Login**.
- Go to **System Maintenance** page and choose **Admin Setting**.

System Maintenance >> Admin Setting

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 ; : . " < > * + = \ | ? @ # ^ ! ()

Administrator Local User

<input type="checkbox"/> Local User				
Local User List				
<table border="1"> <thead> <tr> <th>Index</th> <th>User Name</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody> </table>	Index	User Name		
Index	User Name			

- Enter the login password (the default is blank) on the field of **Old Password**. Type **New 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.

 A screenshot of the DrayTek login page. It features a light gray background with a white rounded rectangle containing the login fields. There are two input fields labeled 'Username' and 'Password'. Below them is a 'Login' button. At the bottom, there is a red banner with the text 'Copyright©, DrayTek Corp. All Rights Reserved.' and the 'DrayTek' logo.

1.6 Online Status

Online Status
▶ Physical Connection
▶ Virtual WAN

1.6.1 Physical Connection

Such page displays the physical connection status such as LAN connection status, WAN connection status, ADSL information, and so on.

Physical Connection for IPv4 Protocol

Online Status

Physical Connection

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

53964

729498

WAN 1 Status

>> [Dial PPPoE](#)

Enable

Line

Name

Mode

Up Time

Yes

VDSL

PPPoE

00:00:00

IP

GW IP

TX Packets

TX Rate(Bps)

RX Packets

RX Rate(Bps)

0

0

0

0

Message [PPP Shutdown]

WAN 2 Status

Enable

Line

Name

Mode

Up Time

Yes

Ethernet

Static IP

4:07:44

IP

GW IP

TX Packets

TX Rate(Bps)

RX Packets

RX Rate(Bps)

172.16.3.103

172.16.1.1

29011

351

125630

1230

WAN 3 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

Physical Connection for IPv6 Protocol

Online Status			
Physical Connection			
IPv4		IPv6	
LAN Status			
IP Address			
FE80::250:7FFF:FEEA:7EC8/64 (Link)			
TX Packets		RX Packets	
2		0	
TX Bytes		RX Bytes	
156		0	
WAN IPv6 Status			
Enable		Mode	
No		Offline	
IP		Up Time	
---		---	
		Gateway IP	
---		---	

Detailed explanation (for IPv4) is shown below:

Item	Description
LAN Status	<p>Primary DNS-Displays the primary DNS server address for WAN interface.</p> <p>Secondary DNS -Displays the secondary DNS server address for WAN interface.</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 received packets at the LAN interface.</p>
WAN1/WAN2/WAN3 Status	<p>Enable – Yes in red means such interface is available but not enabled. Yes in green means such interface is enabled.</p> <p>Line – Displays the physical connection (VDSL, ADSL, Ethernet, or USB) of this interface.</p> <p>Name – Display the name of the router.</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 speed of transmitted octets at the LAN interface.</p> <p>RX Bytes - Displays the speed of received octets at the LAN interface.</p>
WAN IPv6 Status	<p>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.</p> <p>Mode - Displays the type of WAN connection (e.g., TSPC).</p>

Item	Description
	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.

1.6.2 Virtual WAN

Such page displays the virtual WAN connection information.

Virtual WAN are used by TR-069 management.

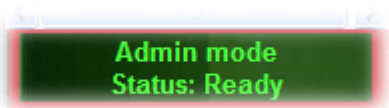
The field of Application will list the purpose of such WAN connection.

Online Status

Virtual WAN						System Uptime: 69:7:20
WAN 5 Status						
Enable	Line	Name	Mode	Up Time	Application	
Yes	ADSL		---	00:00:00	Management	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)	
---	---	0	0	0	0	
WAN 6 Status						
Enable	Line	Name	Mode	Up Time	Application	
Yes	ADSL		---	00:00:00	Management	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)	
---	---	0	0	0	0	
WAN 7 Status						
Enable	Line	Name	Mode	Up Time	Application	
Yes	ADSL		---	00:00:00	Management	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)	
---	---	0	0	0	0	

1.7 Saving Configuration

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



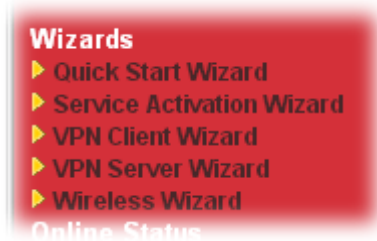
Ready indicates the system is ready for you to input settings.

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

2

Quick Setup

There are several setup wizards offered for you to configure the router simply and quickly.



- **Quick Start Wizard** – used for building network connection, Internet access.
- **Service Activation Wizard** – used for activating the web content filter service.
- **VPN Client Wizard** – used for establishing VPN tunnel; the router is treated as a VPN client.
- **VPN Server Wizard** – used for establishing VPN tunnel; the router is treated as a VPN server.
- **Wireless Wizard** – used for building wireless LAN connection.

2.1 Quick Start Wizard

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

Quick Start Wizard

Enter login password

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

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

On the next page as shown below, please select the WAN interface that you use. If DSL interface is used, please choose WAN1; if Ethernet interface is used, please choose WAN2; if 3G USB modem is used, please choose WAN3. Then click **Next** for next step.

Quick Start Wizard

WAN Interface

WAN Interface:	WAN1 ▾
Display Name:	<input type="text"/>
Physical Mode:	ADSL
Physical Type:	Auto negotiation ▾
VLAN Tag insertion (ADSL):	Disable ▾

[< Back](#) [Next >](#) [Finish](#) [Cancel](#)

WAN1, WAN2 and WAN3 will bring up different configuration page. Refer to the following for detailed information.

2.1.1 For WAN1 (ADSL)

WAN1 is specified for ADSL connection. Please select the appropriate Internet access type **according to the information from your ISP**.

Quick Start Wizard

WAN Interface

WAN Interface:	WAN1 ▾
Display Name:	<input type="text"/>
Physical Mode:	ADSL
Physical Type:	Auto negotiation ▾
VLAN Tag insertion (ADSL):	Disable ▾

[< Back](#) [Next >](#) [Finish](#) [Cancel](#)

Available settings are explained as follows:

Item	Description
Display Name	Type a name to identify such WAN.
Physical Mode	Display the physical mode (ADSL) for such router.

VLAN Tag insertion (ADSL)	<p>The settings configured in this field are available for WAN1 and WAN2.</p> <p>Enable – Enable the function of VLAN with tag.</p> <p>The router will add specific VLAN number to all packets on the WAN while sending them out.</p> <p>Please type the tag value and specify the priority for the packets sending by WAN1.</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 from 0 to 4095.</p> <p>Priority – Type the packet priority number for such VLAN. The range is from 0 to 7.</p>
----------------------------------	---

2.1.1.1 PPPoE/PPPoA

PPPoE/PPPoA: 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.

1. Choose **WAN1** as WAN Interface and click the **Next** button; you will get the following page. Choose **PPPoE XXXX** or **PPPoA XXXXX** as the protocol.

Quick Start Wizard

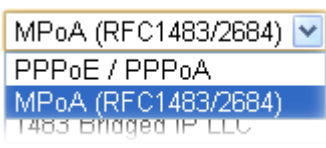
Connect to Internet

WAN 1	
Protocol	PPPoE / PPPoA
Encapsulation	PPPoE LLC/SNAP
VPI	0 Auto detect
VCI	33
Fixed IP	<input type="radio"/> Yes <input checked="" type="radio"/> No(Dynamic IP)
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS	8.8.8.8
Second DNS	8.8.4.4

< Back
Next >
Finish
Cancel

Available settings are explained as follows:

Item	Description
Protocol	There are two modes offered for you to choose for WAN1 interface.

	 <p>Choose PPPoE/PPPoA as the protocol.</p>
Encapsulation	There are several modes offered for you to choose for WAN1 interface.
VPI	Type in the value provided by ISP. Auto detect – Click this button to have the VPI and VCI to be detected by the system automatically
VCI	Type in the value provided by ISP.
Fixed IP	Click Yes to enable Fixed IP feature.
IP Address	Type the IP address if Fixed IP is enabled.
Subnet Mask	Type the subnet mask.
Default Gateway	Type the IP address as the default 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.

2. After finished the above settings, simply click **Next**.

Quick Start Wizard

Set PPPoE / PPPoA

WAN 1

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

Username	Type in the valid user name (maximum 63 characters) provided by the ISP in this field.
Password	Type 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. Then click **Next** for viewing summary of such connection.

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN1
Physical Mode:	ADSL
VPI:	0
VCI:	33
Protocol / Encapsulation:	PPPoE / LLC
Fixed IP:	No
Primary DNS:	8.8.8.8
Secondary DNS:	8.8.4.4

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

Quick Start Wizard Setup OK !!!

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

MPoA

1. Choose **WAN1** as WAN Interface and click the **Next** button; you will get the following page. Choose **MPoA** as the protocol.

Quick Start Wizard

Connect to Internet

WAN 1

Protocol	MPoA (RFC1483/2684) ▼	
Encapsulation	1483 Bridged IP LLC ▼	
VPI	0	Auto detect
VCI	33	
Fixed IP	<input type="radio"/> Yes <input checked="" type="radio"/> No(Dynamic IP)	
IP Address	<input type="text"/>	
Subnet Mask	<input type="text"/>	
Default Gateway	<input type="text"/>	
Primary DNS	8.8.8.8	
Second DNS	8.8.4.4	

Available settings are explained as follows:

Item	Description
Encapsulation	There are several modes offered for you to choose for WAN1 interface.
VPI	Type in the value provided by ISP. Auto detect – Click this button to have the VPI and VCI to be detected by the system automatically
VCI	Type in the value provided by ISP.
Fixed IP	Click Yes to enable Fixed IP feature.
IP Address	Type the IP address if Fixed IP is enabled.
Subnet Mask	Type the subnet mask.
Default Gateway	Type the IP address as the default 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.

2. Please type in the IP address/mask/gateway information originally provided by your ISP. Then click **Next** for viewing summary of such connection.

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN1
Physical Mode:	ADSL
VPI:	0
VCI:	33
Protocol / Encapsulation:	1483 Bridge LLC
Fixed IP:	No
Primary DNS:	8.8.8.8
Secondary DNS:	8.8.4.4

< Back

Next >

Finish

Cancel

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

Quick Start Wizard Setup OK !!!

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

2.1.2 For WAN2 (Ethernet)

WAN2 is dedicated to physical mode in Ethernet. If you choose WAN2, please specify physical type. Then, click **Next**.


Quick Start Wizard

WAN Interface

WAN Interface:	WAN2
Display Name:	
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
VLAN Tag insertion	Enable
Tag value	0 (0~4095)
Priority	0 (0~7)

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
Display Name	Type a name for the router.
Physical Type	<p>You can change the physical type for WAN2 or choose Auto negotiation for determined by the system.</p> 
VLAN Tag insertion	<p>The settings configured in this field are available for WAN1 and WAN2.</p> <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. Please type the tag value and specify the priority for the packets sending by WAN1.</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 packet priority number for such VLAN. The range is from 0 to 7.</p>

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

Quick Start Wizard

Connect to Internet

WAN 2

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

- ☒ PPPoE
- ☐ PPTP
- ☐ L2TP
- ☐ Static IP
- ☐ DHCP

< Back

Next >

Finish

Cancel

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.

1. Choose **WAN2** 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 2

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 continue.

Quick Start Wizard

PPPoE Client Mode

WAN 2
Enter the user name and password provided by your ISP.

Service Name (Optional)	<input type="text" value="CHT"/>
Username	<input type="text" value="84005657@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.
Username	Type in the valid user name (maximum 63 characters) provided by the ISP in this field.
Password	Type 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:	WAN2
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.

[< 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.

PPTP/L2TP

1. Choose **WAN2** 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 2

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

- ☐ PPPoE
- ☒ PPTP
- ☐ L2TP
- ☐ Static IP
- ☐ DHCP

< Back

Next >

Finish

Cancel

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

Quick Start Wizard

L2TP Client Mode

WAN 2

Enter the username, password, WAN IP configuration and L2TP server IP provided by your ISP.

Username	<input type="text" value="test"/>
Password	<input type="password" value="...."/>
Confirm Password	<input type="password" value="...."/>
WAN IP Configuration	
<input type="radio"/> Obtain an IP address automatically	
<input checked="" type="radio"/> Specify an IP address	
IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Gateway	<input type="text"/>
L2TP Server	<input type="text"/>

< Back

Next >

Finish

Cancel

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.

- Please type in the IP address/mask/gateway information originally provided by your ISP. Then click **Next** for viewing summary of such connection.

Quick Start Wizard

Please confirm your settings:

WAN Interface: WAN2
 Physical Mode: Ethernet
 Physical Type: Auto negotiation
 Internet Access: L2TP

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.

Static IP

1. Choose **WAN2** 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 2

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 Internet Access type. Simply click **Next** to continue.

Quick Start Wizard

Static IP Client Mode

WAN 2

Enter the Static IP configuration provided by your ISP.

WAN IP	172.16.3.102
Subnet Mask	255.255.0.0
Gateway	172.16.1.1
Primary DNS	8.8.8.8
Secondary DNS	8.8.4.4 (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.

3. Please type in the IP address information originally provided by your ISP. Then click **Next** for next step.

Quick Start Wizard

Please confirm your settings:

WAN Interface: WAN2
 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.

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

Quick Start Wizard Setup OK !!!

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

DHCP

1. Choose **WAN2** as 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 2

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

- ☐ PPPoE
- ☐ PPTP
- ☐ L2TP
- ☐ Static IP
- ☒ DHCP

< Back

Next >

Finish

Cancel

2. Click **DHCP** as the Internet Access type. Simply click **Next** to continue.

Quick Start Wizard

DHCP Client Mode

WAN 2

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

Host Name

(optional)

MAC

- - - - - (optional)

< Back

Next >

Finish

Cancel

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 finished the settings above, click **Next** for viewing summary of such connection.

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN2
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.

2.1.3 For WAN3 (USB)

To use 3G USB modem for network connection, please choose WAN3.

1. Choose **WAN3** as WAN Interface.

Quick Start Wizard

WAN Interface

WAN Interface:	WAN3 ▼
Display Name:	<input type="text"/>
Physical Mode:	USB

< Back Next > Finish Cancel

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

Quick Start Wizard

Connect to Internet

WAN 3	
Internet Access :	3G/4G USB Modem(PPP mode) ▼
3G/4G USB Modem(PPP mode)	
SIM PIN code	<input type="text"/>
Modem Initial String	AT&FE0V1X1&D2&C1S0=0 (Default:AT&FE0V1X1&D2&C1S0=0)
APN Name	<input type="text"/> Apply

< Back Next > Finish Cancel

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)	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. Modem Initial String – Such value is used to initialize USB modem. Please use the default value. If you have any

	<p>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>
3G/4G USB Modem (DHCP mode)	<p>SIM Pin code –Type PIN code of the SIM card that will be used to access Internet.</p> <p>Network Mode – Force Vigor router to connect Internet with the mode specified here. If you choose 4G/3G/2G as network mode, the router will choose a suitable one according to the actual wireless signal automatically.</p> <p>APN Name – APN means Access Point Name which is provided and required by some ISPs.</p>

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

Quick Start Wizard

Please confirm your settings:

WAN Interface: WAN3
 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.

- 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 activate WCF service (Web Content Filter) 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.**

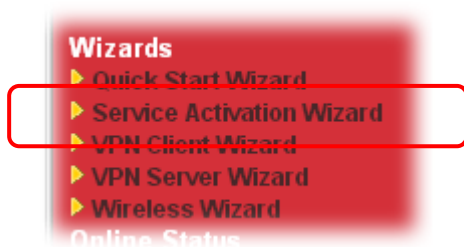
Service Activation Wizard is a tool which allows you to use trial version or update the license of WCF directly without accessing into the server (**MyVigor**) located on <http://myvigor.draytek.com>. For using Web Content Filter Profile, please refer to later section **Web Content Filter Profile** for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

Note 1: Web Content Filter (WCF) is not a built-in service of Vigor router but a service powered by **CommTouch**. If you want to use such service (trial or formal edition), you have to perform the procedure of activation first. For the service of formal edition, please contact with your dealer/distributor for detailed information.

Note 2: CommTouch is merged by **Cyren**, and **GlobalView** services will be continued to deliver powerful cloud-based information security solutions! Refer to: <http://www.prnewswire.com/news-releases/commtouch-is-now-cyren-239025151.html>

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

1. Open **Service Activation Wizard**.



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

Next >

Finish

Cancel

Free trial edition: it offers a period of trial for you to get acquainted with WCF function.

3. In the following page, you can activate the Web content filter services 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.

For WCF service :

☐ Web Content Filter (BPjM) [License Agreement](#) Activation Date : 2015-04-28
BPjM is the web content filter based on service operated in Germany. We recommend only users live in Germany to try the BPjM WCF service. This is a free service without guarantee.

☒ Web Content Filter (Cyren / Commtouch) [License Agreement](#) Activation Date : 2015-04-28
Cyren (Commtouch) is the web content filter based on Cyren (Commtouch) operated in the worldwide. There is a 30-day trial period. After trial, you can purchase DrayTek's prepared Cyren (Commtouch) GlobalView WCF package from retailing outlets.

☒ 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.

< Back Next > Finish Cancel

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. In addition, Commtouch is merged by **Cyren**, and **GlobalView** services will be continued to deliver powerful cloud-based information security solutions! Refer to:

<http://www.prnewswire.com/news-releases/commtouch-is-now-cyren-239025151.html>

BPjM is WCF for German Speaking users. The fragfINN is whitelist for German Speaking users. The BPjM is ideal for your family to provide more Internet security for youngsters.

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.

< Back Next > Finish Cancel

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

Next >

Finish

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

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

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

Service Activation Wizard

Server Enabled!

DrayTek Service Activation

Service Name	Start Date	Expire Date	Status
Web Content filter	2011-09-21	2011-10-22	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.

When all the trial editions for various web content filters had been enabled, the configuration page of Service Activation Wizard will be invalid as shown below.

Service Activation Wizard

Select the service type that you want to activate

This wizard is used for activating
- N/A
Please choose the edition you need.

☒ Free trial edition

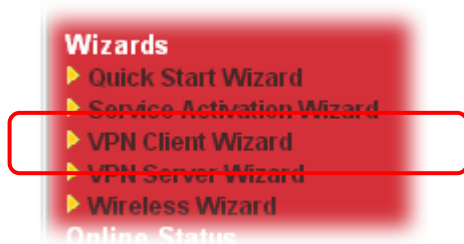
Next >

Finish

Cancel

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:

Route Mode ▾

Please choose a LAN-to-LAN Profile:

[Index] [Status] [Name] ▾

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

< Back

Next >

Finish

Cancel

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>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)

1. L2TP over IPSec
2. IPSec
3. PPTP (Encryption)
4. L2TP
5. PPTP (None Encryption)

Throughput ranking (1 is the highest; 5 is the lowest)

1. PPTP (None Encryption)
2. L2TP
3. IPSec
4. L2TP over IPSec
5. PPTP (Encryption)

Select VPN Type:

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

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

- 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. 5551234, 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

- 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

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

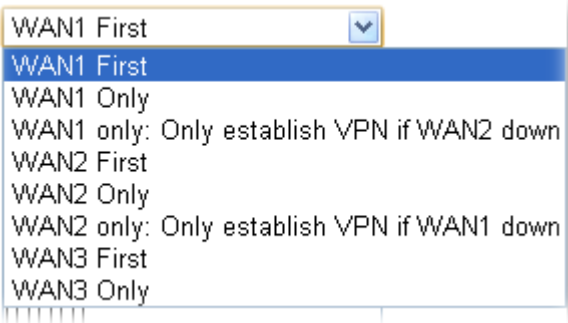
VPN and Remote Access >> VPN Client Wizard

VPN Client L2TP over IPSec (Nice to Have) Settings

Profile Name	VPN-2
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)	
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 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

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 - While connecting, the router will use WAN1/WAN2/WAN3 as the first channel for VPN connection. If WAN1/WAN2/WAN3 fails, the router will use another WAN interface instead.</p> <p>WAN1 Only /WAN2 Only/WAN 3 Only- While connecting, the router will use WAN1/WAN2/WAN3 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>
Always On	Check to enable router always keep VPN connection.
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. 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> <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>

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.

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

VPN and Remote Access >> VPN Client Wizard

Please confirm your settings

LAN-to-LAN Index:	3
Profile Name:	VPN-1
VPN Connection Type:	L2TP over IPSec (Must)
VPN Connection Through:	WAN1 First
Always on:	No
Server IP/Host Name:	draytek.com
IKE Authentication Method:	Digital Signature (X.509)
IPSec Security Method:	AH-SHA1
Remote Network IP:	192.168.1.6
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:

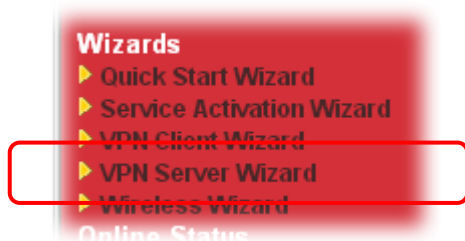
- ☒ Go to the VPN Connection Management.
- ☐ Do another VPN Client Wizard setup.
- ☐ View more detailed configurations.

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.



1. Open **VPN and Remote Access>>VPN Server Wizard**. The following page will appear.

VPN Server Wizard

Choose VPN Establishment Environment

VPN Server Mode Selection:	Remote Dial-in User (Teleworker) ▼
Please choose a LAN-to-LAN Profile:	4 x ??? ▼
Please choose a Dial-in User Accounts:	17 x ??? ▼
Allowed Dial-in Type:	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec <input checked="" type="checkbox"/> L2TP with IPsec Policy None ▼ <input checked="" type="checkbox"/> SSL Tunnel

< 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><div>Site to Site VPN (LAN-to-LAN) ▼</div><div>Site to Site VPN (LAN-to-LAN)</div><div>Remote Dial-in User (Teleworker)</div></div>

<p>Please choose a LAN-to-LAN Profile</p>	<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> <table><tr><th>[Index]</th><th>[Status]</th><th>[Name]</th></tr><tr><td>1</td><td>x</td><td>???</td></tr><tr><td>2</td><td>x</td><td>???</td></tr><tr><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></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> <div><div><input checked="" type="checkbox"/> PPTP</div><div><input checked="" type="checkbox"/> IPsec</div><div><input checked="" type="checkbox"/> L2TP with IPsec Policy</div><div><input checked="" type="checkbox"/> SSL Tunnel</div></div> <div><div>None</div><div>None</div><div>Nice to Have</div><div>Must</div></div> <p>Different Dial-in Type will lead to different configuration page. In addition, adjustable items for each dial-in type will be changed according to the VPN Server Mode (Site to Site VPN and Remote Dial-in User) selected.</p>																																																																																										

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

Here we take the examples of choosing **Remote-Dial-in User** as the **VPN Server Mode**.

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

VPN Server Wizard

VPN Authentication Setting

Profile Name	???
PPTP / L2TP / L2TP over IPsec / SSL Tunnel Authentication	
Username	???
Password	
Peer IP/VPN Client IP	
Site to Site Information	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

- When you check **PPTP/IPSec/L2TP** (three types) or **PPTP/IPSec** (two types) or **L2TP with Policy (Nice to Have/Must)**, you will see the following graphic:

VPN and Remote Access >> VPN Server Wizard

VPN Authentication Setting

PPTP / L2TP / L2TP over IPsec Authentication	
Username	server1
Password	
IPSec / L2TP over IPsec Authentication	
<input checked="" type="checkbox"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input type="checkbox"/> Digital Signature (X.509)	
Peer ID	None
Peer IP/VPN Client IP	192.168.1.99
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

None

Peer IP/VPN Client IP

Peer ID

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.
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 of the remote host) for building VPN connection.
Remote Network Mask	Please type the network mask (according to the real location of the remote host) for building VPN connection.

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

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.

< 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.

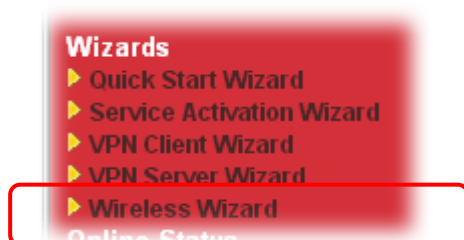
2.5 Wireless Wizard

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).

Note: This wizard is available for “n” model only.

Follow the steps listed below:

1. Open **Wireless Wizard**.



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

Wireless Wizard

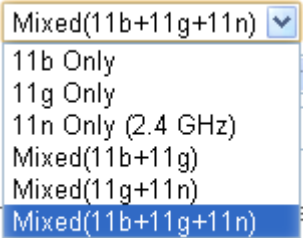
Host AP Configuration

Name:	<input type="text" value="DrayTek"/>
Mode:	<input type="text" value="Mixed(11b+11g+11n)"/>
Channel:	<input type="text" value="Channel 6, 2437MHz"/>
Password:	<input type="text" value="1235678996"/>

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. The default name is defined with DrayTek.
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.
Security Key	<p>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.</p> <p>Either 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").</p>
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:

Security key:

Rate Control:
 ☐ Enable
 Upload kbps
 Download kbps

Bandwidth Limit:
 ☐ Enable
 Total Upload kbps
 Total Download kbps

Note: The configured guest AP will not be able to access VPN connections or communicate with wireless devices connecting to the router's other APs. The guest AP will be configured to be not able to connect to LAN interfaces also. However if the VLAN configurations were already made, then the guest AP will be able to connect to LAN ports belonging in the same VLAN group. This AP interface is by default configured 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)

Security Key	<p>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.</p> <p>Either 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").</p>
Rate Control	<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>
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 following page will display the configuration summary for wireless setting.

Wireless Wizard

Configuration Summary

Basic Wireless Settings

Mode: Mixed(11b+11g+11n)
Channel: Channel 6, 2437MHz

Host AP Configurations

Name: DrayTek
Security key: *****

Guest AP Configurations

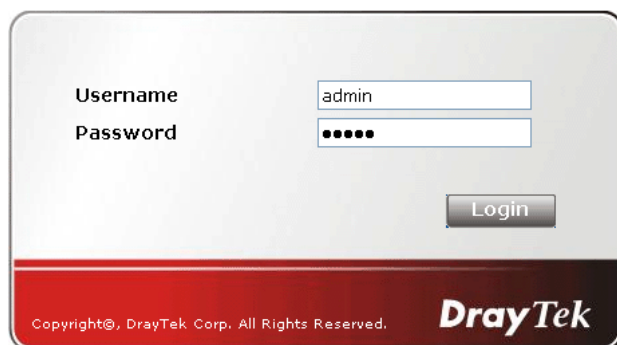
Status: Disabled
Name: DrayTek_Guest
Security key: *****
Rate Control: Disabled

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

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.



The image shows the login page of the Vigor router's web configuration interface. It features a light gray background with a white login form. The form has two input fields: 'Username' with the text 'admin' and 'Password' with five black dots. A 'Login' button is located to the right of the password field. At the bottom of the page, there is a red banner with the text 'Copyright©, DrayTek Corp. All Rights Reserved.' and the 'DrayTek' logo.

- 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**. If not, please refer to section **4.13 Creating an Account for MyVigor**.



Please take a moment to register.

Membership Registration entitles you to upgrade firmware for your purchased product and receive news about upcoming products and services!

Once you receive the DrayTek membership, welcome your further login to advise us of your opinion about DrayTek product. Your precious suggestions will be of further help for innovation and enhancement. By joining MyVigor, your data will be handled carefully and not passed onto any 3rd party unrelated organizations. Your data will only be used/accessed by DrayTek Corp and regional offices/agents within your own country.

LOGIN

Language : English

UserName :

Password :

Auth Code :

20290

[Forgotten password?](#)

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

Become the MyVigor member, you can receive the e-newsletter update.
Please join customer survey after you are a member! Your opinion is very appreciated.

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

DrayTek Login User : carrieni (Logout) **MyVigor**

About Us

My Information

My Product

My Password

My Settings

Vigor Series

Product Registration

Customer Survey

My Information - My Products

Welcome, **carrieni**
Last login time : 2015-02-25 10:00:31
Last login from : 220.132.109.130
Current login time : 2015-03-04 13:35:34
Current login from : 220.132.109.130

Rows : 10 Page : 1

My Device List

Serial Number / Host ID	Device Name	Model	Note
111900325027	2130	Vigor2130	-
2013030811172502	vigor2760	Vigor2760	-

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

DrayTek Login User : carrieni (Logout) MyVigor

Search for this site GO

Printable page Email to Friend(s)

My Information - My Products

Registration Device

Registration Date : * 03-04-2015

Serial number : 2015030413341201

Nickname : * Vigor2830

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

- 6 When the following page appears, your router information has been added to the database.

Your device has been successfully added to the database.

OK

- 7 Now, you have finished the product registration.
- 8 After clicking **OK**, you will see the following page. Your router has been registered to myvigor website successfully.

DrayTek Login User : carrieni (Logout) MyVigor

My Information - My Products

Welcome, carrieni

Last login time : 2015-02-25 10:00:31

Last login from : 220.132.109.130

Current login time : 2015-03-04 13:35:34

Current login from : 220.132.109.130

Rows : 10 Page : 1

My Device List

Serial Number / Host ID	Device Name	Model	Note
111900325027	2130	Vigor2130	-
2013030811172502	vigor2760	Vigor2760	-
2015022415571701	Vigor2830	Vigor2830	-

3

Advanced Configuration

This chapter will guide users to execute advanced web configuration.

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. Note that different model will have different web pages.

The screenshot shows the Vigor2830n v2 web interface. The left sidebar contains a menu with options like Wizards, Online Status, WAN, LAN, Load-Balance/Route Policy, NAT, Firewall, User Management, Objects Setting, CSM, Bandwidth Management, Applications, VPN and Remote Access, Certificate Management, Wireless LAN, SSL VPN, USB Application, System Maintenance, Diagnostics, External Devices, and Support Area. The main content area displays the System Status page, which includes a table for LAN settings, a table for Wireless LAN settings, a table for WAN settings, and a table for IPv6 settings.

LAN					
	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-1D-AA-00-00-00	192.168.1.1	255.255.255.0	ON	8.8.8.8
LAN2	00-1D-AA-00-00-00	192.168.2.1	255.255.255.0	ON	8.8.8.8
LAN3	00-1D-AA-00-00-00	192.168.3.1	255.255.255.0	ON	8.8.8.8
LAN4	00-1D-AA-00-00-00	192.168.4.1	255.255.255.0	ON	8.8.8.8
IP Routed Subnet	00-1D-AA-00-00-00	192.168.0.1	255.255.255.0	ON	8.8.8.8

Wireless LAN			
MAC Address	Frequency Domain	Firmware Version	SSID
00-1D-AA-00-00-00	Europe	2.7.1.5	DrayTek

WAN					
	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Disconnected	00-1D-AA-00-00-01	PPPoE	---	---
WAN2	Disconnected	00-1D-AA-00-00-02	---	---	---
WAN3	Disconnected	00-1D-AA-00-00-03	---	---	---

IPv6		
Address	Scope	Internet Access Mode
LAN FE80::21D:AAFF:FE00:0/64	Link	---

3.1 WAN

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

3.1.1 Basics of Internet Protocol (IP) Network

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

From 10.0.0.0 to 10.255.255.255

From 172.16.0.0 to 172.31.255.255

From 192.168.0.0 to 192.168.255.255

What are Public IP Address and Private IP Address

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

Get Your Public IP Address from ISP

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

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

Network Connection by 3G/4G USB Modem

For 3G/4G mobile communication through Access Point is popular more and more, Vigor2830 adds the function of 3G/4G network connection for such purpose. By connecting 3G/4G USB Modem to the USB port of Vigor2830, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor2830n with 3G/4G USB Modem allows you to receive 3G signals at any place such as your car or certain location holding outdoor activity and share the bandwidth for using by more people. Users can use four LAN ports on the router to access Internet. Also, they can access Internet via 802.11n wireless function of Vigor2830n, and enjoy the powerful firewall, bandwidth management, VPN features of Vigor2830n series.



After connecting into the router, 3G/4G USB Modem will be regarded as the third WAN port. However, the original WAN1 and WAN2 still can be used and Load-Balance can be done in the router. Besides, 3G/4G USB Modem in WAN3 also can be used as backup device. Therefore, when WAN1 and WAN2 are not available, the router will use 3.5G for supporting automatically. The supported 3G/4G USB Modem will be listed on DrayTek web site. Please visit www.draytek.com for more detailed information.

Below shows the menu items for WAN.



3.1.2 General Setup

This section will introduce some general settings of Internet and explain the connection modes for WAN1, WAN2 and WAN3 in details.

This router supports multiple-WAN 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. Please configure WAN1, WAN2 and WAN3 settings.

This webpage allows you to set general setup for WAN1, WAN2 and WAN3 respectively.

WAN >> General Setup

Load Balance Mode:

Setup				
Index	Enable	Physical Mode/Type	Line Speed(Kbps) DownLink/UpLink	Active Mode
WAN1	V	ADSL/-	0 / 0	Always On
WAN2	V	Ethernet/Auto negotiation	0 / 0	Always On
WAN3	V	USB/-	0 / 0	Always On

Note: The line speed setting of WAN interface is available only when According to Line Speed is selected as the Load Balance Mode.

OK

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 Weight to let the router reach the best load balance.</p> <p>Load Balance Mode: <input type="text" value="Auto Weight"/> Auto Weight According to Line Speed</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	Display the downstream and upstream rate of such WAN interface.
Active Mode	Display whether such WAN interface is Active device or backup device.

Note: In default, each WAN port is enabled.

WAN1 with ADSL

WAN1 is fixed with physical mode of ADSL.

WAN >> General Setup

WAN 1

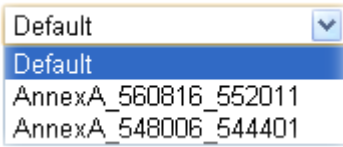
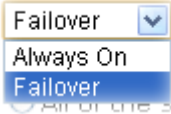
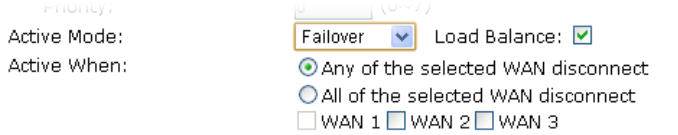
Enable:	<input type="button" value="Yes"/>
Display Name:	<input type="text"/>
Physical Mode:	ADSL
Physical Type:	<input type="button" value="Auto negotiation"/>
DSL Modem Code:	<input type="button" value="Default"/>
Line Speed(Kbps):	
DownLink	<input type="text"/>
UpLink	<input type="text"/>
VLAN Tag insertion :	<input type="button" value="Disable"/> (for channel 1)
Tag value:	<input type="text"/> (0~4095)
Priority:	<input type="text"/> (0~7)
Active Mode:	<input type="button" value="Failover"/> Load Balance: <input checked="" type="checkbox"/>
Active When:	<input checked="" type="radio"/> Any of the selected WAN disconnect <input type="radio"/> All of the selected WAN disconnect <input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3

Note:

The line speed setting of WAN interface is available only when According to Line Speed is selected as the Load Balance Mode.

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	In such WAN interface, no type can be selected.
DSL Modem Code	Choose the correct DSL modem code for ensuring the network connection.

	 <p>If you have no idea about the selection, simply choose Default or contact the dealer for assistance.</p>
Line Speed	<p>If you 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.</p>
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. Please type the tag value and specify the priority for the packets sending by WAN1.</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 from 0 to 4095.</p> <p>Priority – Type the packet priority number for such VLAN. The range is from 0 to 7.</p>
Active Mode	<p>Choose Always On to make the WAN1 connection being activated always.</p>  <p>Load Balance: Check this box to enable auto load balance function for such WAN interface. When the data traffic is large, the WAN interface with the function enabled will balance the data transmission automatically among all of the WAN interfaces in connection status.</p>
Active When	<p>If you choose Failover as the Active Mode, Active When will appear. You have to specify which role the WAN interface should play if you want to backup multiple WANs. However, ignore this setting if you want to backup a single WAN.</p>  <p>Any of the selected WAN disconnect – Such backup WAN will be activated when any master WAN interface disconnects.</p> <p>All of the selected WAN disconnect – Such backup WAN will be activated only when all master WAN interfaces disconnect.</p>

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

WAN2 with Ethernet

WAN2 is fixed with physical mode of Ethernet.

WAN >> General Setup

WAN 2

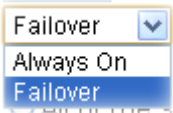
Enable:	Yes <input type="button" value="v"/>
Display Name:	<input type="text"/>
Physical Mode:	Ethernet <input type="button" value="v"/>
Physical Type:	Auto negotiation <input type="button" value="v"/>
Line Speed(Kbps):	
DownLink	<input type="text" value="0"/>
UpLink	<input type="text" value="0"/>
VLAN Tag insertion :	Disable <input type="button" value="v"/> (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:	Failover <input type="button" value="v"/> Load Balance: <input checked="" type="checkbox"/>
Active When:	<input checked="" type="radio"/> Any of the selected WAN disconnect <input type="radio"/> All of the selected WAN disconnect <input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3

Note:

The line speed setting of WAN interface is available only when According to Line Speed is selected as the Load Balance Mode.

Available settings are explained as follows:

Item	Description
Enable	Choose Yes to invoke the settings for this WAN interface. Choose No to disable the settings for this WAN interface.
Display Name	Type the description for such WAN interface.
Physical Mode	Display the physical mode of such WAN interface.
Physical type	You can change the physical type for WAN2 or choose Auto negotiation for determined by the system. <div> <input type="button" value="v"/> <div> Auto negotiation Auto negotiation 10M half duplex 10M full duplex 100M half duplex 100M full duplex 1000M full duplex </div> </div>
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.
VLAN Tag insertion	Enable – Enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the WAN while sending them out.

	<p>Please type the tag value and specify the priority for the packets sending by WAN1.</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 packet priority number for such VLAN. The range is from 0 to 7.</p>
Active Mode	<p>Choose Always On to make such WAN connection being activated always.</p>  <p>Load Balance: 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>
Active When	<p>If you choose Failover as the Active Mode, Active When will appear. You have to specify which role the WAN interface should play if you want to backup multiple WANs. However, ignore this setting if you want to backup a single WAN.</p> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 20px;"> <p>Active Mode: Failover</p> <p>Active When:</p> </div> <div> <p>Load Balance: <input checked="" type="checkbox"/></p> <p><input checked="" type="radio"/> Any of the selected WAN disconnect</p> <p><input type="radio"/> All of the selected WAN disconnect</p> <p><input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3</p> </div> </div> <p>Any of the selected WAN disconnect – Such backup WAN will be activated when any master WAN interface disconnects.</p> <p>All of the selected WAN disconnect – Such backup WAN will be activated only when all master WAN interfaces disconnect.</p>

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

WAN3 with USB

To use 3G network connection through 3G/4G USB Modem, please configure **WAN3** interface.

WAN >> General Setup

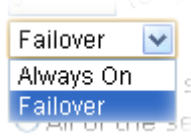
WAN 3

Enable:	<input type="button" value="Yes"/>
Display Name:	<input type="text"/>
Physical Mode:	USB
Line Speed(Kbps):	
DownLink	<input type="text"/>
UpLink	<input type="text"/>
Active Mode:	<input type="button" value="Failover"/> Load Balance: <input checked="" type="checkbox"/>
Active When:	<input checked="" type="radio"/> Any of the selected WAN disconnect <input type="radio"/> All of the selected WAN disconnect
	<input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3

Note:

The line speed setting of WAN interface is available only when According to Line Speed is selected as the Load Balance Mode.

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	In such WAN interface, no type can be selected.
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	<p>Choose Always On to make such WAN connection being activated always.</p>  <p>Load Balance: 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>

Active When	<p>If you choose Failover as the Active Mode, Active When will appear. You have to specify which role the WAN interface should play if you want to backup multiple WANs. However, ignore this setting if you want to backup a single WAN.</p> <p>Active When:</p> <p> <input checked="" type="radio"/> Any of the selected WAN disconnect <input type="radio"/> All of the selected WAN disconnect <input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 </p> <p>Any of the selected WAN disconnect – Such backup WAN will be activated when any master WAN interface disconnects.</p> <p>All of the selected WAN disconnect – Such backup WAN will be activated only when all master WAN interfaces disconnect.</p>
--------------------	--

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

3.1.3 Internet Access

For the router supports multi-WAN function, the users can set different WAN settings (for WAN1/WAN2/WAN3) for Internet Access. Due to different Physical Mode for 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		ADSL	PPPoE / PPPoA	Details Page	IPv6
WAN2		Ethernet	None	Details Page	IPv6
WAN3		USB	MPoA (RFC1483/2684)	Details Page	IPv6

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

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode		
WAN1		ADSL	PPPoE / PPPoA	Details Page	IPv6
WAN2		Ethernet	None	Details Page	IPv6
WAN3		USB	None	Details Page	IPv6

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

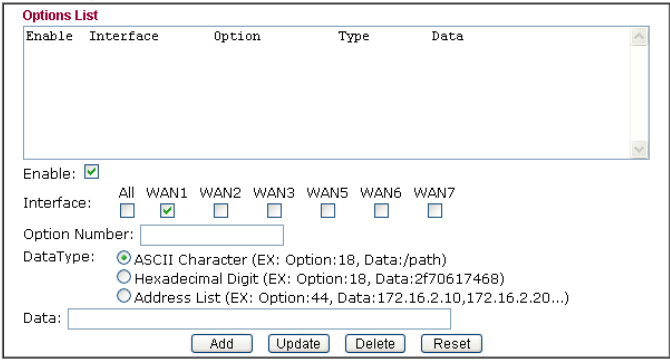
WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode		
WAN1		ADSL	PPPoE / PPPoA	Details Page	IPv6
WAN2		Ethernet	None	Details Page	IPv6
WAN3		USB	None	Details Page	IPv6

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

Available settings are explained as follows:

Item	Description
Index	Display the WAN interface.
Display Name	It shows the name of the WAN1/WAN2/WAN3 that entered in general setup.
Physical Mode	It shows the physical connection for WAN1(ADSL)/WAN2 (Ethernet) /WAN3 (3G/4G 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	<p>This button will open different web page (based on Physical Mode) to setup IPv6 Internet Access Mode for WAN interface.</p> <p>If IPv6 service is active on this WAN interface, the color of “IPv6” will become green.</p>
Advanced	<p>This button allows you to configure DHCP client options. DHCP packets can be processed by adding option number and data information when such function is enabled and configured.</p> <p>WAN >> Internet Access</p> <hr/> <p>DHCP Client Options Status</p>  <p>Note: Option 61 has been given a default value. You can configure option 61(Client Identifier) in "WAN >> Internet Access" page. If you choose to configure option 61 here, the settings in "WAN >> Internet Access, Details Page" will be overwritten. Option 12 is reserved, you cannot configure it here but you can configure it in "Router Name" field of "WAN >> Internet Access".</p> <p>OK</p> <p>Enable – Check the box to enable the function of DHCP Option. Each DHCP option is composed by an option number with data. For example, Option number:100 Data: abcd</p> <p>When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets.</p> <p>Interface – Specify the WAN interface(s) that will be overwritten by such function. WAN5 ~ WAN7 can be</p>

	<p>located under WAN>>Multi-PVCs.</p> <p>Option Number – Type a number for such function.</p> <div style="border: 1px solid black; padding: 5px;"> <p>Note: If you choose to configure option 61 here, the detailed settings in WAN>>Interface Access will be overwritten.</p> </div> <p>Data Type – Choose the type (ASCII, Hex or IP address) for the data to be stored.</p> <p>Data – Type the content of the data to be processed by the function of DHCP option.</p>
--	--

Details Page for PPPoE/PPPoA in WAN1

To choose PPPoE /PPPoA as the accessing protocol of the Internet, please select **PPPoE/PPPoA** from the **WAN>>Internet Access >>WAN1** page. The following web page will be shown.

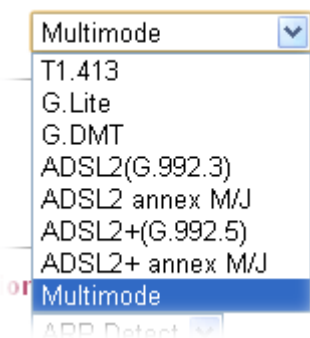
WAN 1

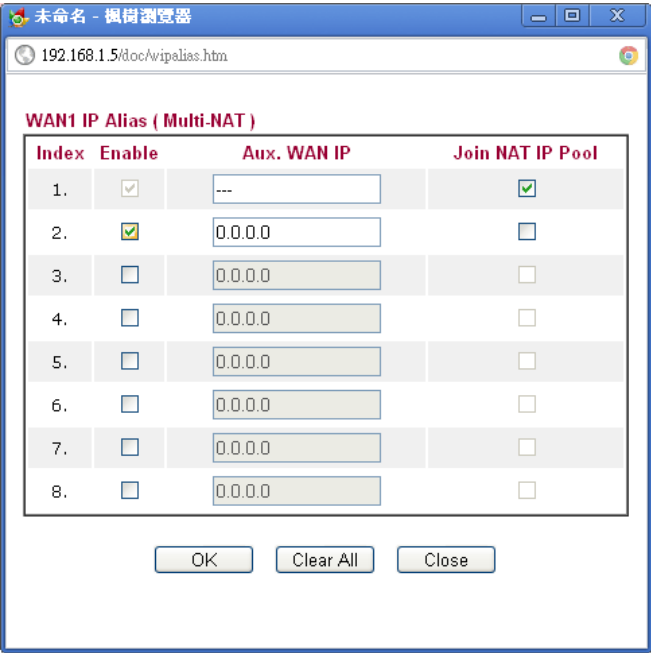
PPPoE / PPPoA	MPoA (RFC1483/2684)	IPv6
<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
DSL Modem Settings Multi-PVC channel: Channel 1 VPI: 0 VCI: 33 Encapsulating Type: LLC/SNAP Protocol: PPPoE Modulation: Multimode		
PPPoE Pass-through <input type="checkbox"/> For Wired LAN <input type="checkbox"/> For Wireless LAN		
WAN Connection Detection Mode: ARP Detect		
Bridge Mode <input type="checkbox"/> Enable Bridge Mode		
MTU : 1492 (Max:1492)		
ISP Access Setup Service Name (Optional): Username: Password: PPP Authentication: PAP or CHAP Idle Timeout: -1 second(s) IP Address From ISP : WAN IP Alias Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address: <input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: 00 1D AA 00 00 01 Index(1-15) in Schedule Setup: => , , ,		

OK Cancel

Available settings are explained as follows:

Item	Description
Enable/Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
DSL Modem Settings	<p>Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP.</p> <p>Multi-PVC channel - The selections displayed here are determined by the page of Internet Access >> Multi PVCs. Select M-PVCs Channel means no selection will be chosen.</p> <p>VPI - Type in the value provided by ISP.</p> <p>VCI - Type in the value provided by ISP.</p> <p>Encapsulating Type - Drop down the list to choose the type provided by ISP.</p> <p>Protocol - Drop down the list to choose the one (PPPoE or PPPoA) provided by ISP.</p> <p>If you have already used Quick Start Wizard to set the protocol, then it is not necessary for you to change any settings in this group.</p> <p>Modulation -Default setting is Multimode. Choose the one</p>

	<p>that fits the requirement of your router.</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> <p>Note: To have PPPoA Pass-through, please choose PPPoA protocol and check the box(es) here. The router will behave like a modem which only serves the PPPoE client on the LAN. That's, the router will offer PPPoA dial-up connection.</p>
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. If you choose Ping Detect as the detection mode, you have to type required settings for the following items.</p> <ul style="list-style-type: none"> ● Primary/Secondary Ping IP – If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● Ping Gateway IP – If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● TTL (Time to Live) – Set TTL value of PING operation. ● Ping Interval – Type the interval for the system to execute the PING operation. ● Ping Retry – Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.

Bridge Mode	Enable Bridge Mode - If you choose Bridged IP as the protocol, you can check this box to invoke the function. The router will work as a bridge modem.
MTU	It means Max Transmit Unit for packet. The default setting is 1492.
ISP Access Setup	<p>Enter your allocated username, password and authentication parameters according to the information provided by your ISP.</p> <p>Username – Type in the valid user name (maximum 63 characters) provided by the ISP in this field.</p> <p>Password – Type in the password provided by ISP in this field.</p> <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 From ISP	<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>  <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</p>

	<p>boxes of MAC Address for the router.</p> <p>Specify a MAC Address – Type the MAC address for the router manually.</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 Applications >> Schedule web page and you can use the number that you have set in that web page.</p>
--	--

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

Details Page for MPoA (RFC1483/2684) in WAN1

MPoA is a specification that enables ATM services to be integrated with existing LANs, which use either Ethernet, token-ring or TCP/IP protocols. The goal of MPoA is to allow different LANs to send packets to each other via an ATM backbone.

To use **MPoA** as the accessing protocol of the Internet, select **MPoA** from the **WAN>>Internet Access >>WAN1** page. The following web page will appear.

WAN >> Internet Access

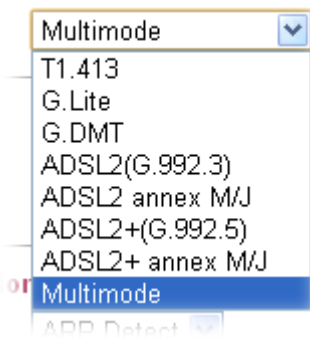
WAN 1

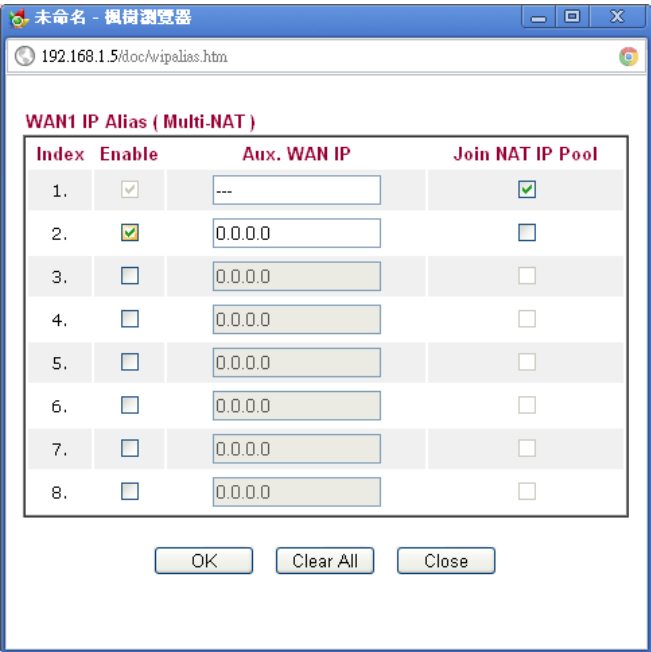
PPPoE / PPPoA	MPoA (RFC1483/2684)	IPv6
<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
DSL Modem Settings Multi-PVC channel: Channel 2 Encapsulation: 1483 Bridged IP LLC VPI: 0 VCI: 33 Modulation: Multimode		
WAN Connection Detection Mode: ARP Detect		
MTU : 1492 (Max:1500)		
RIP Protocol <input type="checkbox"/> Enable RIP		
Bridge Mode <input type="checkbox"/> Enable Bridge Mode		
WAN IP Network Settings WAN IP Alias <input type="radio"/> Obtain an IP address automatically Router Name: Vigor Domain Name: * : Required for some ISPs DHCP Client Identifier for some ISP <input type="checkbox"/> Enable Username: Password: <input checked="" type="radio"/> Specify an IP address IP Address: Subnet Mask: Gateway IP Address:		<input type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: 00 1D AA 00 00 01
DNS Server IP Address Primary IP Address: 8.8.8.8 Secondary IP Address: 8.8.4.4		

OK Cancel

Available settings are explained as follows:

Item	Description
Enable/Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
DSL Modem Settings	Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP. Multi-PVC channel - The selections displayed here are

	<p>determined by the page of Internet Access >>Multi PVCs. Select M-PVCs Channel means no selection will be chosen.</p> <p>VPI - Type in the value provided by ISP.</p> <p>VCI - Type in the value provided by ISP.</p> <p>Encapsulating - Drop down the list to choose the type provided by ISP.</p> <p>Modulation –Default setting is Multimode. Choose the one that fits the requirement of your router.</p> 
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 or Always On for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items.</p> <ul style="list-style-type: none"> ● Primary/Secondary Ping IP – If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for ping. ● Ping Gateway IP – If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for ping. With the IP address(es) ping, Vigor router can check if the WAN connection is on or off. ● TTL (Time to Live) – Set TTL value of PING operation. ● Ping Interval – Type the interval for the system to execute the PING operation. ● Ping Retry – Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
MTU	It means Max Transmit Unit for packet. The default setting is 1492.
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 choose Bridged IP as the protocol, you can check this box to invoke the function. The router will work as a

	bridge modem.
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. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.</p>  <p>Obtain an IP address automatically – Click this button to obtain the IP address automatically.</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.</p> <ul style="list-style-type: none"> ● IP Address – Type in the private IP address. ● Subnet Mask – Type in the subnet mask.

	<ul style="list-style-type: none"> ● Gateway IP Address – Type in gateway IP address. <p>Default MAC Address – Type in MAC address for the router. You can use Default MAC Address or specify another MAC address for your necessity.</p> <p>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.</p>
DNS Server IP Address	Type in the primary IP address for the router. If necessary, type in secondary IP address for necessity in the future.

Details Page for PPPoE in WAN2

To choose PPPoE as the accessing protocol of the Internet, please select **PPPoE** from the **WAN>>Internet Access >>WAN2** page. The following web page will be shown.

WAN >> Internet Access

WAN 2

PPPoE

☐ Enable
☒ Disable

Static or Dynamic IP

PPTP/L2TP

IPv6

ISP Access Setup

Service Name (Optional)

Username

Password

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

WAN Connection Detection

Mode

Primary Ping IP

Secondary Ping IP

☐ Ping Getaway IP

TTL

Ping Interval second(s)

Ping Retry times

MTU

(Max:1492)

PPP/MP Setup

PPP Authentication

Idle Timeout second(s)

IP Address Assignment Method (IPCP)

☒ WAN IP Alias

Fixed IP: ☐ Yes ☒ No (Dynamic IP)

Fixed IP Address

☒ Default MAC Address

☐ Specify a MAC Address

MAC Address:

Available settings are explained as follows:

Item	Description
Enable/Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP.

	<p>Service Name (Optional) – Type the description of the specific network service.</p> <p>Username – Type in the valid user name (maximum 63 characters) provided by the 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>
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. If you choose Ping Detect as the detection mode, you have to type required settings for the following items.</p> <ul style="list-style-type: none"> ● Primary/Secondary Ping IP – If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● Ping Gateway IP – If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● TTL (Time to Live) – Set TTL value of PING operation. ● Ping Interval – Type the interval for the system to execute the PING operation. ● Ping Retry – Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
MTU	It means Max Transmit Unit for packet.
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. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.</p>

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	<input checked="" type="checkbox"/>	---	<input checked="" type="checkbox"/>
2.	<input checked="" type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
3.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
4.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
5.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
6.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
7.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
8.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>

OK Clear All Close

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

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

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

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

Details Page for Static or Dynamic IP in WAN2

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.

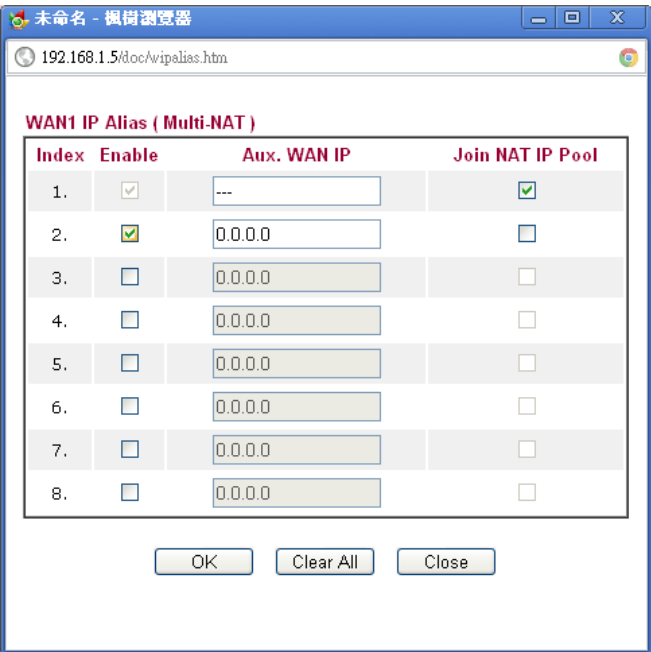
To use **Static or Dynamic IP** as the accessing protocol of the internet, please click the **Static or Dynamic IP** tab. The following web page will be shown.

WAN 2

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
<input type="radio"/> Enable <input checked="" type="radio"/> Disable		WAN IP Network Settings WAN IP Alias	
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)		<input type="radio"/> Obtain an IP address automatically Router Name <input type="text"/> * Domain Name <input type="text"/> * <small>* : Required for some ISPs</small>	
WAN Connection Detection Mode ARP Detect		DHCP Client Identifier for some ISP <input type="checkbox"/> Enable Username <input type="text"/> Password <input type="text"/>	
MTU <input type="text"/> 1500 (Max:1500)		<input checked="" type="radio"/> Specify an IP address IP Address <input type="text"/> Subnet Mask <input type="text"/> Gateway IP Address <input type="text"/>	
RIP Protocol <input type="checkbox"/> Enable RIP		<input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: <input type="text"/> 00 <input type="text"/> 1D <input type="text"/> AA <input type="text"/> 00 <input type="text"/> 00 <input type="text"/> 02	
		DNS Server IP Address Primary IP Address <input type="text"/> 8.8.8.8 Secondary IP Address <input type="text"/> 8.8.4.4	

Available settings are explained as follows:

Item	Description
Enable / Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
Keep WAN Connection	<p>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.</p> <p>PING to the IP - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive.</p> <p>PING Interval - Enter the interval for the system to execute the PING operation.</p>
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 or Always On for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items.</p> <p>● Primary/Secondary Ping IP – If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging.</p>

	<ul style="list-style-type: none"> ● Ping Gateway IP – If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● TTL (Time to Live) – Set TTL value of PING operation. ● Ping Interval – Type the interval for the system to execute the PING operation. ● Ping Retry – Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
MTU	It means Max Transmit Unit for packet.
RIP Protocol	Routing Information Protocol is abbreviated as RIP(RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.
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> <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>Default MAC Address: Click this radio button to use default MAC address for the router.</p> <p>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.</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 activate them.

Details Page for PPTP/L2TP in WAN2


To use **PPTP/L2TP** as the accessing protocol of the internet, please click the **PPTP/L2TP** tab. The following web page will be shown.

WAN >> Internet Access

WAN 2

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
<input type="radio"/> Enable PPTP <input type="radio"/> Enable L2TP <input checked="" type="radio"/> Disable		PPP Setup PPP Authentication: PAP or CHAP (dropdown) Idle Timeout: -1 second(s)	
Server Address: <input type="text"/> Specify Gateway IP Address: <input type="text"/>		IP Address Assignment Method (IPCP) <input type="button" value="WAN IP Alias"/>	
ISP Access Setup 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"/>		Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address: <input type="text"/>	
MTU <input type="text" value="1442"/> (Max: 1460)		WAN IP Network Settings <input type="radio"/> Obtain an IP address automatically <input checked="" type="radio"/> Specify an IP address IP Address: <input type="text"/> Subnet Mask: <input type="text"/>	

Detailed explanation is shown below:

Item	Description
PPTP/L2TP	<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 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	It means Max Transmit Unit for packet.
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>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>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>
WAN IP Network Settings	<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) in WAN3

To use **PPP** (for 3G/4G USB Modem) as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **PPP** mode for WAN2. The following web page will be shown.

WAN >> Internet Access

WAN 3

3G/4G USB Modem(PPP mode)	3G/4G USB Modem(DHCP mode)	IPv6
Modem Support List		
3G/4G USB Modem(PPP mode) <input checked="" type="radio"/> Enable <input 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="button" 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="button" value="ARP Detect"/>		

Available settings are explained as follows:

Item	Description
3G/4G USB Modem (PPP mode)	<p>Enable / Disable - Click Enable for activating this function. If you click Disable, this function will be closed and all the settings that you adjusted in this page will be invalid.</p> <p>SIM PIN code - Type PIN code of the SIM card that will be used to access Internet.</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.</p> <p>APN Name - APN means Access Point Name which is provided and required by some ISPs. Type the name and click Apply.</p> <p>Modem Initial String2 - The initial string 1 is shared with APN. In some cases, user may need another initial AT command to restrict 3G band or do any special settings.</p> <p>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.</p>

	<p>PPP Username - Type the PPP username (optional).</p> <p>PPP Password - Type the PPP password (optional).</p> <p>PPP Authentication - Select PAP only or PAP or CHAP for PPP.</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>
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. If you choose Ping Detect as the detection mode, you have to type required settings for the following items.</p> <ul style="list-style-type: none"> ● Primary/Secondary Ping IP – If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for ping. ● Ping Gateway IP – If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for ping. With the IP address(es) ping, Vigor router can check if the WAN connection is on or off. ● TTL (Time to Live) – Set TTL value of PING operation. ● Ping Interval – Type the interval for the system to execute the PING operation. ● Ping Retry – Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.

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

Details Page for 3G/4G USB Modem (DHCP) in WAN3

To use **3G/4G USB Modem (DHCP mode)** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **3G/4G USB Modem (DHCP mode)** for WAN3. The following web page will be shown.

WAN 3

3G/4G USB Modem(PPP mode)

3G/4G USB Modem(DHCP mode)

IPv6

[Modem Support List](#)

3G/4G USB Modem(DHCP mode)		<input checked="" type="radio"/> Enable <input type="radio"/> Disable
SIM PIN code	<input type="text"/>	
Network Mode	4G/3G/2G (Default: 4G/3G/2G)	
APN Name	<input type="text"/>	
MTU	1380 (Default: 1380)	
Path MTU Discovery	<input type="button" value="Choose IP"/>	
LTE hardware version	---	
WAN Connection Detection		
Mode	Ping Detect	
Primary Ping IP	<input type="text"/>	
Secondary Ping IP	<input type="text"/>	
<input type="checkbox"/> Ping Getaway IP	<input type="text"/>	
TTL	255	
Ping Interval	1 second(s)	
Ping Retry	10 times	

Note: Please note that in some case USB port connection will be terminated temporarily to activate the new configuration.

Available settings are explained as follows:

Item	Description
3G/4G USB Modem (DHCP 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. The maximum length of the PIN code you can set is 19 characters.
Network Mode	Force Vigor router to connect Internet with the mode specified here. If you choose 4G/3G/2G as network mode, the router will choose a suitable one according to the actual wireless signal automatically.
APN Name	APN means Access Point Name which is provided and required by some ISPs. Type the name and click Apply . The maximum length of the name you can set is 47 characters.
MTU	It means Max Transmit Unit for packet. The default setting is 1380.

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. If you choose Ping Detect as the detection mode, you have to type required settings for the following items.</p> <ul style="list-style-type: none">● Primary/Secondary Ping IP – If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging.● Ping Gateway IP – If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off.● TTL (Time to Live) – Set TTL value of PING operation.● Ping Interval – Type the interval for the system to execute the PING operation.● Ping Retry – Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.												
Modem Support List	<p>It lists all of the modems supported by such router.</p> <p>4G Modem Support List</p> <hr/> <p style="text-align: center;">Last updated on 2013-03-26</p> <table><tr><th>Standard</th><th>Brand</th><th>Module</th><th>Status</th></tr><tr><td>LTE</td><td>LG</td><td>VL600</td><td>Y</td></tr><tr><td>WIMAX</td><td>Samsung</td><td>swc-u200</td><td>Y</td></tr></table> <p>Y: Tested and is supported. M: Has not been tested but might be supported.</p>	Standard	Brand	Module	Status	LTE	LG	VL600	Y	WIMAX	Samsung	swc-u200	Y
Standard	Brand	Module	Status										
LTE	LG	VL600	Y										
WIMAX	Samsung	swc-u200	Y										

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

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

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

WAN >> Internet Access

WAN 1

PPPoE / PPPoA	MPoA (RFC1483/2684)	IPv6
<p>Internet Access Mode</p> <p>Connection Type Offline</p>		

Details Page for IPv6 – PPP in WAN1/WAN2

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

PPPoE / PPPoA	MPoA (RFC1483/2684)	IPv6
Internet Access Mode		
Connection Type		PPP
Note : IPv4 WAN setting should be PPPoE client.		

OK Cancel

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

Online Status

Physical 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	
7		8		618	
				RX Bytes	
				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	
7		4		544	
				RX Bytes	
				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

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 3

3G/4G USB Modem(PPP mode)

3G/4G USB Modem(DHCP mode)

IPv6

Internet Access Mode

Connection Type

TSPC ▼

TSPC Configuration

Username

Password

Tunnel Broker

WAN Connection Detection

Mode

Ping Detect ▼

Ping IP/Hostname

TTL(1-255,0:Auto)

OK

Cancel

Available settings are explained as follows:

Item	Description
Username	Type the name obtained from the broker. It is suggested for you to apply another username and password for http://gogonet.gogo6.com/page/freenet6-account .
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.
WAN Connection Detection	<p>Such function allows you to verify whether network connection is alive or not through Ping Detect.</p> <p>Mode – Choose Always On or Ping Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always.</p> <ul style="list-style-type: none"> ● Ping IP/Hostname – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. ● TTL (Time to Live) –If you choose Ping Detect as detection mode, you have to type TTL value.

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

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

WAN >> Internet Access



WAN 3

3G/4G USB Modem(PPP mode)

3G/4G USB Modem(DHCP mode)

IPv6

Internet Access Mode

Connection Type

AICCU

AICCU Configuration

☐ Always On

Username

Password

Tunnel Broker

tic.sixxs.net

Tunnel ID

Subnet Prefix

WAN Connection Detection

Mode

Ping Detect

Ping IP/Hostname

TTL(1-255,0:Auto)

0

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

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
WAN Connection Detection	<p>Such function allows you to verify whether network connection is alive or not through Ping Detect.</p> <p>Mode – Choose Always On or Ping Detect for the system to execute for WAN detection.</p> <ul style="list-style-type: none"> ● Ping IP/Hostname – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. ● TTL (Time to Live) –If you choose Ping Detect as detection mode, you have to type TTL value.

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

Details Page for IPv6 – DHCPv6 Client in WAN1/WAN2

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

WAN >> Internet Access



WAN 1

PPPoE / PPPoA	MPoA / Static or Dynamic IP	IPv6
Internet Access Mode Connection Type: DHCPv6 Client		
DHCPv6 Client Configuration IAID (Identity Association ID): <input type="text" value="44194851"/>		
WAN Connection Detection Mode: Ping Detect Ping IP/Hostname: <input type="text"/> TTL(1-255,0:Auto): <input type="text" value="0"/>		
Bridge Mode <input type="checkbox"/> Enable Bridge Mode Bridge Subnet: LAN 1		

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.
WAN Connection Detection	<p>Such function allows you to verify whether network connection is alive or not through NS Detect or Ping Detect.</p> <p>Mode – Choose Always On, Ping Detect or NS Detect for the system to execute for WAN detection. With NS Detect mode, the system will check if network connection is established or not, like IPv4 ARP Detect. Always On means no detection will be executed. The network connection will be on always.</p> <ul style="list-style-type: none"> ● Ping IP/Hostname – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. ● TTL (Time to Live) –If you choose Ping Detect as detection mode, you have to type TTL value.
Bridge Mode	<p>Enable Bridge Mode - If the function is enabled, the router will work as a bridge modem.</p> <p>Bridge Subnet – Make a bridge between the selected LAN subnet and such WAN interface.</p>

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

Details Page for IPv6 – Static IPv6 in WAN1/WAN2

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

WAN >> Internet Access



WAN 1

PPPoE / PPPoA	MPoA / Static or Dynamic IP	IPv6			
Internet Access Mode Connection Type: Static IPv6					
Static IPv6 Address Configuration IPv6 Address: <input type="text"/> / Prefix Length: <input type="text"/> <input type="button" value="Add"/> <input type="button" value="Delete"/>					
Current IPv6 Address Table <table border="1"><thead><tr><th>Index</th><th>IPv6 Address/Prefix Length</th><th>Scope</th></tr></thead><tbody></tbody></table>			Index	IPv6 Address/Prefix Length	Scope
Index	IPv6 Address/Prefix Length	Scope			
Static IPv6 Gateway configuration IPv6 Gateway Address: <input type="text"/>					
WAN Connection Detection Mode: Always On					
Bridge Mode <input checked="" type="checkbox"/> Enable Bridge Mode Bridge Subnet: LAN 1					

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.

WAN Connection Detection	<p>Such function allows you to verify whether network connection is alive or not through Ping Detect.</p> <p>Mode – Choose Always On or Ping Detect or NS Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always.</p> <ul style="list-style-type: none"> ● Ping IP/Hostname – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. ● TTL (Time to Live) –If you choose Ping Detect as detection mode, you have to type TTL value.
Bridge Mode	<p>Enable Bridge Mode - If the function is enabled, the router will work as a bridge modem.</p> <p>Bridge Subnet – Make a bridge between the selected LAN subnet and such WAN interface.</p>

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

Details Page for IPv6 – 6in4 Static Tunnel in WAN1/WAN2

This type allows you to setup 6in4 Static Tunnel for WAN interface.

Such mode allows the router to access IPv6 network through IPv4 network.

However, 6in4 offers a prefix outside of 2002::0/16. So, you can use a fixed endpoint rather than any cast endpoint. The mode has more reliability.

WAN >> Internet Access



WAN 1

PPPoE / PPPoA	MPoA / Static or Dynamic IP	IPv6
Internet Access Mode		
Connection Type		6in4 Static Tunnel
6in4 Static Tunnel		
Remote Endpoint IPv4 Address		
6in4 IPv6 Address		/ 64 (default:64)
LAN Routed Prefix		/ 64 (default:64)
Tunnel TTL		255 (default:255)
WAN Connection Detection		
Mode		Ping Detect
Ping IP/Hostname		
TTL(1-255,0:Auto)		0

OK Cancel

Available settings are explained as follows:

Item	Description
Remote Endpoint IPv4 Address	Type the static IPv4 address for the remote server.
6in4 IPv6 Address	Type the static IPv6 address for IPv4 tunnel with the value for prefix length.
LAN Routed Prefix	Type the static IPv6 address for LAN routing with the value for prefix length.
Tunnel TTL	Type the number for the data lifetime in tunnel.
WAN Connection Detection	<p>Such function allows you to verify whether network connection is alive or not through Ping Detect.</p> <p>Mode – Choose Always On or Ping Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always.</p> <ul style="list-style-type: none">● Ping IP/Hostname – If you choose Ping Detect as detection mode, you have to type IP address in this field for ping.● TTL (Time to Live) –If you choose Ping Detect as detection mode, you have to type TTL value.

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

Below shows an example for successful IPv6 connection based on 6in4 Static Tunnel mode.

Online Status

Physical Connection		System Uptime: 0day 0:4:16	
IPv4		IPv6	
LAN Status			
IP Address			
2001:4DD0:FF00:83E4:21D:AAFF:FE83:11B4/64 (Global)			
FE80::21D:AAFF:FE83:11B4/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
14	80	1244	6815
WAN1 IPv6 Status			
Enable	Mode	Up Time	
Yes	6in4 Static Tunnel	0:04:07	
IP			Gateway IP
2001:4DD0:FF10:83E4::2131/64 (Global)			---
FE80::C0A8:651D/128 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
3	26	211	2302

Details Page for IPv6 – 6rd in WAN1/WAN2

This type allows you to setup 6rd for WAN interface.

WAN >> Internet Access



WAN 1

PPPoE / PPPoA	MPoA / Static or Dynamic IP	IPv6
Internet Access Mode Connection Type: 6rd		
6rd Settings 6rd Mode: <input checked="" type="radio"/> Auto 6rd <input type="radio"/> Static 6rd Note : Please setup IPv4 WAN as "DHCP" for Auto 6rd connection.		
WAN Connection Detection Mode: Ping Detect Ping IP/Hostname: <input type="text"/> TTL(1-255,0:Auto): 0		
<div>OK Cancel</div>		

Available settings are explained as follows:

Item	Description
6rd Mode	Auto 6rd – Retrieve 6rd prefix automatically from 6rd service provider. The IPv4 WAN must be set as "DHCP". Static 6rd - Set 6rd options manually.
IPv4 Border Relay	Type the IPv4 addresses of the 6rd Border Relay for a given 6rd domain.
IPv4 Mask Length	Type a number of high-order bits that are identical across all CE IPv4 addresses within a given 6rd domain. It may be any value between 0 and 32.

6rd Prefix	Type the 6rd IPv6 address.
6rd Prefix Length	Type the IPv6 prefix length for the 6rd IPv6 prefix in number of bits.
WAN Connection Detection	<p>Such function allows you to verify whether network connection is alive or not through Ping Detect.</p> <p>Mode – Choose Always On or Ping Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always.</p> <ul style="list-style-type: none"> ● Ping IP/Hostname – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. ● TTL (Time to Live) –If you choose Ping Detect as detection mode, you have to type TTL value.

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

Below shows an example for successful IPv6 connection based on 6rd mode.

Online Status

Physical Connection

System Uptime: 0day 0:9:15

IPv4		IPv6	
LAN Status			
IP Address			
2001:E41:A865:1D00:21D:AAFF:FE83:11B4/64 (Global)			
FE80::21D:AAFF:FE83:11B4/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
15	113	1354	18040
WAN1 IPv6 Status			
Enable	Mode	Up Time	
Yes	6rd	0:09:06	
IP		Gateway IP	
2001:E41:A865:1D01:21D:AAFF:FE83:11B5/128 (Global)		---	
FE80::C0A8:651D/128 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
13	29	967	2620

3.1.4 Multi-PVC/VLAN

This router allows you to create multi-PVC for different data transferring for using. Simply go to **Internet Access** and select **Multi-PVC** page.

General

The system allows you to set up to eight channels which are ready for choosing as the first PVC line that will be used as multi-PVC.

Note: Channel 3 and channel 4 are reserved for USB WAN3 and WAN4. However, USB WAN does not support Multi-PVC, nothing will be displayed for Channel 3 and 4.

WAN >> Multi-PVC/VLAN

Multi-PVC/VLAN

General		Advanced				
Channel	Enable	WAN Type	VPI/VCI	VLAN Tag	Port-based Bridge	
1	Yes	ADSL	0/33	None		
2	Yes	Ethernet(WAN2)		None		
5. WAN5	No	ADSL	1/45	None	<input type="checkbox"/> Enable	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
6. WAN6	No	ADSL	1/46	None	<input type="checkbox"/> Enable	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
7. WAN7	No	ADSL	1/47	None	<input type="checkbox"/> Enable	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
8.	No	ADSL	1/48	None	<input type="checkbox"/> Enable	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4

OK Cancel

Available settings are explained as follows:

Item	Description
Channel	Display the number of each channel. Channels 1 and 2 are used by the Internet Access web user interface and can not be configured here. Channels 5 ~ 8 are configurable.
Enable	Display whether the settings in this channel are enabled (Yes) or not (No).
WAN Type	Displays the physical medium that the channel will use.
VPI/VCI	Display the value for VPI and VCI.
VLAN Tag	Displays the VLAN tag value that will be used for the packets traveling on this channel.
Port-based Bridge	The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value. Enable - Check this box to enable the port-based bridge function on this channel. P1 ~ P4 – Check the box(es) to build bridge connection on LAN.

WAN link for **Channel 5, 6 and 7** are provided for router-borne application such as **TR-069**. The settings must be applied and obtained from your ISP. For your special request, please contact with your ISP and then click WAN link of Channel 5, 6 or 7 to configure your router.

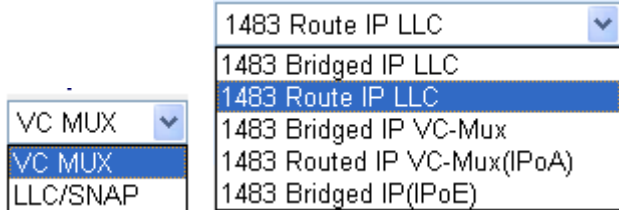

WAN >> Multi-PVC/VLAN >> Channel 5

Multi-PVC/VLAN Channel 5: <input type="radio"/> Enable <input checked="" type="radio"/> Disable	
WAN Type : <input type="text" value="ADSL"/>	
General Settings VPI <input type="text" value="1"/> VCI <input type="text" value="45"/> Protocol <input type="text" value="PPPoA"/> Encapsulation <input type="text" value="VC MUX"/> <input type="checkbox"/> Add VLAN Header VLAN Tag <input type="text" value="0"/> Priority <input type="text" value="0"/>	ATM QoS QoS Type <input type="text" value="UBR"/> PCR <input type="text" value="0"/> SCR <input type="text" value="0"/> MBS <input type="text" value="0"/>
<input type="checkbox"/> Open Port-based Bridge Connection for this Channel Physical Members <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4	
<input type="checkbox"/> Open WAN Interface for this Channel WAN Application: <input type="text" value="Management"/> WAN Connection Detection Mode <input type="text" value="ARP Detect"/> Ping IP <input type="text"/>	
PPPoE/PPPoA Client ISP Access Setup ISP Name <input type="text"/> Username <input type="text"/> Password <input type="text"/> PPP Authentication <input type="text" value="PAP or CHAP"/> <input checked="" type="checkbox"/> Always On Idle Timeout <input type="text" value="-1"/> second(s)	MPoA (RFC1483/2684) <input type="radio"/> Obtain an IP address automatically Router Name <input type="text" value="Vigor"/> * Domain Name <input type="text"/> * *: Required for some ISPs <input checked="" type="radio"/> Specify an IP address IP Address <input type="text"/> Subnet Mask <input type="text"/> Gateway IP Address <input type="text"/> DNS Server IP Address Primary IP Address <input type="text" value="8.8.8.8"/> Secondary IP Address <input type="text" value="8.8.4.4"/>
IP Address From ISP Fixed IP <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address <input type="text"/>	

OK

Cancel

Available settings are explained as follows:

Item	Description
Multi-VLAN Channel 5/6/7	<p>Enable – Click it to enable the configuration of this channel.</p> <p>Disable – Click it to disable the configuration of this channel.</p>
WAN Type	<p>The connections and interfaces created in every channel may select a specific WAN type to be built upon. In the Multi-PVCs application, only the Ethernet WAN type is available. The user will be able to select the physical WAN interface the channel shall use here.</p>
General Settings	<p>VPI - Type in the value provided by your ISP.</p> <p>VCI - Type in the value provided by your ISP.</p> <p>Protocol - Select a proper protocol for this channel.</p> <p>Encapsulation - Choose a proper type for this channel. The types will be different according to the protocol setting that you choose.</p>  <p>Add VLAN Header – Check the box to enable the following two options.</p> <p>VLAN Tag – Type the value as the VLAN ID number. Valid settings are in the range from 1 to 4095. The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value.</p> <p>Priority – Choose the number to determine the packet priority for such VLAN. The range is from 0 to 7.</p>
ATM OoS	<p>QoS Type - Select a proper QoS type for the channel.</p>  <p>Type the values for PCR, SCR and MBS respectively.</p>
Open Port-based Bridge Connection for this Channel	<p>The settings here will create a bridge between the LAN ports selected and the WAN. The WAN interface of the bridge connection will be built upon the WAN type selected using the VLAN tag configured.</p> <p>Physical Members – Group the physical ports by checking the corresponding check box(es) for applying the port-based bridge connection.</p>

Open WAN Interface for this Channel	<p>Check the box to enable relating function.</p> <p>WAN Application –</p> <p>Management – It can be specified for general management (Web configuration/telnet/TR069). If you choose Management, the configuration for this VLAN will be effective for Web configuration/telnet/TR069.</p> <p>IPTV - The IPTV configuration will allow the WAN interface to send IGMP packets to IPTV servers.</p>
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>
PPPoE/PPPoA Client	<p>Enter your allocated username, password and authentication parameters according to the information provided by your ISP.</p> <p>ISP Name – Type in the name of your ISP.</p> <p>Username – Type in the username provided by ISP in this field. The maximum length of the name you can set is 80 characters.</p> <p>Password – Type in the password provided by ISP in this field. The maximum length of the password you can set is 48 characters.</p> <p>PPP Authentication – Select PAP only or PAP or CHAP for PPP.</p> <p>Always On – Check it to keep the network connection always.</p> <p>Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action.</p> <p>Fixed IP – Click Yes to use this function and type in a fixed IP address in the box of Fixed IP Address.</p>
MPoA (RFC1483/2684)	<p>Obtain an IP address automatically – Click this button to obtain the IP address automatically.</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>Specify an IP address – Click this radio button to specify some data.</p> <ul style="list-style-type: none"> ● IP Address – Type in the private IP address. ● Subnet Mask – Type in the subnet mask. ● Gateway IP Address – Type in 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</p>

	necessary, type in secondary IP address for necessity in the future.
--	--

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

Advanced

Such configuration is applied to upstream packets. Such information will be provided by ISP. Please contact with your ISP for detailed information.

WAN >> Multi-PVC/VLAN

Multi-PVC/VLAN

General Advanced

ATM QoS					
Channel	QoS Type	PCR	SCR	MBS	PVC to PVC Binding
1.	UBR	0	0	0	Disable
2.	UBR	0	0	0	Disable
5.	UBR	0	0	0	Disable
6.	UBR	0	0	0	Disable
7.	UBR	0	0	0	Disable
8.	UBR	0	0	0	Disable

Note:

1. If the parameters in the ATM QoS settings are set to zero, then their default settings will be used. Also, PCR(max)=ADSL Up Speed /53/8.
2. Multiple channels may use the same ADSL channel link through the PVC Binding configuration. The PVC Binding configuration is only supported for channels using ADSL, please make sure the channel that you are binding to is using ADSL as its WAN type. The binding will work only under PPPoE and MPoA 1483 Bridge mode.

OK Cancel

Available settings are explained as follows:

Item	Description
QoS Type	Select a proper QoS type for the channel according to the information that your ISP provides. <div> <div>UBR</div> <div>UBR</div> <div>CBR</div> <div>ABR</div> <div>rtVBR</div> <div>rtVBR</div> </div>
PCR	It represents Peak Cell Rate. The default setting is "0".
SCR	It represents Sustainable Cell Rate. The value of SCR must be smaller than PCR.
MBS	It represents Maximum Burst Size. The range of the value is 10 to 50.
PVC to PVC Binding	It allows the PVC channel to use the same ADSL connection settings of another PVC channel. Please choose the PVC channel via the drop down list.

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

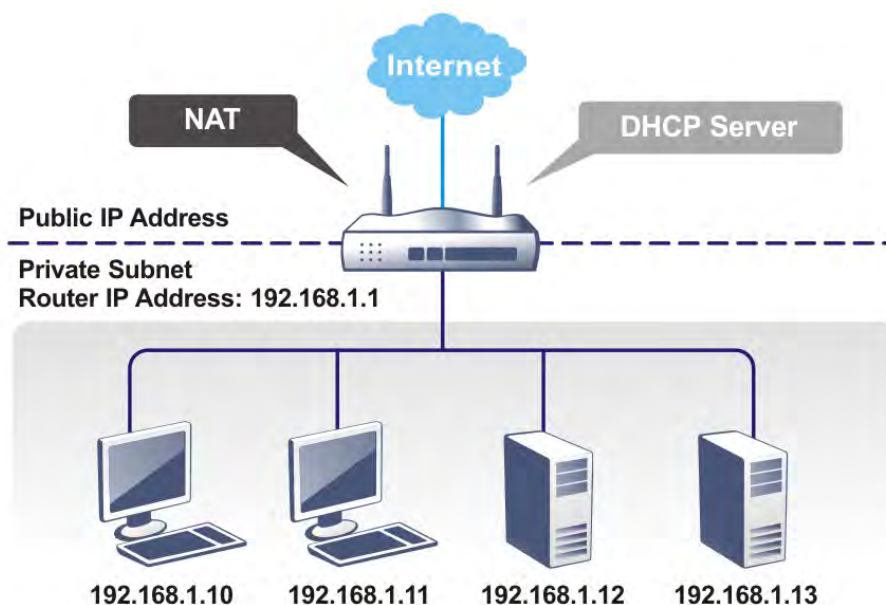
3.2 LAN

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

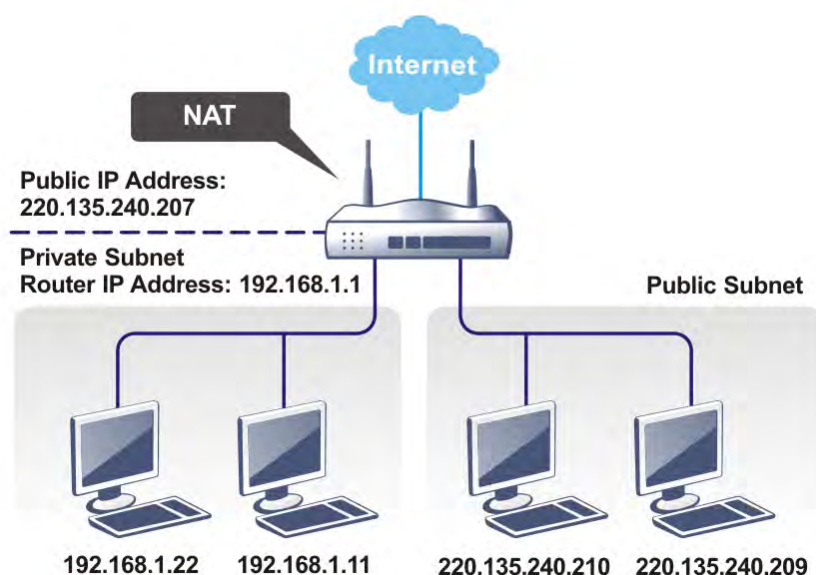


3.2.1 Basics of LAN

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



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



What is Routing Information Protocol (RIP)

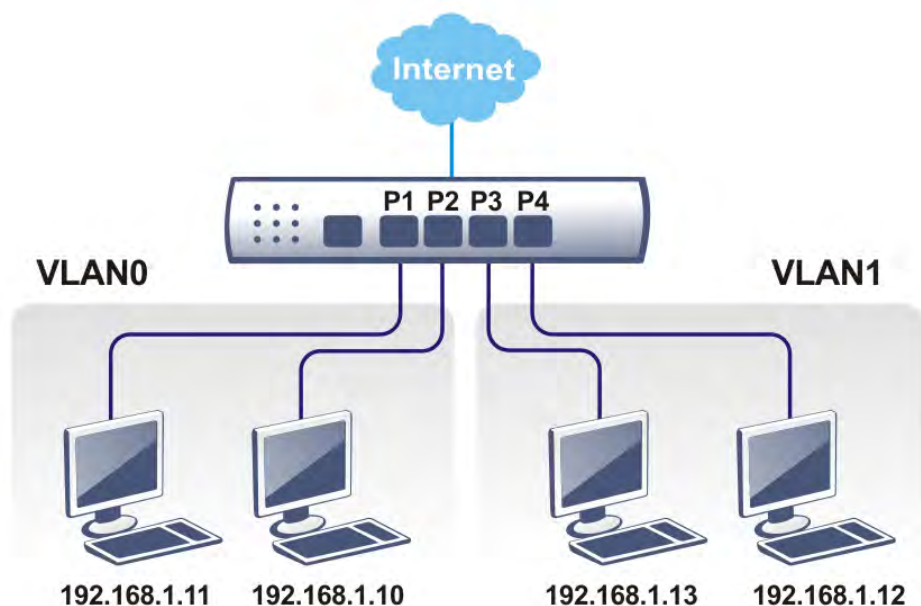
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

What is Static Route

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

What are Virtual LANs and Rate Control

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



3.2.2 General Setup

This page provides you the general settings for LAN. Click **LAN** to open the LAN settings page and choose **General Setup**.

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

LAN >> General Setup

General Setup

Index	Status	DHCP	IP Address		
LAN 1	V	V	192.168.1.1	Details Page	IPv6
LAN 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.2.1	Details Page	IPv6
LAN 3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.3.1	Details Page	IPv6
LAN 4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.4.1	Details Page	IPv6
IP Routed Subnet	<input type="checkbox"/>	<input type="checkbox"/>	192.168.0.1	Details Page	

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

☐ Force router to use "DNS server IP address" settings specified in LAN1

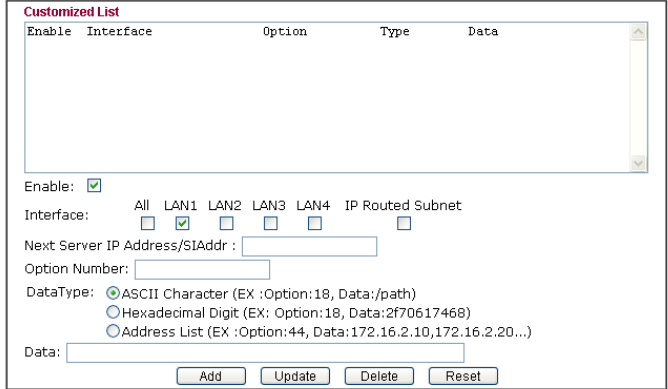
Inter-LAN Routing

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

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

[OK](#)

Available settings are 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.</p> <p>Status - Basically, LAN1 status is enabled in default. LAN2, LAN3, LAN3 and IP Routed Subnet can be observed by checking the box of Status.</p> <p>DHCP - 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 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	<p>When the router receives the DHCP request from LAN client, the router will assign an IP with the DHCP packets adding option number and data information.</p> <p>LAN >> General Setup</p>  <p>Note:</p> <ol style="list-style-type: none"> 1. Configuring options 44, 46 or 66 here will overwrite the settings by telnet command "msubnet". 2. Configuring option 3 here will overwrite the setting in "LAN >> General Setup" Details Page's "Gateway IP Address" field. 3. Configuring option 15 here will overwrite the setting in "WAN >> Internet Access >> Static or Dynamic IP Address" field. <p>Enable – Check the box to enable the function of DHCP Option. Each DHCP option is composed by an option number with data. For example,</p> <p>Option number:100</p> <p>Data: abcd</p> <p>When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets.</p> <p>Option Number – Type a number for such function.</p> <p>Data Type – Choose the type (ASCII, Hex or IP address) for the data to be stored.</p> <p>Data – Type the content of the data to be processed by the function of DHCP option.</p>
Force router to use “DNS server IP address” settings as specified in ...	<p>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).</p>

Inter-LAN Routing	Check the box to link two or more different subnets (LAN and LAN).
--------------------------	--

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

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

Details Page for LAN1

LAN1 is the default configuration for basic host connection.

[LAN >> General Setup](#)

LAN 1 Ethernet TCP / IP and DHCP Setup	LAN 1 IPv6 Setup
Network Configuration For NAT Usage IP Address <input type="text" value="192.168.1.1"/> Subnet Mask <input type="text" value="255.255.255.0"/> RIP Protocol Control <input type="button" value="Disable"/>	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="192.168.1.10"/> IP Pool Counts <input type="text" value="200"/> Gateway IP Address <input type="text" value="192.168.1.1"/> Lease Time <input type="text" value="86400"/> (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>For NAT 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> <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 – 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 dispatches 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

	<p>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>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>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 Configuration	<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> <div><div>System Status</div><div>System Uptime: 71:47:46</div><table><tr><td>LAN Status</td><td colspan="2">Primary DNS: 194.109.6.66</td><td>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></div> <p>If both the Primary IP and Secondary IP Address fields are left empty, the router will use the DNS server assigned by</p>	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	
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											

	<p>ISP. If not, the router will assign its own IP address to local users as a DNS proxy server.</p> <p>Force router to use address for DNS- Force Vigor router to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).</p>
--	--

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

Details Page for LAN1 – IPv6 Setup

There are two configuration pages for LAN1, Ethernet TCP/IP and DHCP Setup (based on IPv4) and IPv6 Setup. Click the tab for each type and refer to the following explanations for detailed information. Below shows the settings page for IPv6.

LAN >> General Setup

LAN 1 Ethernet TCP / IP and DHCP Setup

LAN 1 IPv6 Setup

☒ Enable IPv6

WAN Primary Interface WAN1

Static IPv6 Address

IPv6 Address

Prefix Length

Add

Delete

Unique Local Address(ULA) configuration

Off

/ 64

Current IPv6 Address Table

Index	IPv6 Address/Prefix Length	Scope
1	FE80::21D:AAFF:FE00:0/64	Link

DNS Server IPv6 Address

Primary DNS Server

2001:4860:4860::8888

Secondary DNS Server

2001:4860:4860::8844

Management

SLAAC(stateless)

Other Option(O-bit)

DHCPv6 Server

☒ Enable Server
 ☐ Disable Server

☒ Auto IPv6 range

Start IPv6 Address

End IPv6 Address

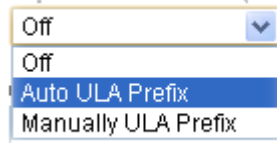
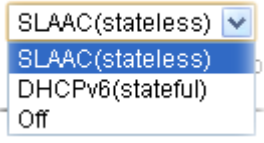
Advance setting

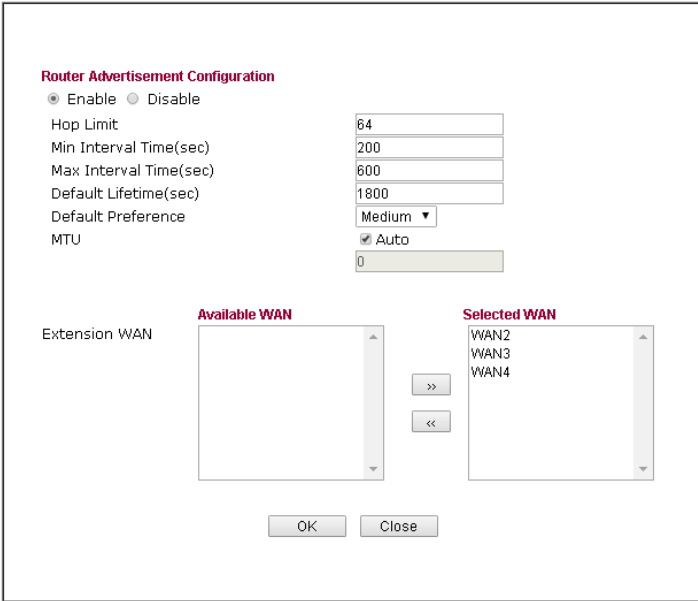
Edit

OK

It provides 2 daemons for LAN side IPv6 address configuration. One is **SLAAC**(stateless) and the other is **DHCPv6 Server** (Stateful).

Available settings are explained as follows:

Item	Description
Enable IPv6	Check the box to enable the configuration of LAN 1 IPv6 Setup.
WAN Primary Interface	Use the drop down list to specify a WAN interface for IPv6.
Static IPv6 Address	<p>IPv6 Address –Type static IPv6 address for LAN.</p> <p>Prefix Length – Type the fixed value for prefix length.</p> <p>Add – Click it to add a new entry.</p> <p>Delete – Click it to remove an existed entry.</p>
Unique Local Address (ULA) configuration	<p>Such feature is used for the host without assigned IPv6 address to obtain IPv6 address automatically or have an IPv6 address specified manually via ULA configuration. It is convenient for communication among different subnets.</p>  <p>Auto ULA Prefix – The system will generate the required IPv6 address.</p> <p>Manually ULA Prefix – A user can type the ULA IPv6 address manually.</p>
DNS Server IPv6 Address	<p>Primary DNS Server – Type the IPv6 address for Primary DNS server.</p> <p>Secondary DNS Server –Type another IPv6 address for DNS server if required.</p>
Management	<p>Host under LAN can be assigned IP address from Vigor router via the following method.</p>  <ul style="list-style-type: none"> ● SLAAC(stateless) – The IP address (with Prefix) of the host shall be formed according to RA transmitted by Vigor router. ● DHCPv6(stateful) - The IP address of the host shall be assigned after communicating with DHCPv6 server for answering the request of client. ● Off – No IP address is assigned. <p>Other Option (O-bit) – Check this box to enable the O-bit for obtaining additional information (e.g., DNS) from DHCPv6.</p>
DHCPv6 Server	<p>Enable Server –Click it to enable DHCPv6 server. DHCPv6 Server could assign IPv6 address to PC according to the Start/End IPv6 address configuration.</p> <p>Disable Server –Click it to disable DHCPv6 server.</p>

	<p>Start IPv6 Address / End IPv6 Address –Type the start and end address for IPv6 server.</p>
Advance setting	<p>More options are offered under the Advance setting. Click Edit to open the pop-up window.</p>  <p>Router Advertisement Configuration – Click Enable to enable router advertisement server. The router advertisement daemon sends Router Advertisement messages, specified by RFC 2461, to a local Ethernet LAN periodically and when requested by a node sending a Router Solicitation message. These messages are required for IPv6 stateless auto-configuration.</p> <p>Disable – Click it to disable router advertisement server.</p> <p>Hop Limit – The value is required for the device behind the router when IPv6 is in use.</p> <p>Min/Max Interval Time (sec) – It defines the interval (between minimum time and maximum time) for sending RA (Router Advertisement) packets.</p> <p>Default Lifetime (sec) –Within such period of time, Vigor2832 can be treated as the default gateway.</p> <p>Default Preference – It determines the priority of the host behind the router when RA (Router Advertisement) packets are transmitted.</p> <p>MTU – It means Max Transmit Unit for packet. If Auto is selected, the router will determine the MTU value for LAN.</p> <p>Extension WAN – Not only the IP address can be obtained from the primary WAN, but also the prefix for IPv6 LAN IP address can be assigned by extension WAN specified here.</p>

Details Page for LAN2/LAN3/LAN4

LAN >> General Setup

Lan 2 Ethernet TCP / IP and DHCP Setup

Network Configuration	DHCP Server Configuration
<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input checked="" type="radio"/> Enable Server <input type="radio"/> Disable Server
<input checked="" type="radio"/> For NAT Usage <input type="radio"/> For Routing Usage	<input type="checkbox"/> Enable Relay Agent
IP Address <input type="text" value="192.168.2.1"/>	Start IP Address <input type="text" value="192.168.2.10"/>
Subnet Mask <input type="text" value="255.255.255.0"/>	IP Pool Counts <input type="text" value="100"/>
	Gateway IP Address <input type="text" value="192.168.2.1"/>
	Lease Time <input type="text" value="259200"/> (s)
	<input checked="" type="checkbox"/> Retrieve IPs from 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>Enable/Disable - Click Enable to enable such configuration. Click Disable to disable such configuration.</p> <p>For NAT Usage - Click this radio button to invoke NAT function.</p> <p>For Routing Usage - Click this radio button to invoke this function.</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</p>

	<p>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>Lease Time – Enter the time to determine how long the IP address assigned by DHCP server can be used.</p> <p>Retrieve IPs from 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 Configuration	<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> <div><div>System Status</div><div>System Uptime: 71:47:46</div><table><tr><td>LAN Status</td><td colspan="2">Primary DNS: 194.109.6.66</td><td>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></div> <p>If both the Primary IP and Secondary IP Address fields are left empty, the router will use the DNS server assigned by ISP. If not, the router will assign its own IP address to local users as a DNS proxy server.</p> <p>Force router to use address for DNS- Force Vigor router to use DNS servers in this page instead of DNS servers</p>	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	
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											

	given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).
--	---

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

LAN >> General Setup

Available settings are explained as follows:

DrayTek

the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.

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

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

Use LAN Port – Specify an IP for IP Route Subnet. If it is enabled, DHCP server will assign IP address automatically for the clients coming from P1 and/or P2. Please check the box of P1 and P2.

Use MAC Address - Check such box to specify MAC address.

MAC Address: Enter the MAC Address of the host one by one and click **Add** to create a list of hosts to be assigned, deleted or edited IP address from above pool. Set a list of MAC Address for 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.

Add – Type the MAC address in the boxes and click this button to add.

Delete – Click it to delete the selected MAC address.

Edit – Click it to edit the selected MAC address.

Cancel – Click it to cancel the job of adding, deleting and editing.

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

3.2.3 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

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.
Viewing Routing Table	Displays the routing table for your reference. Diagnostics >> View Routing Table <div> <div>Current Running Routing Table Refresh </div> <div> Key: C - connected, S - static, R - RIP, * - default, ~ - private * 0.0.0.0/ 0.0.0.0 via 172.16.3.1, WAN1 C~ 192.168.1.0/ 255.255.255.0 is directly connected, LAN C 172.16.3.0/ 255.255.255.0 is directly connected, WAN1 </div> </div>
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.

Static Route for IPv6

You can set up to 40 profiles for IPv6 static route.

[LAN >> Static Route Setup](#)

IPv4			IPv6			Set to Factory Default View IPv6 Routing Table	
Index	Destination Address	Status	Index	Destination Address	Status		
1.	::/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
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.
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.

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

LAN ▾

OK

Cancel

Delete

Available settings are explained as follows:

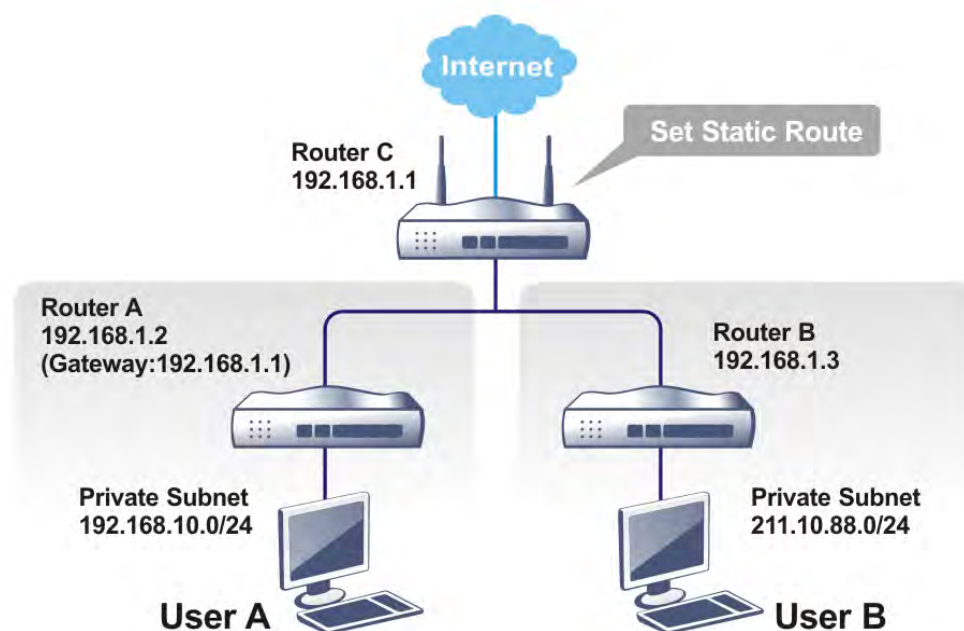
Item	Description
Enable	Click it to enable this profile.
Destination IPv6 Address / Prefix Len	Type the IP address with the prefix length for this entry.
Gateway IPv6 Address	Type the gateway address for this entry.
Network Interface	Use the drop down list to specify an interface for this static route. <div> <div>LAN ▾</div> <div> LAN WAN1 WAN2 WAN3 </div> </div>

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

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

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

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



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

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

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

LAN >> Static Route Setup

Index No. 1

<input checked="" type="checkbox"/> Enable	
Destination IP Address	192.168.10.0
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.2
Network Interface	LAN1

Note: WAN5, WAN6, WAN7 are router-borne WANs.

OK Cancel Delete

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

LAN >> Static Route Setup

Index No. 2

<input checked="" type="checkbox"/> Enable	
Destination IP Address	<input type="text" value="211.100.88.0"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway IP Address	<input type="text" value="192.168.1.3"/>
Network Interface	<input type="text" value="LAN1"/>

Note: WAN5, WAN6, WAN7 are router-borne WANs.

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

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	WAN2
S~ 192.168.10.0/ 255.255.255.0	via 192.168.1.2	LAN1
C~ 192.168.1.0/ 255.255.255.0	directly connected	LAN1
C 172.16.0.0/ 255.255.0.0	directly connected	WAN2
S~ 211.100.88.0/ 255.255.255.0	via 192.168.1.3	LAN1

Note: WAN5, WAN6, WAN7 are router-borne WANs.

3.2.4 VLAN (Multi-Subnet)

Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. Go to **LAN** page and select **VLAN**. The following page will appear. Click **Enable** to invoke VLAN function. The multi-subnet can let a small businesses have much better isolation for multi-occupancy applications.

Tagged VLAN

The tagged VLANs (802.1q) can also mark data with a VLAN identifier. This identifier can be carried through an onward Ethernet switch to specific ports. The specific VLAN clients can also pick up this identifier as it passes to the LAN. Users can set the priorities for LAN-side QoS and can assign each of the VLANs to each of the different IP subnets that the router may also be operating in order to provide even more isolation. This functionality is **tag-based multi-subnet**.

Port-Based VLAN

Relative to tag-based VLAN which groups clients with an identifier, port-based VLAN uses physical ports to separate the clients into different VLAN group.

LAN >> VLAN Configuration

VLAN Configuration

<input checked="" type="checkbox"/> Enable											
LAN				Wireless LAN				VLAN Tag			
P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0

☒ Permit untagged device in P1 to access router

1. Tag based VLAN only applied for LAN Ports;

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

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

OK

Clear

Cancel

Note: Such page will be different slightly in accordance with the type of the router you have and settings in this page only applied to LAN port but not WAN port.

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable such function.
LAN	P1 – P4 – Check the LAN port(s) to be grouped under the selected VLAN.
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.
VLAN Tag	<p>Enable – Check it 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>
Permit untagged device in P1 to access router	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.

Note: Leave one VLAN untagged at least to prevent from not connecting to Vigor router due to unexpected error.

Vigor2830 series features a hugely flexible VLAN system. In its simplest form, each of the Gigabit LAN ports can be isolated from each other, for example to feed different companies or departments but keeping their local traffic completely separated.

Configuring port-based VLAN for wireless and non-wireless clients

1. All the wire network clients are categorized to group VLAN0 in subnet 192.168.1.0/24 (LAN1).
2. All the wireless network clients are categorized to group VLAN1 in subnet 192.168.2.0/24 (LAN2).
3. Open **LAN>>VLAN Configuration**. Check the boxes according to the statement in step 1 and Step 2.

LAN >> VLAN Configuration

VLAN Configuration

☒ Enable

	LAN				Wireless LAN				Subnet	VLAN Tag		
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4		Enable	VID	Priority
VLAN0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LAN 2	<input type="checkbox"/>	0	0
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 3	<input type="checkbox"/>	0	0
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0

☒ Permit untagged device in P1 to access router

1. For each VLAN row, if enable is checked for the VLAN Tag then the corresponding VID will be applied to wired LAN traffic.
2. Wireless LAN traffic is always untagged, but will still be a member of the VLAN group selected.
3. Each VID must be unique.

OK Clear Cancel

4. Click **OK**.
5. Open **LAN>>General Setup**. If you want to let the clients in both groups communicate with each other, simply activate **Inter-LAN Routing** by checking the box between **LAN1** and **LAN2**.

LAN >> General Setup

General Setup

Index	Status	DHCP	IP Address		
LAN 1	V	V	192.168.1.1	Details Page	<input checked="" type="checkbox"/> 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	
IP Routed Subnet	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.0.1	Details Page	

☐ Advanced You can configure DHCP server 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
LAN 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN 4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

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

OK

Vigor router supports up to six private IP subnets on LAN. Each can be independent (isolated) or common (able to communicate with each other). This is ideal for departmental or multi-occupancy applications.

Note: As for the VLAN applications, refer to "Appendix I: VLAN Application on Vigor Router" for more detailed information.

3.2.5 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 | [Select All](#) | [Sort](#) | [Refresh](#)

IP Address	Mac Address
192.168.1.11	E0-CB-4E-DA-48-79

IP Bind List (Limit: 300 entries) | [Select All](#) | [Sort](#)

Index	IP Address	Mac Address
-------	------------	-------------

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.

Backup IP Bind List : <input type="button" value="Backup"/>	Upload From File: <input type="button" value="Choose File"/> <input type="button" value="Restore"/>
--	--

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 and Update	<p>IP Address – Type the IP address that will be used for the specified MAC address.</p> <p>Mac Address – Type the MAC address that is used to bind with the assigned IP address.</p> <p>Comment – Type a brief description for the entry.</p> <p>Show Comment – Check it to display the content of the comment.</p>
IP Bind List	It displays a list for the IP bind to MAC information.
Add	It allows you to add the one you choose from the ARP table or the IP/MAC address typed in Add and Edit to the table of IP Bind List .
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 .
Backup	Store the configuration for Bind IP to MAC as a file.
Restore	Restore the previously stored configuration file and apply to such page.

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.

3.2.6 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. Next, it is more convenient and easy to configure in user's interface. Last, connect a PC with Smart Monitor installed to the mirror port of this router to capture monitored information.

LAN >> LAN Port Mirror

LAN Port Mirror

Port Mirror:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable					
	Port1	Port2	Port3	Port4	WAN1	WAN2
Mirror Port		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
Mirrored Tx Port	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mirrored Rx Port	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Note: The mirrored WAN1 is a software mirror, it will lead to a substantial decline in performance.

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.
Mirrored Tx Port	Select which ports are necessary to be mirrored for transmitting the packets.
Mirrored Rx Port	Select which ports are necessary to be mirrored for receiving the packets.

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

3.2.7 Wired 802.1x

IEEE 802.1x is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism for the device that is attached to a LAN or WLAN.

Wired 802.1x provides authentication for one network device on each LAN port. The RADIUS Server settings must be configured before enabling 802.1x because the EAP (Extensible Authentication Protocol) Authenticator relies on the RADIUS Server in its authentication process. Each LAN port with Wired 802.1x configured will only forward 802.1x packets and block all other packets until the authentication has successfully completed.

LAN >> Wired 802.1X

Wired 802.1X

LAN 802.1X:
<input checked="" type="checkbox"/> Enable
802.1X ports:
<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4

Note:

802.1X enabled LAN ports only support a single attached device using EAPOL authentication. To authenticate multiple devices through a LAN port you need an 802.1X-capable switch. Then configure 802.1X on the attached switch instead.

OK

Available settings are explained as follows:

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

Enable	Check the box to enable LAN 802.1x function.
802.1x ports	After enabling the function, simply specify the LAN port(s) to apply such function.

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

3.2.8 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:

Enable	Profile	Status	Interface	
<input type="checkbox"/>	1.	URL Redirect	None	Preview
<input type="checkbox"/>	2.	URL Redirect	None	Preview
<input type="checkbox"/>	3.	URL Redirect	None	Preview
<input type="checkbox"/>	4.	URL Redirect	None	Preview

Note: The router must connect to the Internet before webpage redirection will work.

[OK](#)

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

☐ Enable

Body

URL Redirect

http://www.draytek.com

The requested webpage will be redirected by Web Portal Setup.
Please click Continue to access into the requested webpage.

(Max 4095 characters)

Default Message

Position on screen

☒ Top
 ☐ Bottom

Button

Continue

(Max 39 characters)

☐ User must click button to proceed

☒ Override user management
 ☐ Prefer user management

Subnet

☐ LAN1
 ☐ LAN2
 ☐ LAN3
 ☐ LAN4

WLAN 2.4G

☐ SSID1 (DrayTek)
 ☐ SSID2 (DrayTek_Guest)
 ☐ SSID3
 ☐ SSID4

Priority

Applied Interfaces

Preview

Note: 1. URL Redirect may fail to display some web sites because of their protection for phishing attack. Please click the "Preview" icon to test.
2. HTTPS Redirect will normally generate an untrusted certificate warning to web browsers, the user would need to ignore this warning to successfully display the web portal.

OK Cancel

Available settings are explained as follows:

Item	Description
Disable	Click this button to close this function.
Body	<p>Two types can be specified for web portal setup.</p> <p>URL Redirect - Any user who wants to access into Internet through this router will be redirected to the URL specified here first. It is a useful method for the purpose of advertisement. For example, force the wireless user(s) in hotel to access into the web page that the hotel wants the user(s) to visit.</p> <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.</p> <ul style="list-style-type: none"> Default Message – Click it to restore the default content.
Notice	<p>Content given in this field will be displayed on the screen when a web page is redirected by web portal mechanism.</p> <p>Position on Screen – The content of notice and the defined button can be shown upside (Top) or downside (Bottom) the text defined for message body.</p> <ul style="list-style-type: none"> Button – Define the word (default word is "Continue") shown on the button. User must click button to proceed – Check the box to force the user click the button (with the word defined on Button box) to proceed the operation.

Priority	<p>If User Management (refer to VII-3 User Management) mode and such web portal profile are configured and enabled for filtering users, you have to determine which one shall have the highest priority.</p> <p>Override user management – Web portal profile will be used to filter users first.</p> <p>Prefer user management – User Management profile will be used to filter users first.</p>
Applied Interfaces	<p>Check the box(es) representing different interfaces to be applied by such profile.</p> <p>The advantage is that 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.

3.3 Load-Balance /Route Policy

Route Policy (also well known as PBR, policy-based routing) is a feature where you may need to get a strategy for routing. The packets will be directed to the specified interface if they match one of the policies. You can setup route policies in various reasons such as load balance, security, routing decision, and etc.

Through protocol, IP address, port number and interface configuration, Route Policy can be used to configure any routing rules to fit actual request. In general, Route Policy can easily reach the following purposes:

- **Load Balance**

You may manually create policies to balance the traffic across network interface.

- **Specify Interface**

Through dedicated interface (WAN/LAN/VPN), the data can be sent from the source IP to the destination IP.

- **Address Mapping.**

Allows you specify the outgoing WAN IP address (es) for an internal private IP address or a range of internal private IP addresses.

- **Priority.**

The router will determine which policy will be adopted for transmitting the packet according to the priority of Static Route and Route Policy.

- **Failover to/Failback**

Packets will be sent through another Interface or follow another Policy when the original interface goes down (**Failover to**). Once the original interface resumes service (**Failback**), the packets will be returned to it immediately.

- **Other routing.**

Specify routing policy to determine the direction of the data transmission.

<p>Note: For more detailed information about using policy route, refer to Support >>FAQ/Application Notes on www.draytek.com.</p>

3.3.1 General Setup

Load-Balance/Route Policy



Load-Balance/Route Policy

10 rules per page

[Set to Factory Default](#)

Index	Enable	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 type="checkbox"/>	Any	WAN1	200	Any	Any	Any	Any	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
5	<input type="checkbox"/>	Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
6	<input type="checkbox"/>	Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
7	<input type="checkbox"/>	Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
8	<input type="checkbox"/>	Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
9	<input type="checkbox"/>	Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
10	<input type="checkbox"/>	Any	WAN1	200	Any	Any	Any	Any	Any	Any	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

Available settings are explained as follows:

Item	Description
Index	Click the number of index to access into the configuration web page.
Enable	Check this box to enable this policy.
Protocol	Display the protocol used for this policy.
Interface	Display the interface to send packets to once the policy is matched.
Priority	Display the priority of the selected profile in data transmission.
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	This mode will guide you to configure the common settings with several pages.
Advance Mode	This mode allows you to modify all the settings in one page.

Click **Index 1** to access into the following page for configuring load-balance policy. Here we choose **Advance Mode** as an example.

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

Available settings are explained as follows:

Item	Description
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.

4. 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

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.

5. 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 ~ 192.168.1.66

Interface

WAN1

More options

Force NAT

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

Load-Balance/Route Policy



Load-Balance/Route Policy

10 rules per page | [Set to Factory Default](#)

Index	Enable	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	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 1** to access into the following page.

Load-Balance/Route Policy

Index: 1

☐ Enable

Criteria

Protocol: Any

Source IP:

☒ Any
 ☐ Src IP Range
 ☐ Src IP Subnet

Destination IP:

☒ Any
 ☐ Dest IP Range
 ☐ Dest IP Subnet

Destination Port:

☒ Any
 ☐ Dest Port Start ~ Dest Port End

Send via if Criteria Matched

Interface:

☒ WAN/LAN: WAN1
 ☐ VPN: VPN 1.???

Gateway:

☒ Default Gateway
 ☐ Specific Gateway:

Priority

Priority: 200

Low

250

150

High

0

Default Route

Routes in Routing Table

More Options

Packet Forwarding to WAN via:

☒ Force NAT
 ☐ Force Routing

☐ Failover to:

☒ WAN/LAN: Default WAN
 ☐ VPN: VPN 1.???
 ☐ Route Policy: Index 1

Gateway:

☒ Default Gateway
 ☐ Specific Gateway: 0.0.0.0

Note: Force NAT(Routing): NAT(Routing) will be performed on outgoing packets, regardless of which type of subnet (NAT or IP Routing) they originate from.

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. <div> <div>any</div> <div>any</div> <div>TCP</div> <div>UDP</div> <div>TCP/UDP</div> <div>ICMP</div> </div>

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 destination IP. If this field is blank, it means that all the destination ports will be passed through the WAN interface.</p>
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>
Priority	<p>Packets will be transmitted based on all routes or Route Policy. Vigor router will determine which rule will be adopted for transmitting the packet according to the priority of Static Route and Route Policy.</p> <p>The greater the value is, the lower the priority is. Default value for route policy is “200” which means it has higher priority than the default route.</p>
More options	<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> <p>Failover to – 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> <ul style="list-style-type: none"> ● WAN/LAN – Use the drop down list to choose an interface as an auto failover interface. ● VPN – Use the drop down list to choose a VPN tunnel as a failover tunnel. ● Route Policy – Use the drop down list to choose an existed route policy profile.

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.

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

Load-Balance/Route Policy



Load-Balance/Route Policy

10 rules per page

[Set to Factory Default](#)

Index	Enable	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	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

3.3.2 Diagnose

With the analysis done by such page, possible path (static route, routing table or policy route) of the packets sent out of the router can be traced.

Load-Balance/Route Policy >> Diagnose

Mode

- ☒ analyze how a packet will be sent
- ☐ analyze how multiple packets as specified in the input file will be sent

Packet Information

☒ ICMP
 ☐ UDP
 ☐ TCP
 ☐ ANY

Src IP: 192.168.1.2

Dst IP:

Dst Port:

or

Load-Balance/Route Policy >> Diagnose

Mode

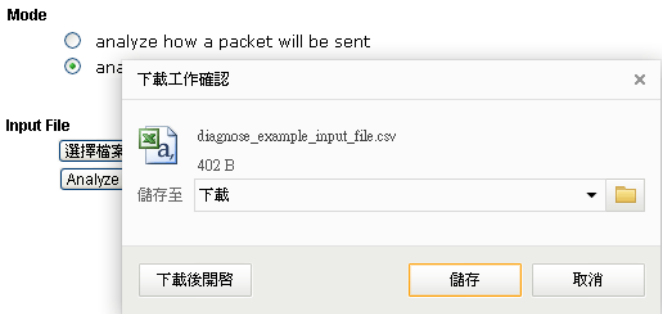
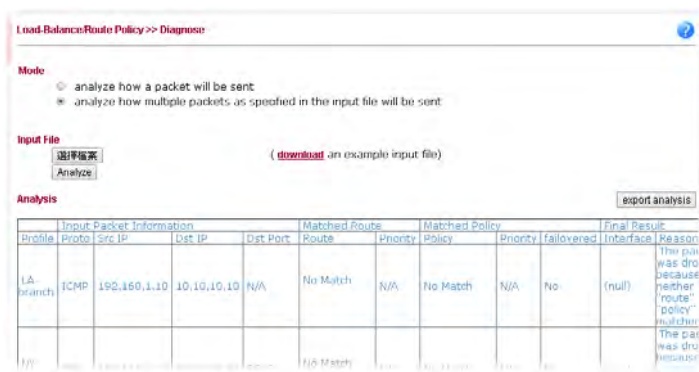
- ☐ analyze how a packet will be sent
- ☒ analyze how multiple packets as specified in the input file will be sent

Input File

未選擇檔案
 [\(download an example input file\)](#)

Available settings are explained as follows:

Item	Description
Mode	Analyze how a packet will be sent – Choose such mode to make Vigor router analyze how a single packet will be sent by a route policy.

	<p>Analyze how multiple packets... - Choose such mode to make Vigor router analyze how multiple packets in a specified file will be sent by a route policy.</p>
Packet Information	<p>Specify the nature of the packets to be analyzed by Vigor router.</p> <p>ICMP/UDP/TCP/ANY- Specify a protocol for diagnosis.</p> <p>Src IP – Type an IP address as the source IP.</p> <p>Dst IP – Type an IP address as the destination IP.</p> <p>Dst Port – Use the drop down list to specify the destination port.</p> <p>Analyze – Click it to perform the job of analyzing. The analyzed result will be shown on the page. If required, click export analysis to export the result as a file.</p>
Input File	<p>Select – Click the download link to get a blank example file. Then, click such button to select that blank “.csv” file for saving the result of analysis.</p>  <p>Analyze – Click it to perform the job of analyzing. The analyzed result will be shown on the page. If required, click export analysis to export the result as a file.</p>  <p>Note that the analysis was based on the current "load-balance/route policy" settings, we do not guarantee it will be 100% the same as the real case.</p>

3.4 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.

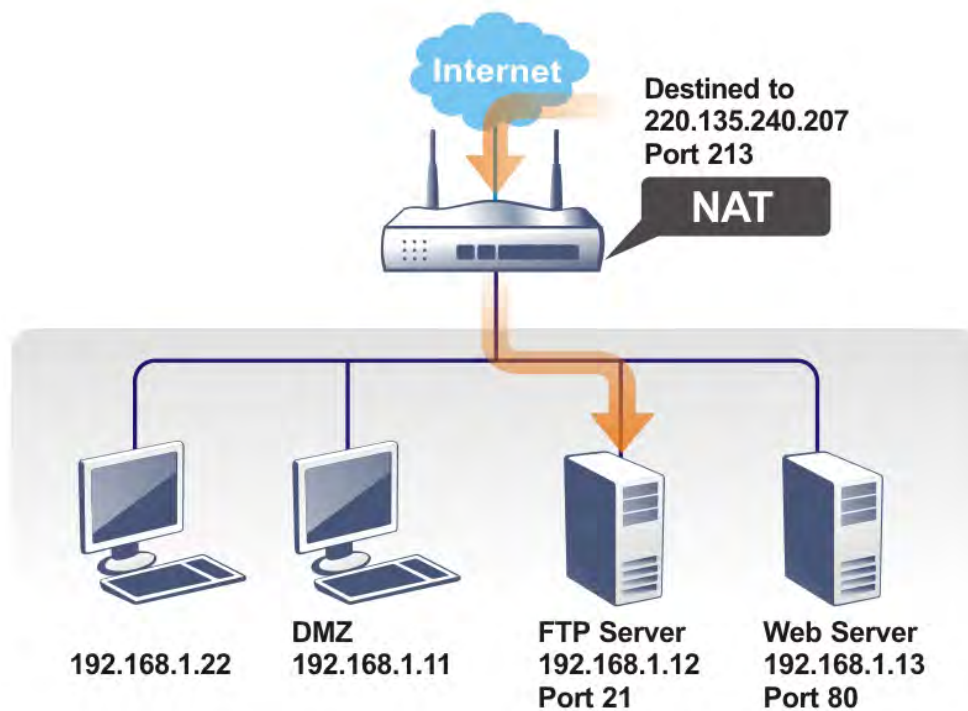
On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by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

Below shows the menu items for NAT.



3.4.1 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 20 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](#) >>

[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

☒ Enable

Mode

Range

Single

Range

Service Name

Protocol

WAN IP

1.All

Public Port

0 -

Private IP

-

Private Port

0

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

OK Clear Cancel

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 IP	Select the WAN IP used for port redirection. There are eight WAN IP alias that can be selected and used for port redirection. The default setting is All which means all the incoming data from any port will be redirected to specified range of IP address and port.
Public Port	Specify which port can be redirected to the specified 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.

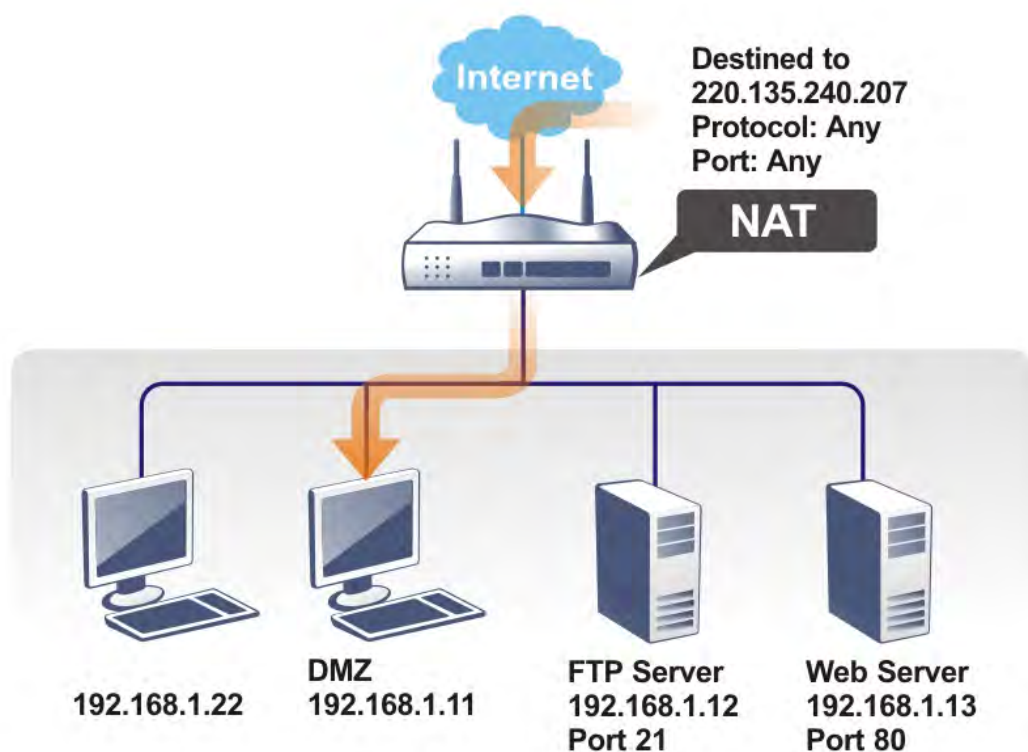
System Maintenance >> Management



IPv4 Management Setup	IPv6 Management Setup
Router Name <input type="text" value="DrayTek"/>	
<input type="checkbox"/> Default:Disable Auto-Logout	
Internet Access Control	Management Port Setup
<input type="checkbox"/> Allow management from the Internet Domain name allowed <input type="text"/>	<input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports
<input type="checkbox"/> FTP Server	Telnet Port <input type="text" value="23"/> (Default: 23)
<input checked="" type="checkbox"/> HTTP Server	HTTP Port <input type="text" value="80"/> (Default: 80)
<input checked="" type="checkbox"/> HTTPS Server	HTTPS Port <input type="text" value="443"/> (Default: 443)
<input checked="" type="checkbox"/> Telnet Server	FTP Port <input type="text" value="21"/> (Default: 21)
<input checked="" type="checkbox"/> TR069 Server	TR069 Port <input type="text" value="8069"/> (Default: 8069)
<input type="checkbox"/> SSH Server	SSH Port <input type="text" value="22"/> (Default: 22)
<input checked="" type="checkbox"/> Disable PING from the Internet	TLS/SSL Encryption Setup
LAN Access Control	<input type="checkbox"/> Enable SSL 3.0
	<input checked="" type="checkbox"/> Device Management
	<input type="checkbox"/> Respond to external device

3.4.2 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:


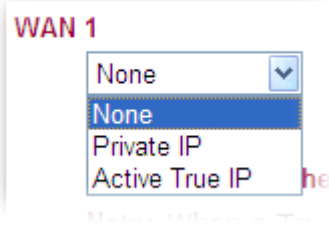
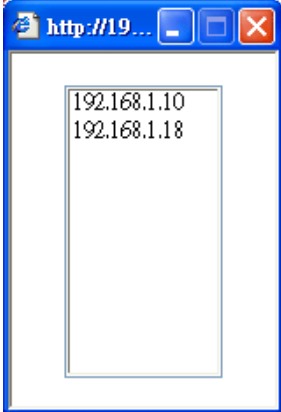
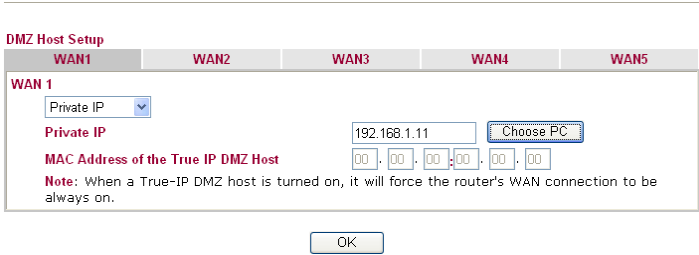
NAT >> DMZ Host Setup

DMZ Host Setup

WAN1	WAN2	WAN3
WAN 1		
<div>None</div>		
Private IP		
<div>Choose PC</div>		
MAC Address of the True IP DMZ Host		
<div>00 . 00 . 00 : 00 . 00 . 00</div>		
Note: When a True-IP DMZ host is turned on, it will force the router's WAN connection to be always on.		
<div>OK</div>		

Available settings are explained as follows:

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

<p>WAN 1</p> <p>None </p>	<p>Choose Private IP or Active True IP first.</p> <p>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> <p>NAT >> DMZ Host Setup</p>  <p>OK</p>

DMZ Host for WAN2 and WAN3 is slightly different with WAN1. **Active True IP** selection is available for WAN1 only. See the following figure.

NAT >> DMZ Host Setup

DMZ Host Setup

WAN1	WAN2	WAN3
WAN 2		
<div> <div>Enable</div> <div>Private IP</div> </div> <div> <input type="checkbox"/> <input type="text" value="0.0.0.0"/> <input type="button" value="Choose PC"/> </div>		

OK

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

NAT >> DMZ Host Setup

DMZ Host Setup

WAN1	WAN2	WAN3
WAN 2		
Index	Enable	Aux. WAN IP
1.	<input type="checkbox"/>	172.16.3.102
2.	<input type="checkbox"/>	172.16.3.200
<div>Private IP</div> <div> <input type="text" value="0.0.0.0"/> <input type="button" value="Choose PC"/> </div>		

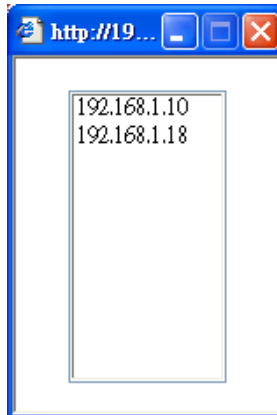
OK Clear

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.

DMZ Host Setup

WAN1		WAN2		WAN3	
WAN 2					
Index	Enable	Aux. WAN IP	Private IP		
1.	<input checked="" type="checkbox"/>	172.16.3.102	192.168.1.10	Choose PC	
2.	<input type="checkbox"/>	172.16.3.200	0.0.0.0	Choose PC	

OK Clear

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

3.4.3 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	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](#) >> [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](#).

Available settings are 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	Display the name for the defined network service.
WAN Interface	Display the WAN interface of the profile.
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	P2P	
WAN Interface	WAN1	
Private IP	192.168.1.11	<input type="button" value="Choose IP"/>

	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	TCP	4500	4700	2.	----	0	0
3.	UDP	4500	4700	4.	----	0	0
5.	----	0	0	6.	----	0	0
7.	----	0	0	8.	----	0	0
9.	----	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	Choose a WAN interface for this profile.
Private IP	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.

3.4.4 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).

OK

Clear

Cancel

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. <div> <div>User Defined ▾</div> <div> User Defined Real Player QuickTime WMP IRC AIM Talk ICQ PalTalk BitTorrent </div> </div>
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. <div> <div>--- ▾</div> <div> --- TCP UDP TCP/UDP </div> </div>
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.

	<div> <div>---</div> <div> <div>---</div> <div>TCP</div> <div>UDP</div> <div>TCP/UDP</div> </div> </div>
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.

3.5 Firewall

3.5.1 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:

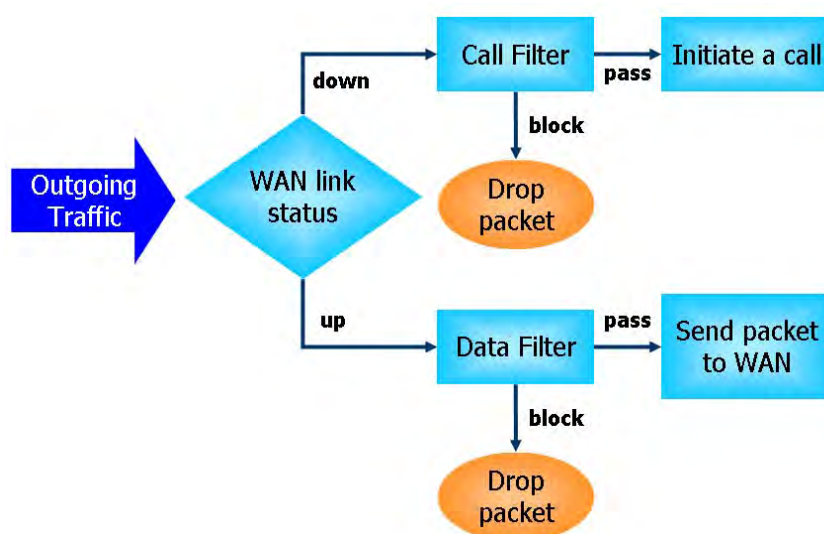
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

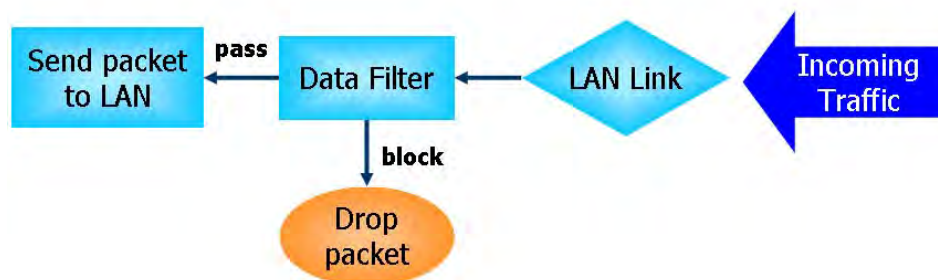
IP Filters

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. Unassigned Numbers |
| 8. Trace route | |

Below shows the menu items for Firewall.



3.5.2 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
☐ Disable

Start Filter Set

Data Filter

☒ Enable
☐ Disable

Start Filter Set

☒ Accept large incoming fragmented UDP or ICMP packets (for some games, ex. CS)
☒ Enable Strict Security Firewall
Accept routing packet from WAN
☐ IPv4 ☐ IPv6

Note: The packets will be filtered with the follow function sequentially:
1. Accept Routing Packet from WAN
2. Data Filter Set and Rule in Firewall
3. Default Rule in Firewall

OK

Cancel

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”.
Enable Strict Security Firewall	<p>Check the box to enable such function.</p> <p>All the packets, while transmitting through Vigor router, will be filtered by firewall settings configured by Vigor router if such feature is enabled. If the firewall system does not have any response (pass or block) for these packets, such as no response coming from web content filter, then the router’s firewall will block the packets directly.</p>
Accept routing packet from WAN	<p>Usually, IPv6 network sessions/traffic from WAN to LAN will be blocked by IPv6 firewall to prevent remote client accessing into the PCs on LAN in default.</p> <p>IPv6 - Check the box to make the packets (routed from WAN to LAN) via IPv6 being accepted by such router. It is effective only for the packets routed but not for packets translated by NAT.</p> <p>IPv4 - Check the box to make the incoming packets via IPv4 being accepted 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:

Application	Action/Profile	Syslog
Filter	Pass	<input type="checkbox"/>
Sessions Control	0 / 60000	<input type="checkbox"/>
Quality of Service	None	<input type="checkbox"/>
User Management	None	<input type="checkbox"/>
APP Enforcement	None	<input type="checkbox"/>
URL Content Filter	None	<input type="checkbox"/>
Web Content Filter	None	<input type="checkbox"/>
DNS Filter	None	<input type="checkbox"/>

Advance Setting

Available settings are explained as follows:

Item	Description
Filter	Select Pass or Block for the packets that do not match with the filter rules.

	Filter <div> Pass Pass Block </div>
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.
Quality of Service	Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later. <div> None None Class 1 Class 2 Class 3 Default </div>
User Management	Such item is available only when Rule-Based is selected in User Management>>General Setup . The general firewall rule will be applied to the user/user group/all users specified here. <div> None None User Object [Create New User] User Group [Create New Group] ALL </div> <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>
APP Enforcement	Select an APP Enforcement profile for global IM/P2P application blocking. If there is no profile for you to select, please choose [Create New] from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the APP Enforcement profile selected here. For detailed information, refer to the section of APP Enforcement profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.
URL Content Filter	Select one of the URL Content Filter profile settings (created in CSM>> URL Content Filter) for applying with this router. Please set at least one profile for choosing in CSM>> URL Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for URL Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.

Web Content Filter	<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>
DNS Filter	<p>Select one of the DNS Filter profile settings (created in CSM>>DNS Filter Profile) for applying with this router. Please set at least one profile in CSM>> Web Content Filter web page first. Or click the DNS Filter link in this page to create a new profile.</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> <div data-bbox="715 853 1390 1070"> <p>Advance Setting</p> <p>Codepage: ANSI(1252)-Latin I</p> <p>Window size: 65535</p> <p>Session timeout: 1440 Minute</p> <p>OK Close</p> </div> <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.</p> <p>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> <div data-bbox="699 1512 1396 1937"> </div> <p>Window size – It determines the size of TCP protocol (0~65535). The more the value is, the better the</p>

	<p>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.

3.5.3 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.

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1

Comments :

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

Firewall >> Edit Filter Set >> Edit Filter Rule

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:

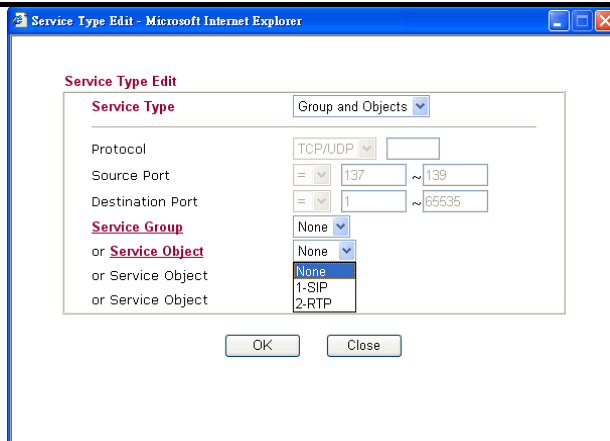
Application	Action/Profile	Syslog
Filter:	<input type="text" value="Block Immediately"/>	<input type="checkbox"/>
Branch to Other Filter Set:	<input type="text" value="None"/>	
Sessions Control	<input type="text" value="0 / 60000"/>	<input type="checkbox"/>
MAC Bind IP	<input type="text" value="Non-Strict"/>	<input type="checkbox"/>
Quality of Service	<input type="text" value="None"/>	<input type="checkbox"/>
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"/>
DNS Filter	<input type="text" value="None"/>	<input type="checkbox"/>

Advance Setting

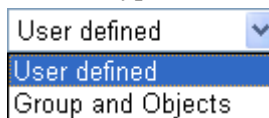
Available settings are explained as follows:

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 the sessions when the above schedule profiles are applied.
Direction	Set the direction of packet flow. It is for Data Filter only. For the Call Filter , this setting is not available since Call Filter is only applied to outgoing traffic.

	<div data-bbox="699 197 1102 347" data-label="Form"> <div>LAN/RT/VPN -> WAN</div> <div>LAN/RT/VPN -> WAN</div> <div>WAN -> LAN/RT/VPN</div> <div>LAN/RT/VPN -> LAN/RT/VPN</div> </div> <p>Note: RT means routing domain for 2nd subnet or other LAN.</p>
Source/Destination IP	<p>Click Edit to access into the following dialog to choose the source/destination IP or IP ranges.</p> <div data-bbox="699 510 1398 999" data-label="Form"> </div> <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> <div data-bbox="699 1216 971 1426" data-label="Form"> <div>Group and Objects</div> <div>Any Address</div> <div>Single Address</div> <div>Range Address</div> <div>Subnet Address</div> <div>Group and Objects</div> </div> <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>
Service Type	<p>Click Edit to access into the following dialog to choose a suitable service type.</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 Type.



Protocol - Specify the protocol(s) which this filter rule will apply to.

Source/Destination Port –

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

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

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

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

Service Group/Object - Use the drop down list to choose the one that you want.

Fragments

Specify the action for fragmented packets. And it is used for **Data Filter** only.

Don't care -No action will be taken towards fragmented packets.

Unfragmented -Apply the rule to unfragmented packets.

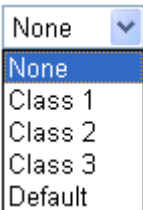
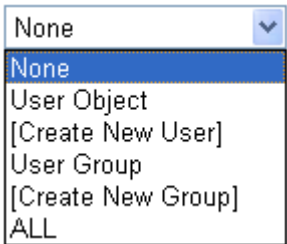
Fragmented - Apply the rule to fragmented packets.

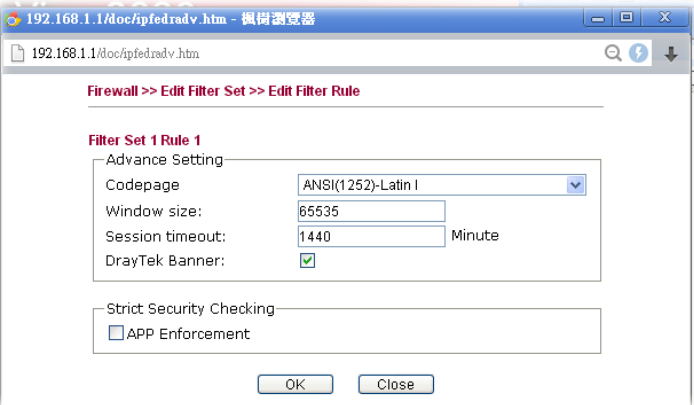
Too Short - Apply the rule only to packets that are too short to contain a complete header.

Filter

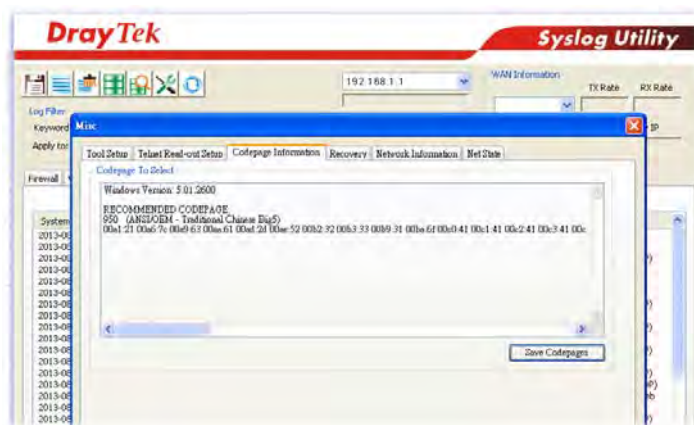
Specifies the action to be taken when packets match the rule.

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

	<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 configured in IP Object for Source IP and Destination IP be bound for applying such filter rule.</p> <p>No-Strict - no limitation.</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> 
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>  <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>
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</p>

	troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.
URL Content Filter	Select one of the URL Content Filter profile settings (created in CSM>> URL Content Filter) for applying with this router. Please set at least one profile for choosing in CSM>> URL Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for URL Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.
Web Content Filter	Select one of the Web Content Filter profile settings (created in CSM>> Web Content Filter) for applying with this router. Please set at least one profile for anti-virus in CSM>> Web Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for Web Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.
DNS Filter	Select one of the DNS Filter profile settings (created in CSM>>DNS Filter Profile) for applying with this router. Please set at least one profile in CSM>> Web Content Filter web page first. Or click the DNS Filter link from the drop down list in this page to create a new profile.
Advance Setting	<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.</p> <p>If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup</p>

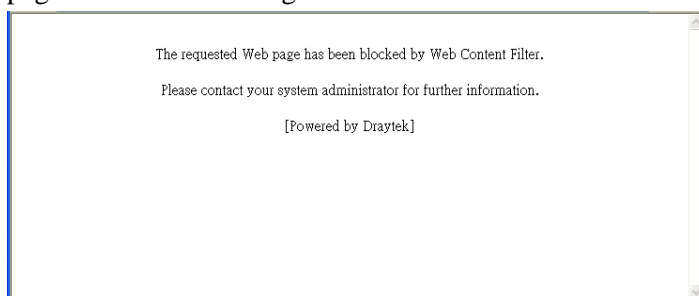
dialog, you will see the recommended codepage listed on the dialog box.



Window size – It determines the size of TCP protocol (0~65535). The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper.

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

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



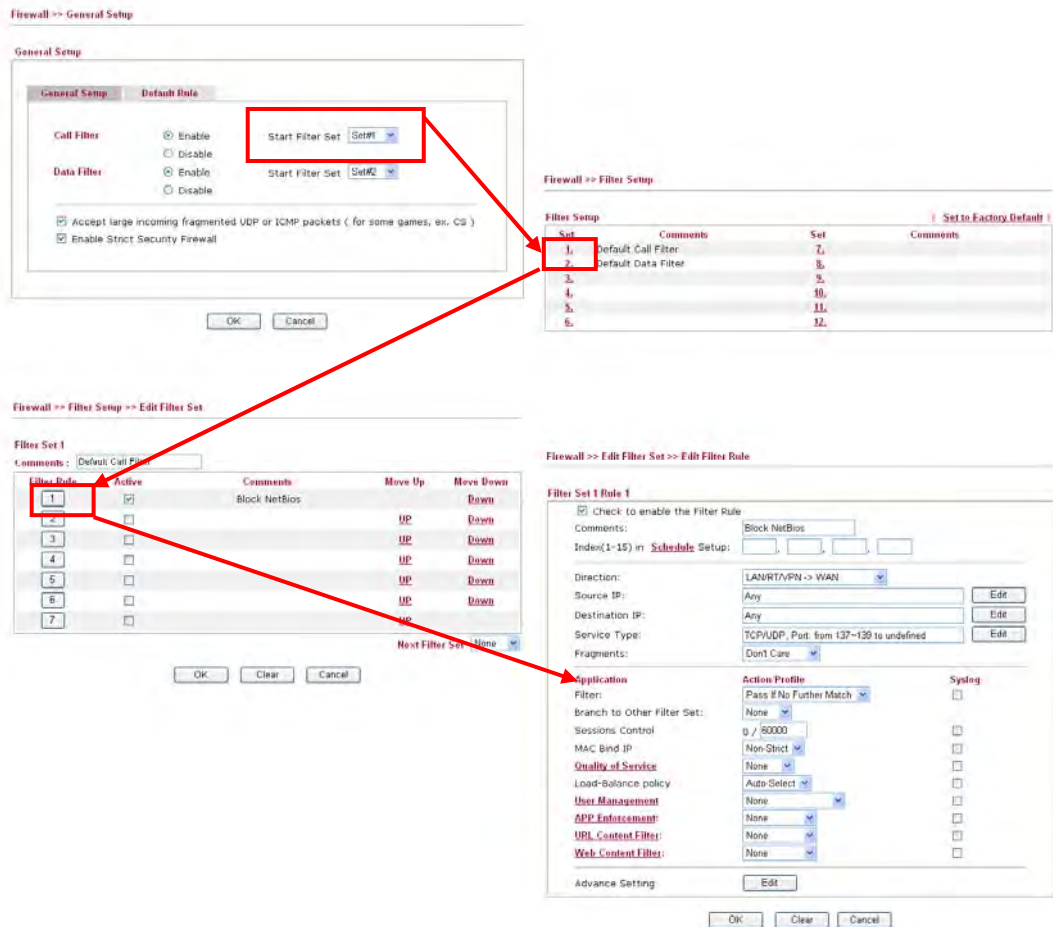
Strict Security Checking - All the packets, while transmitting through Vigor router, will be filtered by firewall settings configured by Vigor router. When the resource is inadequate, the packets will be blocked if Strict Security Checking is enabled. If Strict Security Checking is not enabled, then the packets will pass through the router.

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

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 one 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.



3.5.4 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 Select All

<input type="checkbox"/> Enable SYN flood defense	Threshold	2000	packets / sec
	Timeout	10	sec
<input type="checkbox"/> Enable UDP flood defense	Threshold	2000	packets / sec
	Timeout	10	sec
<input type="checkbox"/> Enable ICMP flood defense	Threshold	250	packets / sec
	Timeout	10	sec
<input type="checkbox"/> Enable Port Scan detection	Threshold	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			

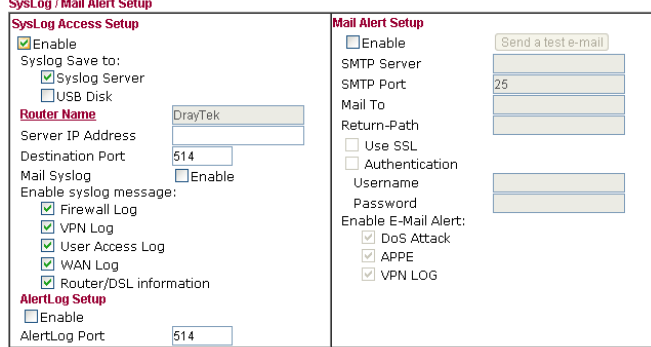
Enable DoS defense function to prevent the attacks from hacker or crackers.

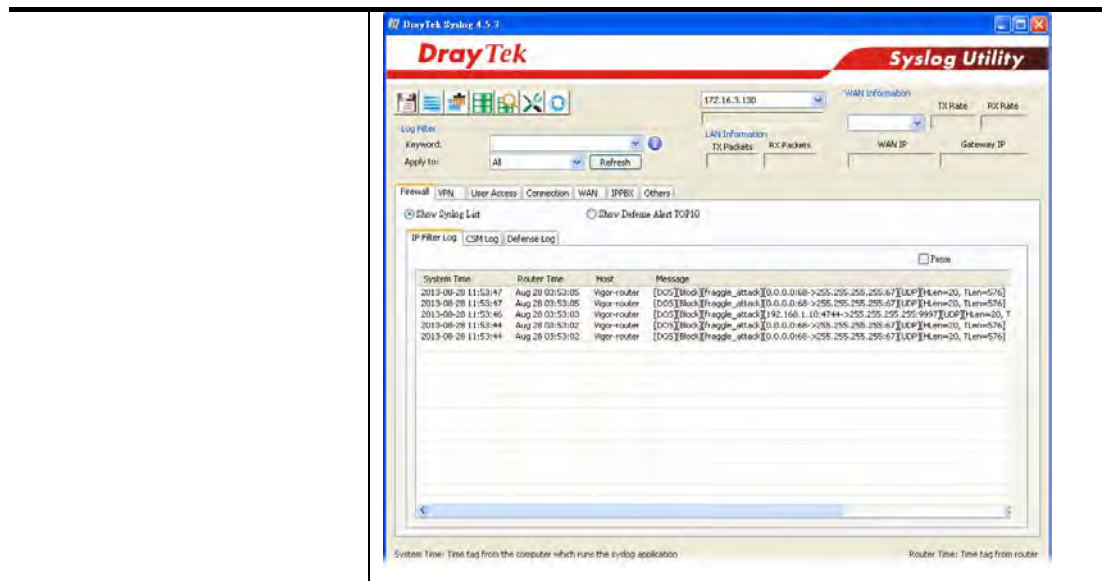
OK Clear All Cancel

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>
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</p>

	means, when 2000 packets per second received, they will be regarded as “attack event” and the session will be paused for 10 seconds.
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 Port Scan 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>
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</p>

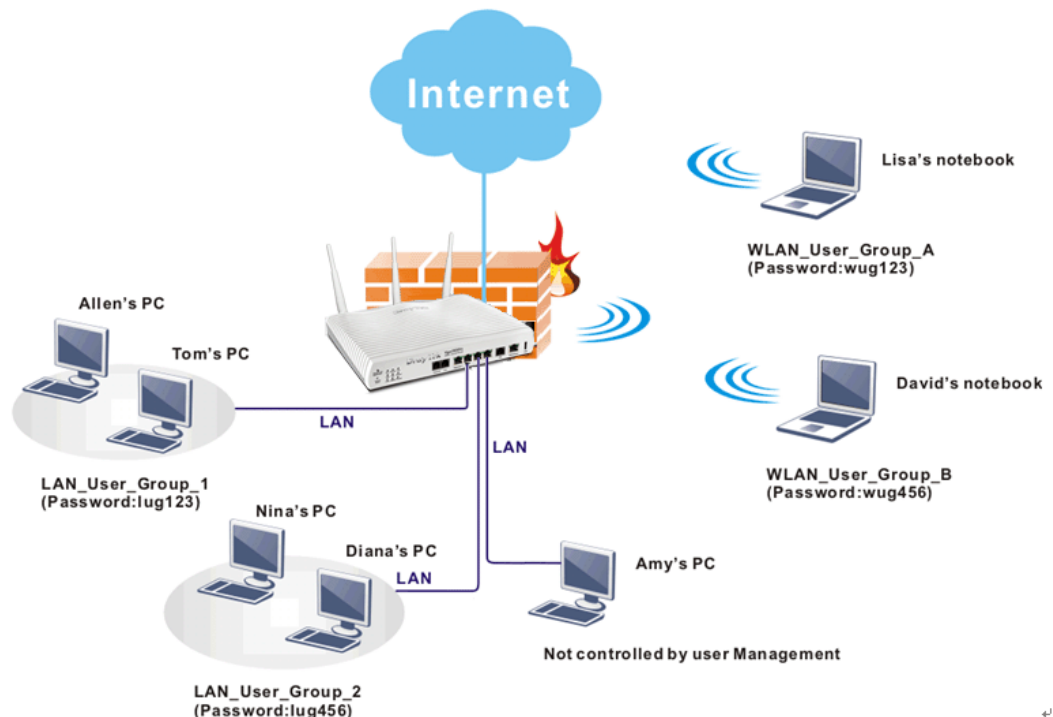
	coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.
Block TCP flag scan	Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include <i>no flag scan</i> , <i>FIN without ACK scan</i> , <i>SYN FINscan</i> , <i>Xmas scan</i> and <i>full Xmas scan</i> .
Block Tear Drop	Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.
Block Ping of Death	Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.
Block ICMP Fragment	Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.
Block Unassigned Numbers	Check the box to activate the Block Unknown Protocol function. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and reject this kind of packets.
Warning Messages	<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> <p>System Maintenance >> SysLog / Mail Alert Setup</p>  <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.</p> <p>OK Clear</p>



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

3.6 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.



3.6.1 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 Selection:

☒ **Rule-Based** is a management method based on IP address. Administrator may set different firewall rules to different IP address.

☐ **User-Based** is a management method based on user profiles. Administrator may set different firewall rules to different user profiles.

Authentication page:

Web Authentication: ☒ HTTPS ☐ HTTP

☐ Display IP address on the dialog box pops up after successful login.

Landing page:

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

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

OK Clear Cancel

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</p>

	Setup and Filter Rule to the users.
Authentication page	Web Authentication - Choose the protocol for web authentication. Display IP Address on tracking window – Check the box to display the IP address of the client on the tracking window.
Landing Page	Type the information to be displayed on the first web page when the LAN user accessing into Internet via such router.

3.6.2 User Profile

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**.

User Management >> User Profile

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

Profile	Enable	Name	Profile	Enable	Name
1.	<input checked="" type="checkbox"/>	admin	17.	<input type="checkbox"/>	
2.	<input checked="" type="checkbox"/>	Dial-In User	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](#) | [65-96](#) | [97-128](#) | [129-160](#) | [161-192](#) | [193-200](#) >>

[Next](#) >>

Note:

1.admin: To change the administrator password, please go to System Maintenance >> Administrator Password.

2.Dial-In User Profile: Dial-In User Profile is reserved for VPN authentication.

3. During authentication Router will check all the local user profiles first and then the profiles in external servers.

To set the user profile, please click any index number link to open the following page. Notice that profile 1 (**admin**) and profile 2 (**System Reservation**) are factory default settings. Profile 2 is reserved for future use.

Profile Index 3

1. Common Settings

<input type="checkbox"/> Enable this account	
Username	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>



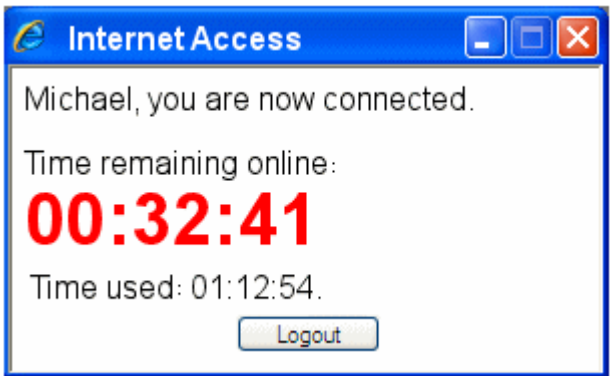


2. Web login Setting

Idle Timeout	<input type="text" value="10"/> min(s) 0:Unlimited
Max User Login	<input type="text" value="0"/> 0:Unlimited
External Server Authentication	<input type="text" value="None"/>
Log	<input type="text" value="None"/>
Pop Browser Tracking Window	<input checked="" type="checkbox"/>
Authentication	<input checked="" type="checkbox"/> Web <input checked="" type="checkbox"/> Alert Tool <input checked="" type="checkbox"/> Telnet
Landing Page	<input type="checkbox"/>
Index(1-15) in Schedule Setup:	<input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>
<input type="checkbox"/> Enable Time Quota	<input type="text" value="0"/> min. <input type="button" value="+"/> <input type="button" value="-"/> <input type="text" value="0"/> min.
<input type="checkbox"/> Enable Data Quota	<input type="text" value="0"/> MB <input type="button" value="+"/> <input type="button" value="-"/> <input type="text" value="0"/> MB
Reset quota to default when scheduling time expired	
<input type="checkbox"/> Enable	Default Time Quota <input type="text" value="0"/> min. Default Data Quota <input type="text" value="0"/> MB

Available settings are explained as follows:

Item	Description
Common Settings	<p>Enable this account - Check this box to enable such user profile.</p> <p>Username - 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.</p> <p>The maximum length of the name you can set is 24 characters.</p> <p>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.</p> <p>The maximum length of the password you can set is 24 characters.</p> <p>Confirm Password - Type the password again for confirmation.</p>

Item	Description
Web login Setting	<p>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.</p> <p>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.</p> <p>External Service Authentication - router will authenticate the dial-in user by itself or by external service such as LDAP server or Radius server or TACACS+ server. If LDAP, Radius or TACACS+ is selected here, it is not necessary to configure the password setting above.</p> <p>Log - Time of login/log out, block/unblock for the user(s) can be sent to and displayed in Syslog. Please choose any one of the log items to take down relational records for the user(s).</p> <p>Pop Browser Tracking Window - If such function is enabled, a pop up window will be displayed on the screen with time remaining for connection if Idle Timeout is set. However, the system will update the time periodically to keep the connection always on. Thus, Idle Timeout will not interrupt the network connection.</p> <p>Authentication - Any user (from LAN side or WLAN side) tries to connect to Internet via Vigor router must be authenticated by the router first. There are three ways offered by the router for the user to choose for authentication.</p> <ul style="list-style-type: none"> ● Web – If it is selected, the user can type the URL of the router from any browser. Then, a login window will be popped up and ask the user to type the user name and password for authentication. If succeed, a Welcome Message (configured in User Management >> General Setup) will be displayed. After authentication, the destination URL (if requested by the user) will be guided automatically by the router. ● Alert Tool – If it is selected, the user can open Alert Tool and type the user name and password for authentication. A window with remaining time of connection for such user will be displayed. Next, the user can access Internet through any browser on Windows. Note that Alert Tool can be downloaded from DrayTek web site. ● Telnet – If it is selected, the user can use Telnet command to perform the authentication job. <p>Landing Page - When a user tries to access into the web user interface of Vigor router 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>

Item	Description
	<p>Check this box to enable such function.</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> <p>Enable Time Quota - Time quota means the total connection time allowed by the router for the user with such profile. Check the box to enable the function of time quota. The first box displays the remaining time of the network connection. The second box allows to type the number of time (unit is minute) which is available for the user (using such profile) to access Internet.</p> <p> – Click this box to set and increase the time quota for such profile.</p> <p> – Click this box to decrease the time quota for such profile.</p> <div data-bbox="703 846 1385 1458" style="border: 1px solid black; padding: 10px;"> <p>Note: A dialog will be popped up to notify how many time remained when a user accesses into Internet through Vigor router successfully.</p>  <p>When the time is up, all the connection jobs including network, IM, social media, facebook, and etc. will be terminated.</p> </div> <p>Enable Data Quota - Data Quota means the total amount for data transmission allowed for the user. The unit is MB/GB.</p> <p> – Click this box to set and increase the data quota for such profile.</p> <p> – Click this box to decrease the data quota for such profile.</p> <p>Reset quota to default when scheduling time expired - Set default time quota and data quota for such profile. When the scheduling time is up, the router will use the default quota settings automatically.</p> <ul style="list-style-type: none"> ● Enable – Check it to use the default setting for time quota and data quota. ● Default Time Quota – Type the value for the time

Item	Description
	manually.
	<ul style="list-style-type: none"> ● Default Data Quota – Type the value for the data manually.

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

3.6.3 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
3-LAN_User_Group_1
4-WLAN_User_Group_A
5-WLAN_User_Group_B

>>

<<

Selected User Objects(Max 32 Objects)


OK

Clear

Cancel

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

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

3.6.4 User Online Status

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

User Management >> User Online Status

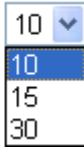
[illegible]

Note:

1. Please click "IP Address" to view all online users.
2. Dial-in User profiles are linked to VPN clients and therefore cannot be logged-out or deleted while connecting.

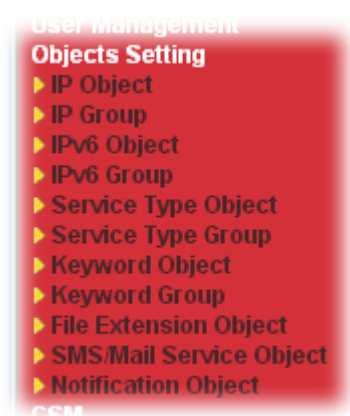
Total Number : 1

Available settings are explained as follows:

Item	Description
Refresh Seconds	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically. Refresh Seconds: 
Refresh	Click this link to refresh this page manually.
Index	Display the number of the data flow.
User	Display the authority of the account.
IP Address	Display the IP address of the device.
Profile	Display the user which connects to Vigor router currently. You can click the link under the username to open the user profile setting page for that user.
Last Login Time	Display the login time that such user connects to the router last time.
Expired Time	Display the expired time of the network connection for the user.
Idle Time	Display the idle timeout setting for such profile.
Action	Block - can prevent specified user accessing into Internet. Unblock – the user will be blocked. Logout – the user will be logged out forcefully.

3.7 Objects Setting

Define objects such as IP address, service type, keyword, file extension and others. These pre-defined objects can be applied in CSM.



3.7.1 IP Object

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).

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

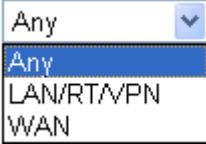
2. The configuration page will be shown as follows:

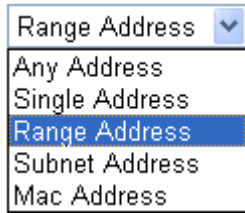
Objects Setting >> IP Object

Profile Index : 11

Name:	<input type="text" value="RD Department"/>
Interface:	<input type="text" value="Any"/>
Address Type:	<input type="text" value="Range Address"/>
Mac Address:	<input type="text" value="00 : 00 : 00 : 00 : 00 : 00"/>
Start IP Address:	<input type="text" value="192.168.1.65"/>
End IP Address:	<input type="text" value="192.168.1.69"/>
Subnet Mask:	<input type="text" value="0.0.0.0"/>
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.
Interface	<div>Choose a proper interface. </div> <div>For example, the Direction setting in Edit Filter Rule will ask you specify IP or IP range for WAN or LAN/RT/VPN or any IP address. If you choose LAN/RT/VPN as the Interface here, and choose LAN/RT/VPN as the direction setting in Edit Filter Rule, then all the IP addresses specified with LAN/RT/VPN interface will be opened for you to choose in Edit Filter Rule page.</div>

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> <p>Select Any Address if this object contains any IP address.</p> <p>Select Mac Address if this object contains Mac address.</p> 
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>

3.7.2 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

2. 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.

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

Objects Setting >> IP Group

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

Index	Name	Index	Name
<u>1.</u>	Administration	<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	

3.7.3 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.	

2. The configuration page will be shown as follows:

Profile Index : 1

Name:	<input type="text"/>
Address Type:	Subnet Address <input type="button" value="v"/>
Mac Address:	<input type="text" value="00:00:00:00:00:00"/>
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> <input type="button" value="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.

3.7.4 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.	

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.

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

Objects Setting >> IP Group

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

Index	Name	Index	Name
1.	v6_group1	17.	
2.		18.	
3.		19.	
4.		20.	

3.7.5 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.	

2. The configuration page will be shown as follows:

Profile Index : 1

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

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile.
Protocol	Specify the protocol(s) which this profile will apply to. <div> <input type="text" value="TCP"/> <div> <div>TCP</div> <div>Any</div> <div>ICMP</div> <div>IGMP</div> <div>TCP</div> <div>UDP</div> <div>TCP/UDP</div> <div>Other</div> </div> <input type="text" value="6"/> </div>
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>	

3.7.6 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.	

2. 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

>>
<<

OK Clear Cancel

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.

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

Objects Setting >> Service Type Group

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

Group	Name	Group	Name
<u>1.</u>	VoIP	<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	

3.7.7 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

OK Clear Cancel

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.	

3.7.8 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)

>>

<<

OK

Clear

Cancel

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.	

3.7.9 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.

[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"/> .vrn
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
<u>1.</u>	game	<u>5.</u>	
<u>2.</u>		<u>6.</u>	
<u>3.</u>		<u>7.</u>	
<u>4.</u>		<u>8.</u>	

3.7.10 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	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:

Objects Setting >> SMS / Mail Service Object

Profile Index: 1

Profile Name	Line_down
Service Provider	kotsms.com.tw (TW) ▼
Username	line1
Password	*****
Quota	10
Sending Interval	3 (seconds)

Note: 1. Only one message can be sent during the "Sending Interval" time.
2. If the "Sending Interval" was set to 0, there will be no limitation.

OK Clear Cancel

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.

Objects Setting >> SMS / Mail Service Object

Profile Index: 9

Profile Name	Custom 1
Service Provider	
<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	10
Sending Interval	3 (seconds)

Note: 1. Only one message can be sent during the "Sending Interval" time.
2. If the "Sending Interval" was set to 0, there will be no limitation.

OK Clear Cancel

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 total number of the messages that the router will send out.
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	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	Pr
<u>1.</u>	
<u>2.</u>	
<u>3.</u>	
<u>4.</u>	

2. The configuration page will be shown as follows:

Objects Setting >> SMS / Mail Service Object

Profile Index: 1

Profile Name	Mail_notify
SMTP Server	192.168.1.98
SMTP Port	485
Sender Address	carrie@draytek.com
<input type="checkbox"/> Use SSL	
<input checked="" type="checkbox"/> Authentication	
Username	john
Password	*****
Sending Interval	0 (seconds)

Note: 1. Only one mail can be sent during the "Sending Interval" time.
2. If the "Sending Interval" was set to 0, there will be no limitation.

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.

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

Object Settings >> SMS / Mail Service Object

SMS Provider		Mail Server	Set to Factory Default
Index	Profile Name		
1.	Mail_Notify		
2.			
3.			
4.			

3.7.11 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.			

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

1. Open **Object Setting>>Notification Object**, and click the number (e.g., #1) under Index column for configuration in details.

Object Settings >> Notification Object

Index	Profile Name
1.	
2.	
3.	
4.	

2. 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	

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such notification profile.
Category	Display the types that will be monitored.
Status	Display the status for the category. You can check the box you want to be monitored.

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

Object Settings >> Notification Object

Set to Factory Default		
Index	Profile Name	Settings
1.	Notify_attack	WAN
2.		
3.		
4.		

3.8 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.
--



3.8.1 APP Enforcement Profile

You can define policy profiles for IM (Instant Messenger)/P2P (Peer to Peer)/Protocol/OTHERS 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.	

Available settings are 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 Others 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 **Protocol**.

CSM >> APP Enforcement Profile

Profile Index : 1 Profile Name:

IM	P2P	Protocol	OTHERS
<input type="button" value="Select All"/>	<input type="button" value="Clear All"/>		
PROTOCOL			
Enable	APP Name	Version	Note
<input type="checkbox"/>	DB2		DB2 is a relational database management system (RDBMS) offered by IBM.
<input type="checkbox"/>	DNS		Domain Name System (DNS) protocol is used to translate easily memorized domain names to numerical IP addresses needed for the purpose of locating computer services and devices worldwide.
<input type="checkbox"/>	FTP		File Transfer Protocol (FTP) is used to transfer files from one host to another host over networks.
<input type="checkbox"/>	HTTP	1.1	Hypertext Transfer Protocol (HTTP) is the data communication protocol for the World Wide Web.
<input type="checkbox"/>	IMAP	4.1	Internet message access protocol (IMAP) is a protocol for e-mail retrieval.
<input type="checkbox"/>	IRC	2.4.0	Internet Relay Chat (IRC) is a protocol for live interactive Internet text messaging (chat), synchronous conferencing and file sharing.
<input type="checkbox"/>	Informix		Informix is a relational database management system (RDBMS) offered by IBM.

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.
Support List	Display the all the information (name, version and note) about IM, P2P, Protocol and others applications that Vigor router supports for APPE function.
Action	Block – Block all the packets passing with the settings configured in this page. Pass – Pass all the packets with the settings configured in this page.

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.

The items categorized under **P2P** -----

CSM >> APP Enforcement Profile

Profile Index : 1 Profile Name:

IM	P2P	Protocol	OTHERS
Select All	Clear All		
BitTorrent			
Enable	APP Name	Version	Note
<input type="checkbox"/>	BitTorrent		The encrypted connection can not be 100% blocked. To block BitComet (1.30), BitSpirit (3.2.1), BitTorrent (4.4.1) and UltraTorrent (2.0).

FastTrack			
Enable	APP Name	Version	Note
<input type="checkbox"/>	FASTTRACK		To block BareShare (6.2.0.45), iMesh (9.1), KazaA (1.0.0.3) and Shareaza (4.1.0).

Gnutella			
Enable	APP Name	Version	Note
<input type="checkbox"/>	GNUTELLA		To block BareShare (5.1.0.26), Foxy (1.9.9), LimeWireWin (4.18.3) and Shareaza (2.3.0.0).

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		
IM			
Enable	APP Name	Version	Note
<input type="checkbox"/> Adv	AIM	5.9	
<input type="checkbox"/>	AIM	6/7	Only block Login. If users have already logged in, AIM services can not be blocked.
<input type="checkbox"/>	AliWW	2008	
<input type="checkbox"/>	Ares	2.0.9	
<input type="checkbox"/>	BaiduHi	37378	
<input type="checkbox"/>	Fetion	2010	
<input type="checkbox"/>	GaduGadu Protocol		
<input type="checkbox"/>	Google Chat		
<input type="checkbox"/>	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.
<input type="checkbox"/>	ICU2	8.0.6	
<input type="checkbox"/>	Jabber		

The items categorized under **OTHERS** -----

CSM >> APP Enforcement Profile

Profile Index : 1 Profile Name:

IM	P2P	Protocol	OTHERS
Select All	Clear All		
TUNNEL			
Enable	APP Name	Version	Note
<input type="checkbox"/>	DNSEncrypt	0.0.6	Only blocks DNSEncrypt login.
<input type="checkbox"/>	DynaPass	1.5	
<input type="checkbox"/>	FreeU	10	
<input type="checkbox"/>	HTTP Proxy		
<input type="checkbox"/>	HTTP Tunnel	4.4.4000	
<input type="checkbox"/>	Hamachi	1.0.2.5	
<input type="checkbox"/>	Hotspot Shield	4.15.3	Block Hotspot Shield from establishing VPN connections. Please note that the APP Enforcement needs to be enabled prior than the VPN connections, or the blocking may not be successful.
<input type="checkbox"/>	MS Teredo		

3.8.2 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)

Default Message

```
<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>
```

OK

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.

Administration Message	<p>You can type the message manually for your necessity.</p> <p>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.</p>
-------------------------------	--

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

☐ Exception List

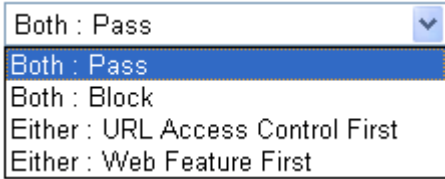
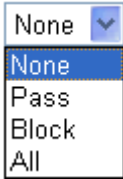
2.Web Feature

☐ Enable Restrict Web Feature

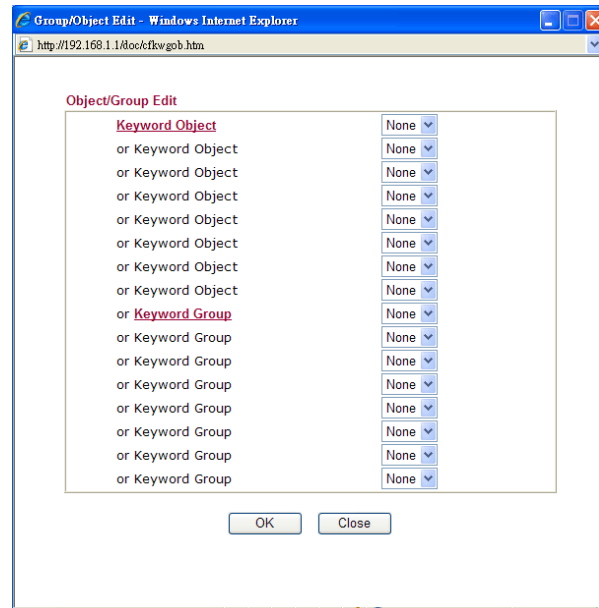
Action: ☐ Cookie ☐ Proxy ☐ Upload **File Extension Profile:**

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,</p>

	<p>the router 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.</p> <ul style="list-style-type: none"> ● 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>Exception List – Specify the object profile(s) as the exception list which will be processed in an opposite manner to the action selected above.</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</p>

router will decline the connection request to the website whose URL string matched to any user-defined keyword. It should be noticed that the more simplified the blocking keyword list is, the more efficiently the Vigor router performs.



Web Feature

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

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

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

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

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

Upload - Check the box to block the file upload by way of web page.

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

	File Extension Profile: <div> None ▼ None 1-default </div>
--	---

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

3.8.3 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 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.

Note 1: Web Content Filter (WCF) is not a built-in service of Vigor router but a service powered by **CommTouch**. If you want to use such service (trial or formal edition), you have to perform the procedure of activation first. For the service of formal edition, please contact with your dealer/distributor for detailed information.

Note 2: CommTouch is merged by **Cyren**, and **GlobalView** services will be continued to deliver powerful cloud-based information security solutions! Refer to:
<http://www.prnewswire.com/news-releases/commtouch-is-now-cyren-239025151.html>

**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)[Default Message](#)Cache : [L1 + L2 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>
```

Legend:

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 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 for a short time (about 1 second) in the router to be accessed quickly if required. Such item can provide accurate URL matching with faster rate.</p> <p>L2 – the router will check the URL that the user wants to access via WCF. If the data has been accessed previously,</p>

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.

L1+L2 Cache – the router will check the URL with fast processing rate combining the feature of L1 and L2.

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

CSM >> Web Content Filter Profile

Profile Index: 1

Profile Name:

Log:

Black/White List

☐ Enable

Action:

Group/Object Selections

Action:

Groups

Child Protection

Categories

☒ Alcohol & Tobacco
☒ Hate & Intolerance
☒ Porn & Sexually
☒ School Cheating
☒ Child Abuse Images

☒ Criminal Activity
☒ Illegal Drug
☒ Violence
☒ Sex Education

☒ Gambling
☒ Nudity
☒ Weapons
☒ Tasteless

Leisure

☐ Entertainment
☐ Travel

☐ Games

☐ Leisure & Recreation

☐ Sports

☐ Fashion & Beauty

Business

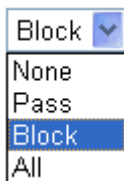
☐ Compromised
☐ Finance
☐ News
☐ Politics
☐ Restaurants & Dining
☐ General
☐ Image Sharing
☐ Private IP Addresses

☐ Dating & Personals
☐ Government
☐ Non-profits & NGOs
☐ Real Estate
☐ Shopping
☐ Cults
☐ Network Errors
☐ Uncategorized Sites

☐ Education
☐ Health & Medicine
☐ Personal Sites
☐ Religion
☐ Translators
☐ Greeting cards
☐ Parked Domains

Available settings are explained as follows:

Item	Description
Black/White List	Enable – Activate white/black list function for such profile. Group/Object Selections – Click Edit to choose the group

	<p>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> <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.

3.8.4 DNS Filter Profile

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.

CSM >> DNS Filter

DNS Filter Profile Table

[Set to Factory Default](#)

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

DNS Filter Local Setting

DNS Filter	<input type="checkbox"/> Enable
Syslog	None <input type="button" value="v"/>
WCF	None <input type="button" value="v"/>
UCF	None <input type="button" value="v"/>
Enable Block Page	<input checked="" type="checkbox"/> Enable

Administration Message (Max 255 characters)

[Default Message](#)

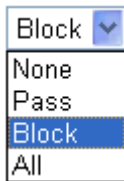
```
<body><center><br><br><br><p>The requested Web page <br> from %SIP% <br>to %URL% <br>that is categorized with %CL% <br>has been blocked by %RNAME% DNS Filter.<p>Please contact your system administrator for further information.</center></body>
```

Legend:

%SID% : Source ID %URL% : URL

Available settings are explained as follows:

Item	Description								
DNS Filter Profile Table	<p>It displays a list of different DNS filter profiles (with specified WCF and UCF).</p> <p>Click the profile link to open the following page. Then, type the name of the profile and specify WCF/UCF based on your requirement.</p> <p>CSM >> DNS Filter</p> <p>Index No. 1</p> <table> <tr> <td>Profile Name</td> <td><input type="text"/></td> </tr> <tr> <td>Syslog</td> <td>None <input type="button" value="v"/></td> </tr> <tr> <td>WCF</td> <td>None <input type="button" value="v"/></td> </tr> <tr> <td>UCF</td> <td>None <input type="button" value="v"/></td> </tr> </table> <p><input type="button" value="OK"/> <input type="button" value="Clear"/> <input type="button" value="Cancel"/></p>	Profile Name	<input type="text"/>	Syslog	None <input type="button" value="v"/>	WCF	None <input type="button" value="v"/>	UCF	None <input type="button" value="v"/>
Profile Name	<input type="text"/>								
Syslog	None <input type="button" value="v"/>								
WCF	None <input type="button" value="v"/>								
UCF	None <input type="button" value="v"/>								

DNS Filter	Check Enable to enable such feature.
Syslog	<p>The filtering result can be recorded according to the setting selected for Syslog.</p> <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> 
DNS Filter Local Setting	<p>DNS Filter Local Setting will be applied to DNS query from clients on LAN when router's DNS server is used.</p> <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 (WCF) - Set the filtering conditions.</p> <p>Service (UCF) - Set the filtering conditions.</p> <p>Cache Time (hour) - Set the time for DNS query.</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.

3.8.5 APPE Support List

This page offers the software versions for each applications managed by APP Enforcement Profiles by Vigor router. Click the IM/P2P/PROTOCOL/OTHERS tab to open the information page for different APP type.

CSM >> APPE Support List

This charts lists out the APP Enforcement supported by Vigor routers.
Last update on 2015-6-18

IM	P2P	PROTOCOL	OTHERS
IM			
APP Name	Version	Note	
AIM	5.9		
AIM	8	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 Protocol/Google			

3.9 Bandwidth Management

Below shows the menu items for Bandwidth Management.



3.9.1 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 proccession 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 proccession 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)

You have reached the maximum number of permitted Internet sessions.<p>Please close one or more applications to allow further Internet access.<p>Contact your system administrator for further information.

Time Schedule

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

Note: Action and Idle Timeout settings will be ignored.

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

Available settings are explained as follows:

Item	Description
Session Limit	<p>Enable - Click this button to activate the function of limit session.</p> <p>Disable - Click this button to close the function of limit session.</p> <p>Default Max Session - Defines the default session number used for each computer in LAN.</p>
Limitation List	Displays a list of specific limitations that you set on this web page.
Specific Limitation	<p>Start IP - Defines the start IP address for limit session.</p> <p>End IP - Defines the end IP address for limit session.</p> <p>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.</p> <p>Add - Adds the specific session limitation onto the list above.</p> <p>Edit - Allows you to edit the settings for the selected limitation.</p> <p>Delete - Remove the selected settings existing on the limitation list.</p>
Administration Message	<p>Type the words which will be displayed when reaches the maximum number of Internet sessions permitted.</p> <p>Click Default Message to display the default message on the screen.</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.

3.9.2 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** ☐ IP Routed Subnet ☒ **Disable**

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, a setting of "0" means unlimited bandwidth.

Time Schedule

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

Note: Action and Idle Timeout settings will be ignored.

OK

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

Available settings are explained as follows:

Item	Description
Bandwidth Limit	<p>Enable - Click this button to activate the function of limit bandwidth.</p> <p>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>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 downstream for each computer in LAN.</p>

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.

3.9.3 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	Enable	--Kbps/--Kbps	Outbound	25%	25%	25%	25%	Inactive	Status Setup
WAN2	Enable	100000Kbps/100000Kbps	Outbound	25%	25%	25%	25%	Inactive	Status Setup
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status Setup

Class Rule

Index	Name	Rule	Service Type
Class 1	VoIP	Edit	Edit
Class 2	HTTP	Edit	
Class 3	Mail	Edit	

☒ **Enable the First Priority for VoIP SIP/RTP:**

SIP UDP Port: (Default: 5060)

[OK](#)

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 the current QoS status of this WAN.</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 control is enabled or not.</p> <p>Online Statistics - Display an online statistics for quality of service for your reference</p> <p>Setup - Allow to configure general QoS setting for WAN interface.</p>
Class Rule	<p>Index - Display the class number that you can edit.</p> <p>Name - Display the name of the class.</p> <p>Rule - Allow to configure detailed settings for the selected Class.</p> <p>Service Type - Allow to configure detailed settings for the service type.</p>

Item	Description
Enable the First Priority for VoIP SIP/RTP	When this feature is enabled, the VoIP SIP/RTP 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.

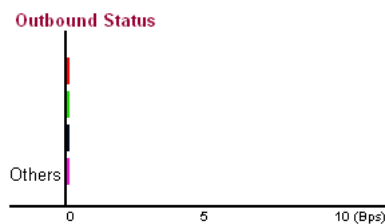
[Bandwidth Management >> Quality of Service](#)

WAN1 Online Statistics

Refresh Interval: seconds

[Refresh](#)

Index	Direction	Class Name	Reserved-bandwidth Ratio	Outbound Throughput (Bytes/sec)
1	OUT		25%	0
2	OUT		25%	0
3	OUT		25%	0
4	OUT	Others	25%	0



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.

WAN1 General Setup

☒ Enable the QoS Control OUT

Index	Class Name	Reserved_bandwidth Ratio
Class 1		25 %
Class 2		25 %
Class 3		25 %
	Others	25 %

☐ Enable UDP Bandwidth Control
 Limited_bandwidth Ratio %

☐ 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.</p> <p>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 WAN2/WAN3. 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 WAN2/WAN3. 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 Ratio	<p>It is reserved for the group index in the form of ratio of reserved bandwidth to upstream speed and reserved bandwidth to downstream speed.</p>
Enable UDP Bandwidth Control	<p>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.</p>

Outbound TCP ACK Prioritize	The difference in bandwidth between download and upload are great in ADSL2+ environment. For the download speed might be impacted by the uploading TCP ACK, you can check this box to push ACK of upload faster to speed the network traffic.
Limited_bandwidth Ratio	The ratio typed here is reserved for limited bandwidth of UDP application.

Edit the Class Rule for QoS

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

Bandwidth Management >> Quality of Service

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

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics
WAN1	Enable	--Kbps/--Kbps	Outbound	25%	25%	25%	25%	Inactive	Status Setup
WAN2	Enable	100000Kbps/100000Kbps	Outbound	25%	25%	25%	25%	Inactive	Status Setup
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status Setup

Class Rule

Index	Name	Rule	Service Type
Class 1	VoIP	Edit	Edit
Class 2	HTTP	Edit	
Class 3	Mail	Edit	

☒ Enable the First Priority for VoIP SIP/RTP:

SIP UDP Port: (Default: 5060)

[OK](#)

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

Bandwidth Management >> Quality of Service

Class Index #1

Name ☒ Tag packets as:

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 <input type="radio"/>	Active	Any	Any	ANY	ANY

[Add](#)
[Edit](#)
[Delete](#)

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

Available settings are explained as follows:

Item	Description
Name	Display the name of such class.
Tag packets as	Check the box to tag the packets with the header selected in the drop down list for this class.
NO	Display the number of the rules defined for such rule.
Status	Display if such rule is enabled (Active) or not.
Local Address	Display the local IP address (on LAN) for the rule.
Remote Address	Display the remote IP address (on LAN/WAN) for the rule.
DiffServ CodePoint	Display the levels of the data for processing with QoS control.
Service Type	Display the service type of the data for processing with QoS control

- 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

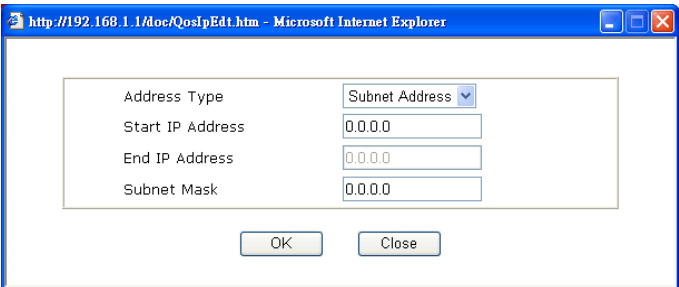
DiffServ CodePoint

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

- 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 type="radio"/>	Active	Any	Any	ANY	ANY
2 <input type="radio"/>	Active	192.168.1.96	172.16.3.228	AF Class1 (Medium Drop)	SNMP-TRAPS (TCP/UDP:162)

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	Enable	--Kbps/--Kbps	Outbound	25%	25%	25%	25%	Inactive	Status Setup
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Status Setup
WAN3	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	-	-

[Add](#)
[Edit](#)
[Delete](#)

[Cancel](#)

3. For adding a new service type, click **Add** to open the following page.

Bandwidth Management >> Quality of Service

Service Type Edit

Service Name

Service Type
TCP

Port Configuration

Type
☒ Single
☐ Range

Port Number
 -

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

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 or other) for the new service.

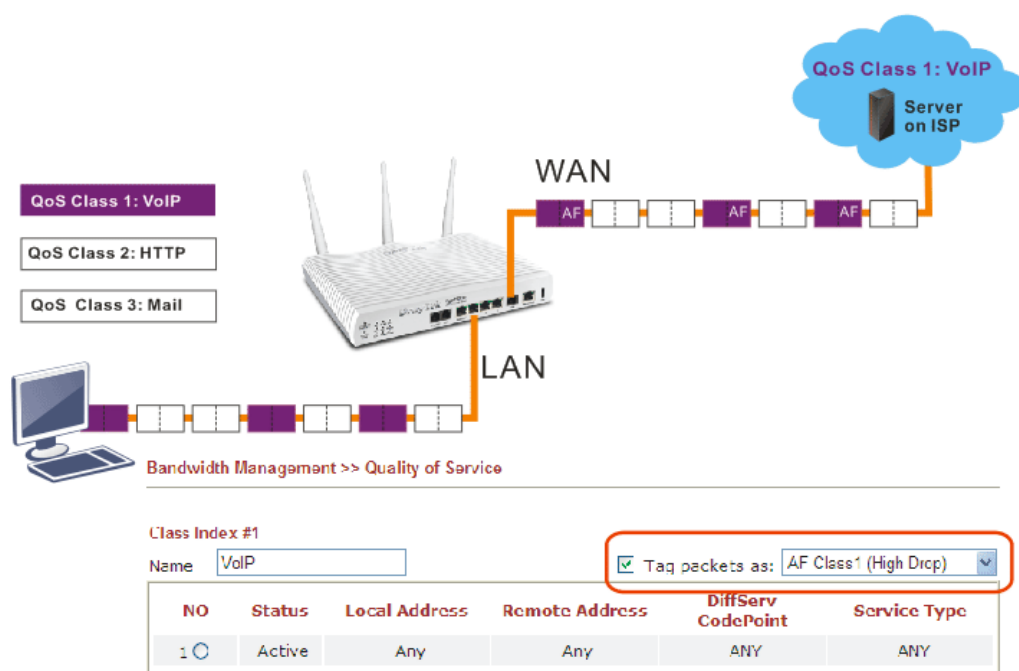
Port Configuration	<p>Type - Click Single or Range as the Type. If you select Range, you have to type in the starting port number and the end porting number on the boxes below.</p> <p>Port Number – Type in the starting port number and the end porting number here if you choose Range as the type.</p>
---------------------------	---

- 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

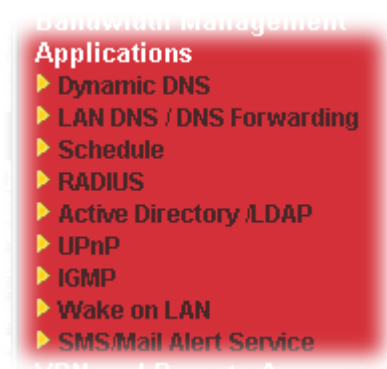
Packets coming from LAN IP can be retagged through QoS setting. When the packets sent out through WAN interface, all the them will be tagged with certain header and that will be easily to be identified by server on ISP.

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.



3.10 Applications

Below shows the menu items for Applications.



3.10.1 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 LogForce 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

OKClear All

Available settings are explained as follows:

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

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

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 WAN1 First

Service Provider dyndns.org (www.dyndns.org)

Service Type Dynamic

Domain Name chronic6653 . dyndns.org dyndns.org

Login Name chronic6653 (max. 64 characters)

Password (max. 23 characters)

☐ Wildcards

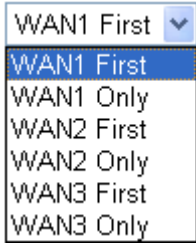
☐ Backup MX

Mail Extender

Determine Real WAN IP 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 First - While connecting, the router will use WAN1/WAN2/WAN3 as the first channel for such account. If WAN1/WAN2/WAN3 fails, the router will use another WAN interface instead. WAN1/WAN2/WAN3 Only - While connecting, the router will use WAN1/WAN2/WAN3 as the only channel for such

	account. 
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>

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

Disable the Function and Clear all Dynamic DNS Accounts

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

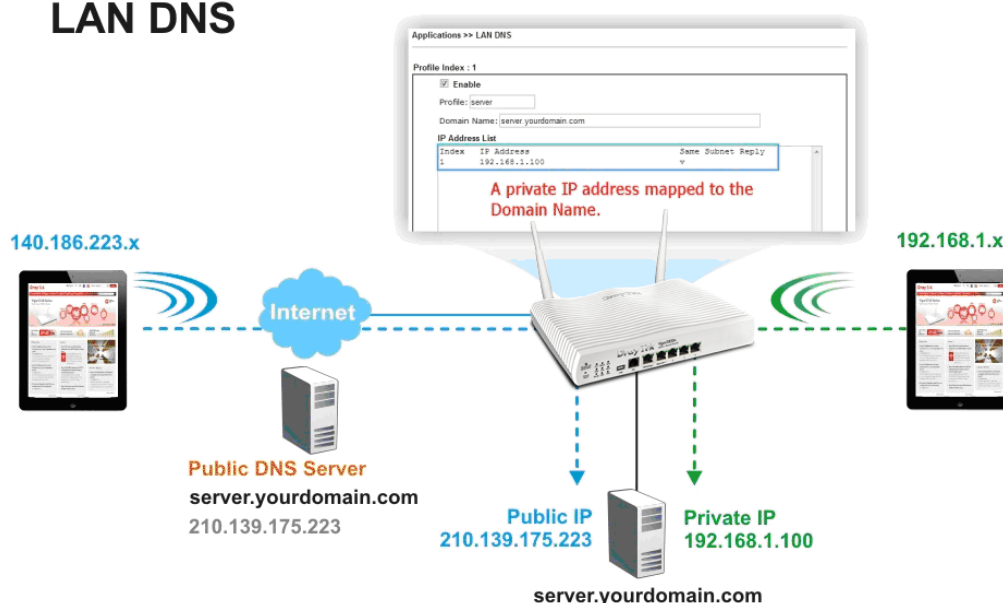
Delete a Dynamic DNS Account

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

3.10.2 LAN DNS / DNS Forwarding

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 Vigor2830 series will respond the specified private IP address.

LAN DNS



Simply click **Application>>LAN DNS / DNS Forwarding** to open the following page.

Applications >> LAN DNS / DNS Forwarding

LAN DNS Resolution / Conditional DNS Forwarding

[Set to Factory Default](#)

Enable	Index	Profile	Domain Name	Forwarding	DNS Server
<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

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles and recover to factory settings.
Enable	Check the box to enable such profile.
Index	Click the number below Index to access into the setting page of schedule.
Profile	Display the name of the profile.

Display the domain name for certain service (e.g., FTP, Mail or Web server) used by such profile.

1. Click any index, for example Index No.1.
2. The detailed settings with index 1 are shown below.

LAN DNS

Conditional DNS Forwarding

Profile Index : 1

☐ Enable

Profile:

Domain Name:

Note: 1. Support wildcard subdomain, ex: *.example.com or www.example.*
2. One domain Name has only one IPv4 address and IPv6 address in the same subnet.

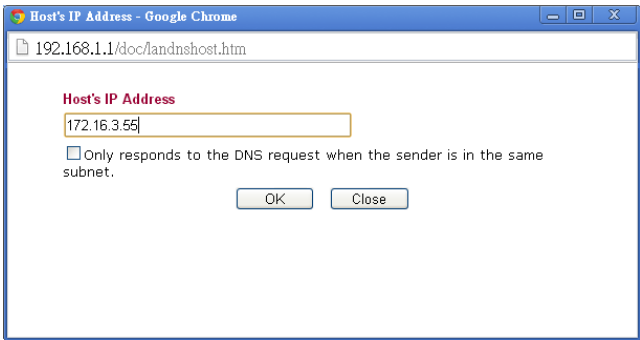
IP Address List

Index	IP Address	Same Subnet Reply
-------	------------	-------------------

Add

Delete

Clear

Item	Description
Enable	Check the box to enable such profile.
Profile	Type a name for such profile.
Domain Name	Type a domain name (e.g., FTP, Mail or Web server) for such profile.
IP Address List	<p>Add – Click it to open the following dialog. You have to give an IP address representing the host.</p>  <ul style="list-style-type: none"> ● Only responds..... - Disable it to apply this profile to all of the LAN subnets. Or enable it to apply such profile to the PCs on the same subnet. <p>Delete – Click it to remove the existed IP address displayed</p>

	on the IP Address List.
--	-------------------------

3. Click **OK** button to save the settings.
4. If you need to configure LAN DNS settings, click index 1 to edit the LAN DNS profile just created. Or, you can click index 2 to use this profile as conditional DNS forwarding.

Applications >> LAN DNS / DNS Forwarding

LAN DNS	Conditional DNS Forwarding
Profile Index : 1 <input checked="" type="checkbox"/> Enable Profile: <input type="text" value="LAN_D1"/> Domain Name: <input type="text"/> Note: Support wildcard subdomain, ex: *.example.com DNS Server IP Address: <input type="text"/>	
<input type="button" value="OK"/> <input type="button" value="Clear"/>	

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 conditional DNS forwarding and click OK to save the configuration, the name also will be applied to LAN DNS automatically.
Domain Name	Type the domain name for such profile.
DNS Server IP Address	Type the IP address of the DNS server you want to use for DNS forwarding.

5. Click **OK** button to save the settings.
6. A new LAN DNS profile has been created.

Applications >> LAN DNS / DNS Forwarding

LAN DNS Resolution / Conditional DNS Forwarding						Set to Factory Default
Enable	Index	Profile	Domain Name	Forwarding	DNS Server	
<input checked="" type="checkbox"/>	1.	LAN_D1	www.draytek.com	-		
<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](#) >>

3.10.3 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

Available settings are 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

OK Clear Cancel

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	<p>Specify which action Call Schedule should apply during the period of the schedule.</p> <p>Force On -Force the connection to be always on.</p> <p>Force Down -Force the connection to be always down.</p> <p>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.</p> <p>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.</p>
Idle Timeout	<p>Specify the duration (or period) for the schedule.</p> <p>How often -Specify how often the schedule will be applied</p> <p>Once -The schedule will be applied just once</p> <p>Weekdays -Specify which days in one week should perform the schedule.</p>

3. Click **OK** button 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

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

3.10.4 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 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"/>

Note: If your radius server does not support MS-CHAP / MS-CHAPv2, please go to [VPN and Remote Access >> PPP General Setup](#), and select 'PAP Only' for 'Dial-In PPP Authentication'.

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.

3.10.5 Active Directory/LDAP

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

Simple Mode

Server Address

Destination Port

389

☐ Use SSL

Regular DN

Regular Password

OK

Cancel

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	<div>There are three types of bind type supported.</div> <div><div>Simple Mode</div><div>Simple Mode</div><div>Anonymous</div><div>Regular Mode</div></div> <div>Simple Mode – Just simply do the bind authentication without any search action.</div> <div>Anonymous – Perform a search action first with Anonymous account then do the bind authentication.</div>

	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 .
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 the box to use the port number specified for SSL.
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 .

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

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.

Applications >> Active Directory /LDAP>>Server Profiles

Index No. 1

Name	<input type="text"/>	
Common Name Identifier	<input type="text"/>	
Base Distinguished Name	<input type="text"/>	
Additional Filter	<input type="text"/>	
Note: Please type in your additional filter for BaseDN search request. For example, 1) For OpenLDAP: (gidNumber=500) 2) For AD: (msNPAllowDialin=TRUE)		
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. The length of the use name is limited to 19 characters.
Common Name Identifier	Type or edit the common name identifier for the LDAP server. The common name identifier for most LDAP server is "cn".
Base Distinguished Name / Group Distinguished Name	Type or edit the distinguished name used to look up entries on the LDAP server. Sometimes, you may forget the Distinguished Name since it's too long. Then you may click the  button to list all the account information on the AD/LDAP Server to assist you finish the setup.
Additional Filter	This is an optional setting.

After finished the above settings, click **OK** to save and exit this page. A new profile will be created.

For detailed information about LDAP application, refer to **section 4.14 How to Implement the AD/LDAP Authentication for User Management?**

3.10.6 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.

Note: UPnP is required for some applications such as PPS, Skype, eMule...and etc. If you are not familiar with UPnP, it is suggested to turn off this function for security.

Applications >> UPnP

UPnP

☒ Enable UPnP Service

☐ Enable Connection Control Service

☐ Enable Connection Status Service

Default WAN ▼

Default WAN

WAN1

WAN2

WAN3

Note: To allow NAT pass-through to a UPnP enabled client the connection control service must also be enabled.

OK Clear Cancel

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 default setting is WAN1.

The reminder as regards concern about Firewall and UPnP

Can't work with Firewall Software

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

Security Considerations

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

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

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

3.10.7 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.

Working Multicast Groups

Refresh

Index	Group ID	P1	P2	P3	P4
-------	----------	----	----	----	----

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/PVC/VLAN. In addition, such function is available in NAT mode.
Enable IGMP Snooping	Check this box to enable this function. Multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.
Refresh	Click this link to renew the working multicast group status.
Group ID	This field displays the ID port for the multicast group. The available range for IGMP starts from 224.0.0.0 to 239.255.255.254.
P1 to P4	It indicates the LAN port used for the multicast group.

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

3.10.8 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 (WOL)** 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 binded IP. If you choose Wake by MAC Address, you have to type the correct MAC address of the host in MAC Address boxes. If you choose Wake by IP Address, you have to choose the correct IP address. Wake by: <input type="button" value="MAC Address"/> <input type="button" value="IP Address"/>
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.

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: MAC Address ▼
IP Address: --- ▼
MAC Address: □ : □ : □ : □ : □ : □ Wake Up!

Result

Send command to client done.

3.10.9 SMS/Mail Alert Service

The function of SMS (Short Message Service)/Mail Alert is that Vigor router sends a message to user's mobile or e-mail box through specified service provider to assist the user knowing the real-time abnormal situations.

Vigor router allows you to set up to **10** SMS profiles which will be sent out according to different conditions.

SMS Alert

This page allows you to specify SMS provider, who will get the SMS, what the content is and when the SMS will be sent.

Applications >> SMS / Mail Alert Service

SMS Alert		Mail Alert		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"/>	1 - ??? ▼	<input type="text"/>	1 - ??? ▼	<input type="text"/>	<input type="text"/>
4 <input type="checkbox"/>	1 - ??? ▼	<input type="text"/>	1 - ??? ▼	<input type="text"/>	<input type="text"/>
5 <input type="checkbox"/>	1 - ??? ▼	<input type="text"/>	1 - ??? ▼	<input type="text"/>	<input type="text"/>
6 <input type="checkbox"/>	1 - ??? ▼	<input type="text"/>	1 - ??? ▼	<input type="text"/>	<input type="text"/>
7 <input type="checkbox"/>	1 - ??? ▼	<input type="text"/>	1 - ??? ▼	<input type="text"/>	<input type="text"/>
8 <input type="checkbox"/>	1 - ??? ▼	<input type="text"/>	1 - ??? ▼	<input type="text"/>	<input type="text"/>
9 <input type="checkbox"/>	1 - ??? ▼	<input type="text"/>	1 - ??? ▼	<input type="text"/>	<input type="text"/>
10 <input type="checkbox"/>	1 - ??? ▼	<input type="text"/>	1 - ??? ▼	<input type="text"/>	<input type="text"/>

Note: All the SMS Alert profiles share the same "Sending Interval" setting if they use the same SMS Provider.

OK

Cancel

Available settings are explained as follows:

Item	Description
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	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	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 Alert

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 Alert		Mail Alert		Set to Factory Default	
Index	Mail Service	Recipient	Notify Profile	Schedule(1-15)	
1 <input type="checkbox"/>	1 - ???		1 - ???		
2 <input type="checkbox"/>	1 - ???		1 - ???		
3 <input type="checkbox"/>	1 - ???		1 - ???		
4 <input type="checkbox"/>	1 - ???		1 - ???		
5 <input type="checkbox"/>	1 - ???		1 - ???		
6 <input type="checkbox"/>	1 - ???		1 - ???		
7 <input type="checkbox"/>	1 - ???		1 - ???		
8 <input type="checkbox"/>	1 - ???		1 - ???		
9 <input type="checkbox"/>	1 - ???		1 - ???		
10 <input type="checkbox"/>	1 - ???		1 - ???		

Note: All the Mail Alert profiles share the same "Sending Interval" setting if they use the sam Mail Server.

OK Cancel

Available settings are explained as follows:

Item	Description
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	Type the schedule number that the notification will be sent out. You can click the Schedule(1-15) link to define the schedule.

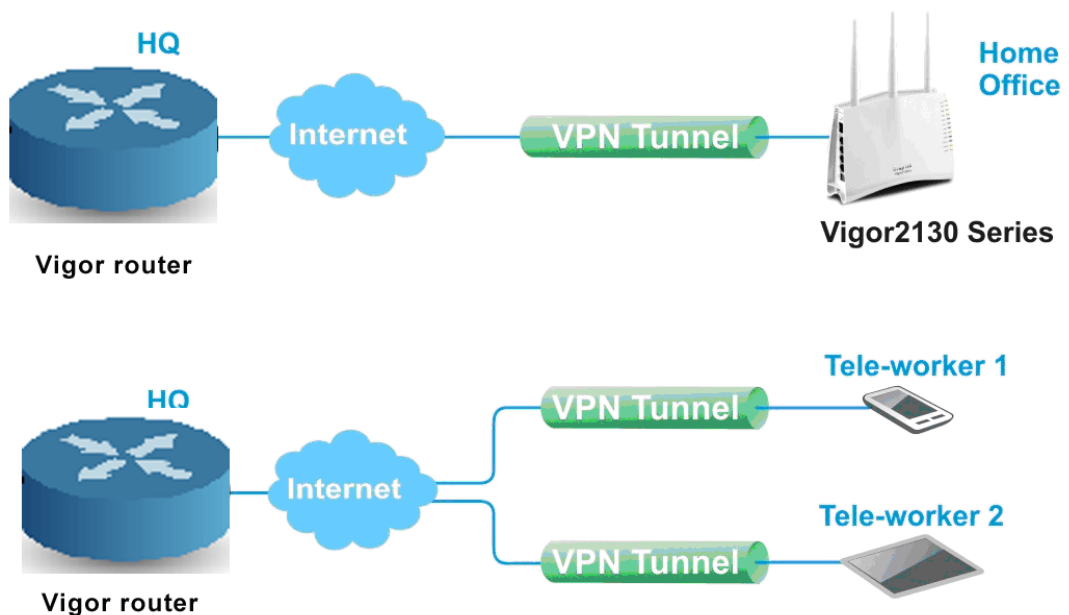
After finishing all the settings here, please click **OK** to save the configuration.

3.11 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.

The VPN built is suitable for:

- Communication between home office and customer
- Secure connection between Teleworker, staff on business trip and main office
- Exchange data between remote office and main office
- POS between chain store and headquarters



Below shows the menu items for VPN and Remote Access.



3.11.1 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 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: To allow VPN pass-through to a separate VPN server on the LAN, disable any services above that use the same protocol and ensure that NAT [Open Ports](#) or [Port Redirection](#) is also configured.

OK Clear Cancel

3.11.2 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

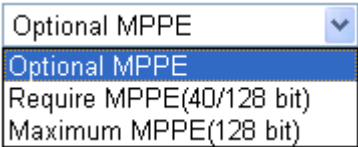
PPP General Setup

PPP/MP Protocol Dial-In PPP Authentication: PAP/CHAP/MS-CHAP/MS-CHAPv2 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 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	PPP Authentication Methods <input checked="" type="checkbox"/> Remote Dial-in User <input checked="" type="checkbox"/> RADIUS <input checked="" type="checkbox"/> AD/LDAP PPTP LDAP Profile Note: Please select 'PAP Only 'Dial-In PPP Authentication', if you want to use AD/LDAP for PPP Authentication. Note: Default priority is Remote Dial-in User -> RADIUS -> AD/LDAP. While using Radius or LDAP Authentication: Assign IP from subnet: LAN1
---	--

OK

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 authentication.</p>
Dial-In PPP Encryption (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 - 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>
IP Address Assignment for Dial-In Users	<p>Assigned IP Start - Enter a start IP address for the dial-in PPP connection. You should choose an IP address from the local private network. For example, if the local private network is 192.168.1.0/255.255.255.0, you could choose 192.168.1.200 as the Start IP Address.</p> <p>You can configure up to four start IP addresses for LAN.</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>

	However, if there is no profile listed, simply click the link of PPTP LDAP Profile to create/add some new LDAP profiles you want.
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.

3.11.3 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.

OK

Cancel

Available settings are explained as follows:

Item	Description
IKE Authentication Method	This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPSec-related VPN connections such as L2TP over IPSec and IPSec tunnel. There are two methods offered by Vigor router for you to authenticate the incoming data coming

	<p>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 - 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.

3.11.4 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 **32** entries of digital certificates for peer dial-in users.

VPN and Remote Access >> IPSec Peer Identity

X509 Peer ID Accounts:

[Set to Factory Default](#)

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

Available settings are 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.

Profile Index : 1

Profile Name <input type="text" value="one"/>	
<input checked="" type="checkbox"/> Enable this account	
<input type="radio"/> Accept Any Peer ID	
<input checked="" type="radio"/> Accept Subject Alternative Name	
Type	<input type="text" value="IP Address"/>
IP	<input type="text"/>
<input type="radio"/> Accept 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"/>


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) .

3.11.5 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 32 access accounts for dial-in users. Besides, you can extend the user accounts to the RADIUS server through the built-in RADIUS client function. The following figure shows the summary table.

VPN and Remote Access >> Remote Dial-in User 

Remote Access User Accounts: [Set to Factory Default](#)

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"/>	---

Note: User Accounts need to be added into User Group to enable SSL Portal Login.

Available settings are 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.

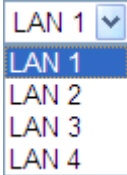
VPN and Remote Access >> Remote Dial-in User

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> <hr/> <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> <hr/> <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="background-color: #e0e0e0;" type="text" value="???"/></p> <p>Password(Max 19 char) <input style="background-color: #e0e0e0;" type="text"/></p> <p><input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP)</p> <p>PIN Code <input style="background-color: #e0e0e0;" type="text"/></p> <p>Secret <input style="background-color: #e0e0e0;" 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="background-color: #e0e0e0;" 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="background-color: #e0e0e0;" 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 – Allow the remote dial-in user to make an SSL VPN connection through Internet.</p> <p>Specify Remote Node - Check the checkbox to specify the IP address of the remote dial-in user, 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> <p>User Name - This field is applicable when you select PPTP or L2TP with or without IPSec policy above. The maximum length for username is 16 characters.</p> <p>Password - This field is applicable when you select PPTP or L2TP with or without IPSec policy above. The maximum length for password is 16 characters.</p> <p>Enable Mobile One-Time Passwords (mOTP) - 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	<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</p>

Item	Description
	<p>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 (optional)- 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.

3.11.6 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 32 VPN tunnels simultaneously.

The following figure shows the summary table according to the item (All/Trunk) selected for View.

VPN and Remote Access >> LAN to LAN

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

View: ☒ All ☐ 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"/>	---

[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 Backup mechanism.

VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles:

View: ☐ All ☒ Trunk

Name	Activate	Members	Status
------	----------	---------	--------

[XXXXXX:This Dial-out profile has already joined for VPN Backup Mechanism]

Available settings are explained as follows:

Item	Description
View	All – Click it to display the LAN to LAN profiles. Trunk – Click it to display the Trunk profiles.
Set to Factory Default	Click to clear all indexes.

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.

Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="???"/> <input type="checkbox"/> Enable this profile VPN Dial-Out Through <input type="text" value="WAN1 First"/> 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.)	Call Direction <input checked="" type="radio"/> Both <input type="radio"/> Dial-Out <input type="radio"/> Dial-in <input type="checkbox"/> Always on Idle Timeout <input type="text" value="300"/> second(s) <input type="checkbox"/> Enable PING to keep alive PING to the IP <input type="text"/>
---	---

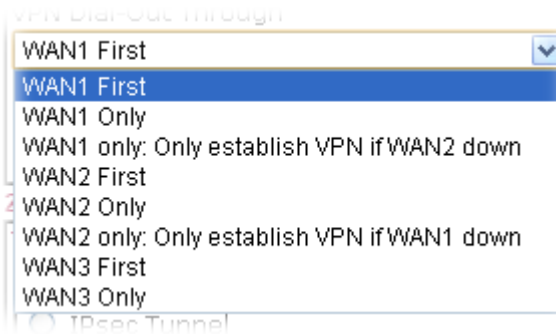
2. Dial-Out Settings

Type of Server I am calling <input checked="" type="radio"/> PPTP <input type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy <input type="text" value="None"/> Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <input type="text"/>	Username <input type="text" value="???"/> Password(Max 15 char) <input type="text"/> PPP Authentication <input type="text" value="PAP Only"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key <input type="text"/> <input type="radio"/> Digital Signature(X.509) Peer ID <input type="text" value="None"/> Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First Local Certificate <input type="text" value="None"/> IPsec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) <input type="text" value="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"/>
--	--

Available settings are explained as follows:

Item	Description
Common Settings	<p>Profile Name – Specify a name for the profile of the LAN-to-LAN connection.</p> <p>Enable this profile - Check here to activate this profile.</p> <p>VPN Dial-Out Through - Use the drop down menu to choose a proper WAN interface for this profile. This setting</p>

is useful for dial-out only.



- **WAN1 /WAN2 /WAN3 First** - While connecting, the router will use WAN1 /WAN2 /WAN3 as the first channel for VPN connection. If WAN1 fails, the router will use another WAN interface instead.
- **WAN1 /WAN2 /WAN3 Only** - While connecting, the router will use WAN1 /WAN2 /WAN3 as the only channel for VPN connection.
- **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.
- **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.

Netbios Naming Packet

- **Pass** – click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.
- **Block** – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.

Multicast via VPN - Some programs might send multicast packets via VPN connection.

- **Pass** – Click this button to let multicast packets pass through the router.
- **Block** – This is default setting. Click this button to let multicast packets be blocked by the router.

Call Direction - Specify the allowed call direction of this LAN-to-LAN profile.

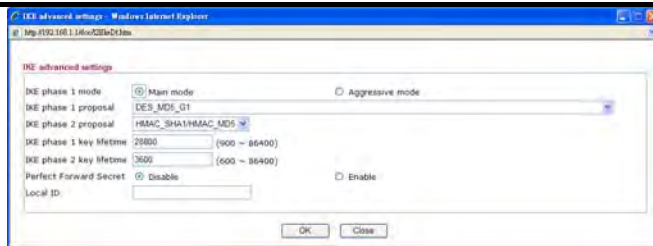
- **Both**:-initiator/responder
- **Dial-Out**- initiator only
- **Dial-In**- responder only.

Always On-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.

	<p>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.</p> <p>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).</p> <p>PING to the IP - Enter the IP address of the remote host that located at the other-end of the VPN tunnel.</p>
Dial-Out Settings	<p>Type of Server I am calling:</p> <p>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.</p> <p>IPSec Tunnel - Build an IPSec VPN connection to the server through Internet.</p> <p>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:</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-out VPN connection becomes one pure L2TP connection. <p>Must: Specify the IPSec policy to be definitely applied on the L2TP connection.</p> <p>User Name - This field is applicable when you select, PPTP or L2TP with or without IPSec policy above. The maximum length for username is 49 characters.</p> <p>Password - This field is applicable when you select PPTP or L2TP with or without IPSec policy above. The maximum length for password is 15 characters.</p> <p>PPP Authentication - This field is applicable when you select, PPTP or L2TP with or without IPSec policy above. PAP/CHAP/MS-CHAP/MS-CHAPv2 is the most common selection due to wild compatibility.</p> <p>VJ compression - This field is applicable when you select PPTP or L2TP with or without IPSec policy above. VJ</p>

	<p>Compression is used for TCP/IP protocol header compression. Normally set to Yes to improve bandwidth utilization.</p> <p>IKE Authentication Method - This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy.</p> <ul style="list-style-type: none"> ● Pre-Shared Key - Input 1-63 characters as pre-shared key. ● Digital Signature (X.509) - Click Digital Signature to invoke this function and select one predefined Profiles set in the VPN and Remote Access >>IPSec Peer Identity as Peer ID. Local ID – Specify which one will be inspected first. ● 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>Local Certificate – Select one of the profiles set in Certificate Management>>Local Certificate.</p> <p>IPSec Security Method - This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.</p> <ul style="list-style-type: none"> ● Medium AH (Authentication Header) means data will be authenticated, but not be encrypted. By default, this option is active. ● High (ESP-Encapsulating Security Payload)- means payload (data) will be encrypted and authenticated. Select from below: ● DES without Authentication -Use DES encryption algorithm and not apply any authentication scheme. ● DES with Authentication-Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm. ● 3DES without Authentication-Use triple DES encryption algorithm and not apply any authentication scheme. ● 3DES with Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm. ● AES without Authentication-Use AES encryption algorithm and not apply any authentication scheme. ● AES with Authentication-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm. <p>Advanced - Specify mode, proposal and key life of each IKE phase, Gateway, etc.</p> <p>The window of advance setup is shown as below:</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.

- **IKE phase 1 proposal**-To propose the local available authentication schemes and encryption algorithms to the VPN peers, and get its feedback to find a match. Two combinations are available for Aggressive mode and nine for **Main** mode. We suggest you select the combination that covers the most schemes.
 - **IKE phase 2 proposal**-To propose the local available algorithms to the VPN peers, and get its feedback to find a match. Three combinations are available for both modes. We suggest you select the combination that covers the most algorithms.
 - **IKE phase 1 key lifetime**-For security reason, the lifetime of key should be defined. The default value is 28800 seconds. You may specify a value in between 900 and 86400 seconds.
 - **IKE phase 2 key lifetime**-For security reason, the lifetime of key should be defined. The default value is 3600 seconds. You may specify a value in between 600 and 86400 seconds.
 - **Perfect Forward Secret (PFS)**-The IKE Phase 1 key will be reused to avoid the computation complexity in phase 2. The default value is inactive this function.
- Local ID**-In **Aggressive** mode, Local ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters.

3. Dial-In Settings

Allowed Dial-In Type <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input checked="" type="checkbox"/> L2TP with IPsec Policy None ▾		Username ??? Password(Max 11 char) VJ Compression On Off
<input type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP or Peer ID 		IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <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 Settings

<input type="checkbox"/> Enable IPsec Dial-Out function GRE over IPsec		
<input type="checkbox"/> Logical Traffic	My GRE IP 	Peer GRE IP

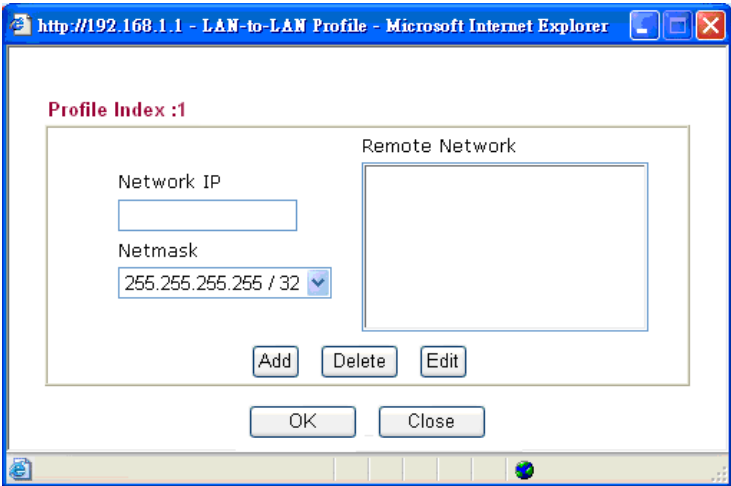
5. TCP/IP Network Settings

My WAN IP 0.0.0.0 Remote Gateway IP 0.0.0.0 Remote Network IP 0.0.0.0 Remote Network Mask 255.255.255.0 Local Network IP 192.168.1.1 Local Network Mask 255.255.255.0 More	RIP Direction Disable ▾ From first subnet to remote network, you have to do Route ▾ <input type="checkbox"/> IPsec VPN with the Same Subnets <input type="checkbox"/> Change default route to this VPN tunnel (Only active if one single WAN is up)
---	---

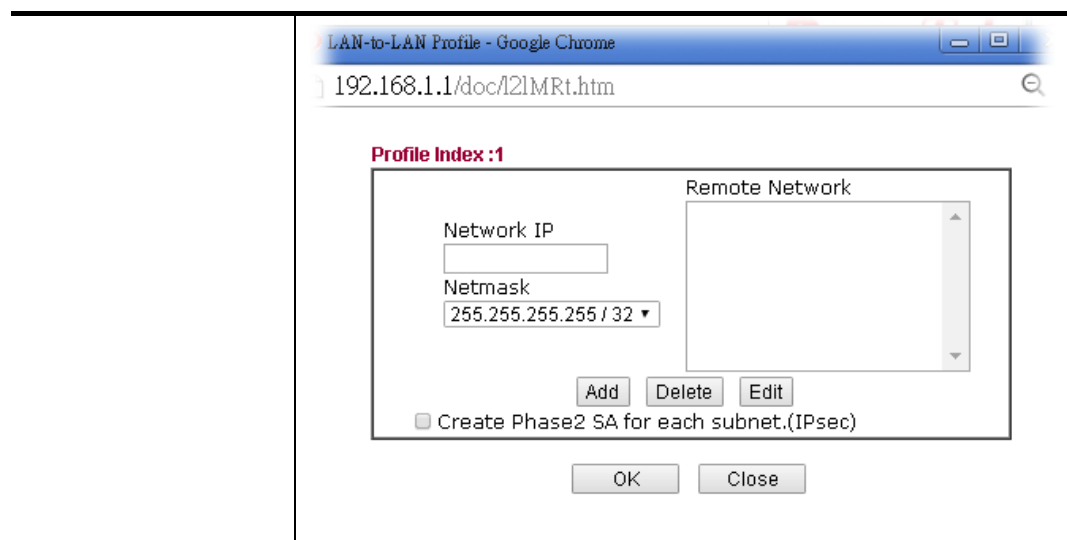
Available settings are explained as follows:

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 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</p>

	<p>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. The maximum length for both username is 11 characters.</p> <p>Password - This field is applicable when you select PPTP or L2TP with or without IPSec policy above. The maximum length for both username is 11 characters.</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 - 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. 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 - This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node.</p> <ul style="list-style-type: none"> ● Medium- Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active. ● High- Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
GRE over IPSec Settings	<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> <p>Logical Traffic: Such technique comes from RFC2890. Define logical traffic for data transmission between both sides</p>

	<p>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>
TCP/IP Network Settings	<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> 

	<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>		
IPSec VPN with the Same subnet	<p>For both ends (e.g., different sections in a company) are within the same subnet, there is a function which allows you to build Virtual IP mapping between two ends. Thus, when VPN connection established, the router will change the IP address according to the settings configured here and block sessions which are not coming from the IP address defined in the Virtual IP Mapping list.</p> <p>After checking the box of IPSec VPN with the Same subnet, the options under TCP/IP Network Settings will be changed as shown below:</p> <p>5. TCP/IP Network Settings</p> <table border="1"> <tr> <td> Remote Network IP Remote Network Mask <input checked="" type="checkbox"/> Translated Local Network LAN1 to 192.168.1.0 Advanced </td> <td> From Local Subnet to Remote network, you have to do Route <input checked="" type="checkbox"/> IPSec VPN with the Same Subnets Translated Type <input checked="" type="radio"/> Whole Subnet <input type="radio"/> Specific IP Address Virtual IP Mapping </td> </tr> </table> <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>Translated Local Network – This function is enabled in default. Use the drop down list to specify a LAN port as the transferred direction. Then specify an IP address. Click Advanced to configure detailed settings if required.</p> <p>Advanced – 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>	Remote Network IP Remote Network Mask <input checked="" type="checkbox"/> Translated Local Network LAN1 to 192.168.1.0 Advanced	From Local Subnet to Remote network, you have to do Route <input checked="" type="checkbox"/> IPSec VPN with the Same Subnets Translated Type <input checked="" type="radio"/> Whole Subnet <input type="radio"/> Specific IP Address Virtual IP Mapping
Remote Network IP Remote Network Mask <input checked="" type="checkbox"/> Translated Local Network LAN1 to 192.168.1.0 Advanced	From Local Subnet to Remote network, you have to do Route <input checked="" type="checkbox"/> IPSec VPN with the Same Subnets Translated Type <input checked="" type="radio"/> Whole Subnet <input type="radio"/> Specific IP Address Virtual IP Mapping		



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

3.11.7 VPN TRUNK Management

VPN trunk includes some features - VPN Backup, 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, and L2TP over IPSec (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.

[VPN and Remote Access >> VPN TRUNK Management](#)



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.

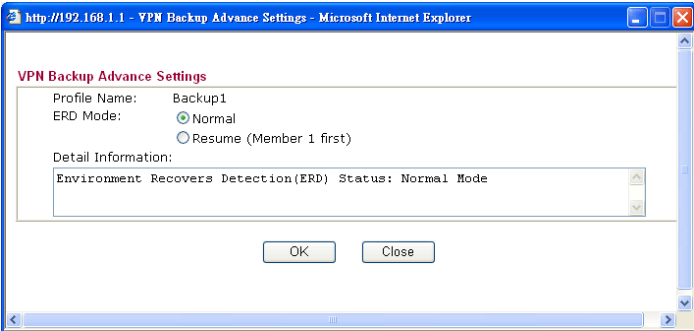
No.	Status	Name	Member1 (Active) Type	Member2 (Active) Type

Advanced

General Setup

Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Profile Name	<input type="text"/>
Member1	<input type="text" value="Please select a LAN-to-LAN Dial-Out profile."/>
Member2	<input type="text" value="Please select a LAN-to-LAN Dial-Out profile."/>
Active Mode	<input checked="" type="radio"/> Backup

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 - “v” means such profile is enabled; “x” means such profile is disabled.</p> <p>Name - Display the name of VPN TRUNK-VPN Backup 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 available only when LAN to LAN profile (or more) is created.</p>  <p>Detailed information for this dialog, see later section - Advanced Backup.</p>
General Setup	<p>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.</p> <p>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.</p> <p>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 mechanism profile.</p> <ul style="list-style-type: none"> ● No - Index number of LAN-to-LAN dial-out profile.

	<ul style="list-style-type: none"> ● 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. <p>Active Mode - Display available mode for you to choose.</p> <p>Add - Add and save new profile to the backup profile list.</p> <p>Update - Click this button to save the changes to the Status (Enable or Disable), profile name, member1 or member2.</p> <p>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.</p>
--	---

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.

How can you set a VPN TRUNK-VPN Backup 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 mechanism profile management well.
2. Access into **VPN and Remote Access>>VPN TRUNK Management**.
3. Set one group of VPN TRUNK – VPN Backup 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.

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)

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 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.

4. GRE over IPSec Settings

☒ Enable IPSec Dial-Out function GRE over IPSec

☐ Logical Traffic

My GRE IP 192.168.50.200 Peer GRE IP 192.168.50.100

5. TCP/IP Network Settings

My WAN IP 0.0.0.0

Remote Gateway IP 0.0.0.0

Remote Network IP 192.168.10.0

Remote Network Mask 255.255.255.0

RIP Direction TX/RX Both

From first subnet to remote network, you have to do

Route

- 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	<input type="text" value="0"/> minute(s)
4. GRE over IPSec Settings			
<input checked="" type="checkbox"/> Enable IPSec Dial-Out function GRE over IPSec <input type="checkbox"/> Logical Traffic			
My GRE IP		<input type="text" value="192.168.50.100"/>	Peer GRE IP <input type="text" value="192.168.50.200"/>
5. TCP/IP Network Settings			
My WAN IP	<input type="text" value="0.0.0.0"/>	RIP Direction	<input type="text" value="TX/RX Both"/>
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)	
<input type="button" value="More"/>			
<input type="button" value="OK"/>		<input type="button" value="Clear"/>	<input type="button" value="Cancel"/>

Advanced Backup

After setting profiles for backup, you can choose any one of them and click **Advanced** for more detailed configuration.

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	<p>ERD means “Environment Recovers Detection”.</p> <p>Normal – choose this mode to make all dial-out VPN TRUNK backup profiles being activated alternatively.</p> <p>Resume – when VPN connection breaks down or disconnects, Member 1 will be the top priority for the system to do VPN connection.</p>
Detail Information	This field will display detailed information for Environment Recovers Detection.

3.11.8 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:

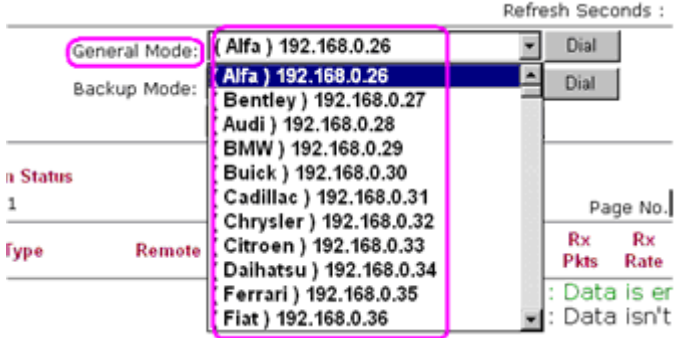
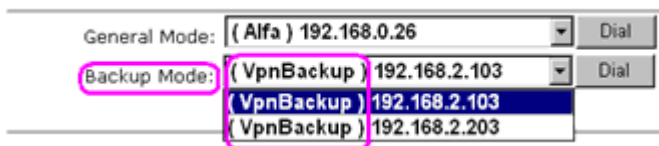
Backup Mode:

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 filed displays the profile configured in LAN-to-LAN (with Index number and VPN Server IP address). The VPN connection built by General Mode does not support VPN backup function.</p>  <p>Backup Mode - This filed 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>  <p>Dial - Click this button to execute dial out function.</p> <p>Refresh Seconds - Choose the time for refresh the dial information among 5, 10, and 30.</p> <p>Refresh - Click this button to refresh the whole connection status.</p>

3.12 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.



3.12.1 Local Certificate

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify	
---	---	---	View	Delete
---	---	---	View	Delete
---	---	---	View	Delete

Note:

1. Please setup the "System Maintenance >> [Time and Date](#)" correctly before signing the local certificate.
2. The Time Zone MUST be setup correctly!!

[GENERATE](#)

[IMPORT](#)

[REFRESH](#)

Available settings are explained as follows:

Item	Description
Generate	Click this button to open Generate Certificate Request window. Type in all the information that the window requests. Then click Generate again.
Import	Click this button to import a saved file as the certification information.
Refresh	Click this button to refresh the information listed below.
View	Click this button to view the detailed settings for certificate request.
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 router’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	
local	/C=TW/O=DrayTek/OU=RD/CN=192...	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><div>Import X509 Local Certificate</div><div><div><div>Congratulation!</div><div>Local Certificate has been imported successfully.</div><div>Please click <div>Back</div> to view the certificate.</div></div></div><div><div>X509 Local Certificate Configuration</div><table><tr><th>Name</th><th>Subject</th><th>Status</th><th colspan="2">Modify</th></tr><tr><td>draytekdemo</td><td>/O=Draytek/OU=Draytek Sales/...</td><td>OK</td><td><div>View</div></td><td><div>Delete</div></td></tr><tr><td>---</td><td>---</td><td>---</td><td><div>View</div></td><td><div>Delete</div></td></tr><tr><td>---</td><td>---</td><td>---</td><td><div>View</div></td><td><div>Delete</div></td></tr></table><div><div>GENERATE</div><div>IMPORT</div><div>REFRESH</div></div></div></div>	Name	Subject	Status	Modify		draytekdemo	/O=Draytek/OU=Draytek Sales/...	OK	<div>View</div>	<div>Delete</div>	---	---	---	<div>View</div>	<div>Delete</div>	---	---	---	<div>View</div>	<div>Delete</div>
Name	Subject	Status	Modify																		
draytekdemo	/O=Draytek/OU=Draytek Sales/...	OK	<div>View</div>	<div>Delete</div>																	
---	---	---	<div>View</div>	<div>Delete</div>																	
---	---	---	<div>View</div>	<div>Delete</div>																	
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</p>																				

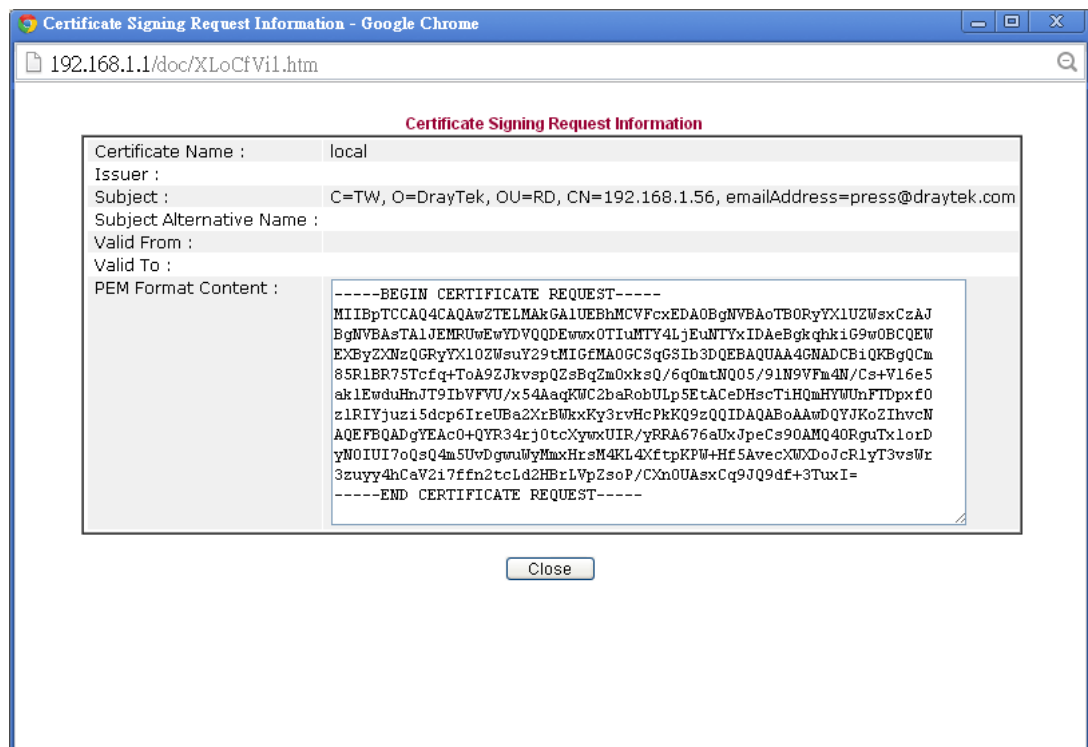
	certificates securely. It is used in (among other things) Netscape and Microsoft Internet Explorer with their import and export options.
Upload Certificate and Private Key	It is useful when users have separated certificates and private keys. And the password is needed if the private key is encrypted.

REFRESH

Click this button to refresh the information listed below.

View

Click this button to view the detailed settings for certificate request.



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.

3.12.2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate.

When the local client and remote client are required to make certificate authentication (e.g., IPsec X.509) for data passing through SSL tunnel and avoiding the attack of MITM, a trusted root certificate authority (Root CA) will be used to authenticate the digital certificates offered by both ends.

However, the procedure of applying digital certificate from a trusted root certificate authority is complicated and time-consuming. Therefore, Vigor router offers a mechanism which allows you to generate root CA to save time and provide convenience for general user. Later, such root CA generated by DrayTek server can perform the issuing of local certificate.

Note: Root CA can be deleted but not edited. If you want to modify the settings for a Root CA, please delete the one and create another one by clicking **Create**.

Certificate Management >> Trusted CA Certificate

X509 Trusted CA Certificate Configuration

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

Note:

1. Please setup the "System Maintenance >> [Time and Date](#)" correctly before you try to generate a RootCA!!
2. The Time Zone MUST be setup correctly!!

IMPORT

REFRESH

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.

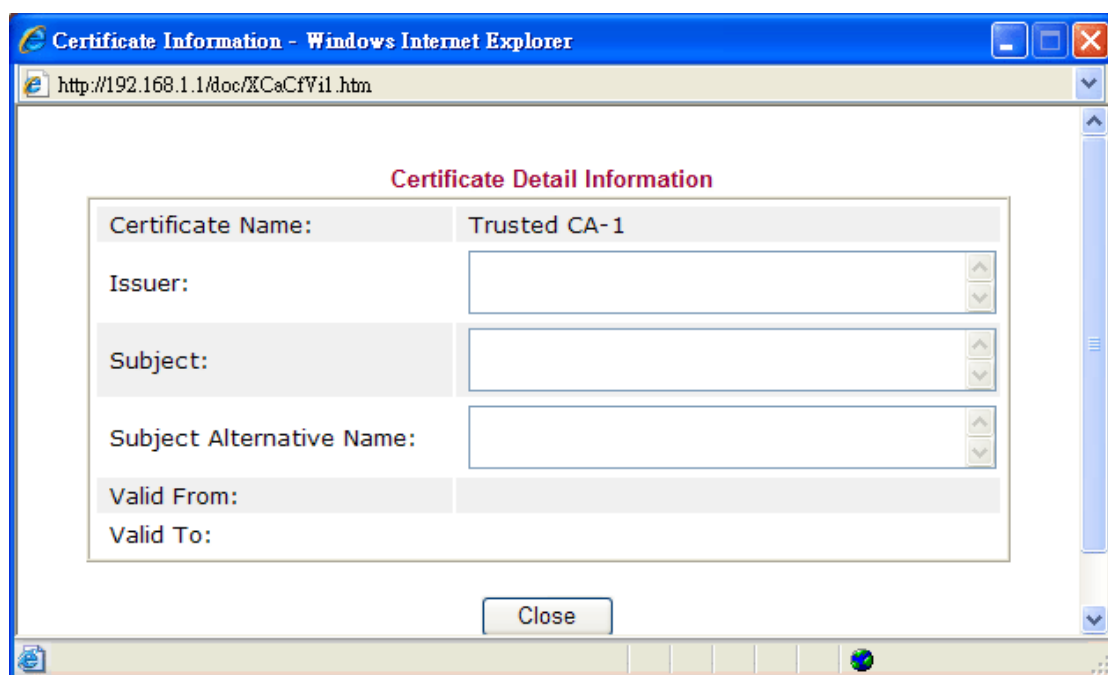
Certificate Management >> Trusted CA Certificate

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.



3.12.3 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: <input type="text"/>
Confirm password: <input type="text"/>
Click <input type="button" value="Backup"/> to download certificates to your local PC as a file.
Restoration
Select a backup file to restore. <input type="button" value="Select"/>
Decrypt password: <input type="text"/>
Click <input type="button" value="Restore"/> to upload the file.

3.13 Wireless LAN

This function is used for “n” models only.

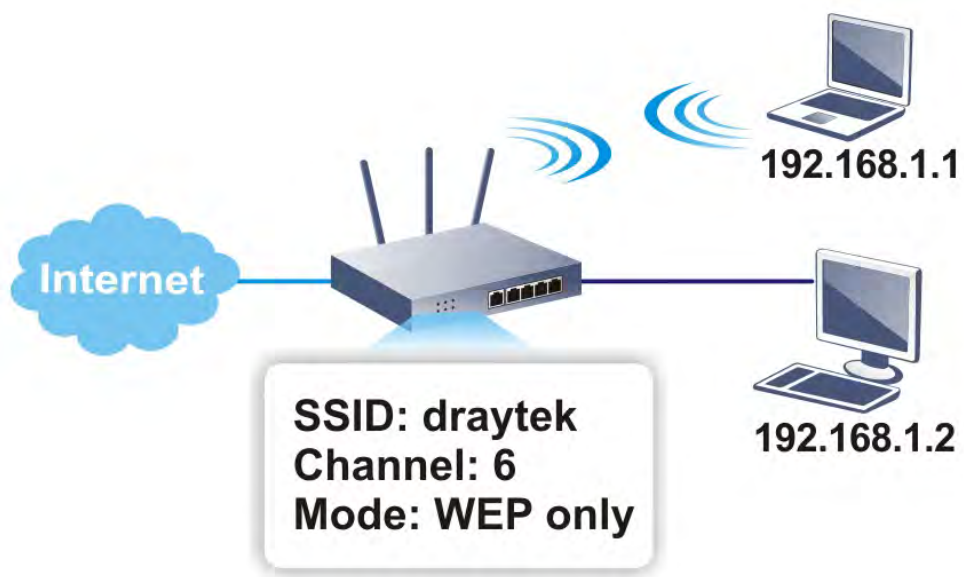
3.13.1 Basic Concepts

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 clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access.

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

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

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



Multiple SSIDs

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

Security Overview

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

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

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

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

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

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

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

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

Below shows the menu items for Wireless LAN.



3.13.2 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) ▼
 Channel: Channel 6, 2437MHz ▼

	Enable	Hide SSID	SSID	Isolate Member	Isolate VPN
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DrayTek	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	DrayTek_Guest	<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"/>

Note:
Enabling the Isolate Member configuration will forbid the wireless clients associated to the same SSID from connecting to each other.

The isolate VPN configuration will isolate the wireless traffic from VPN connections and thus, wireless clients will not be able to access the VPN network under this setting.

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:
Configurable upload and download rates are from 100 to 50,000(kbps).

Associated **Schedule** Profiles: , , ,

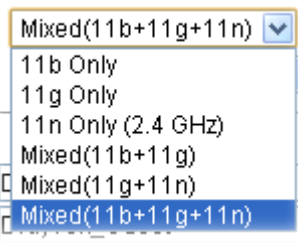
Note:
Only schedule profiles that have the action "Force Down" are applied to the WLAN, all other actions are ignored. Valid settings are profile indexes 1 to 15.

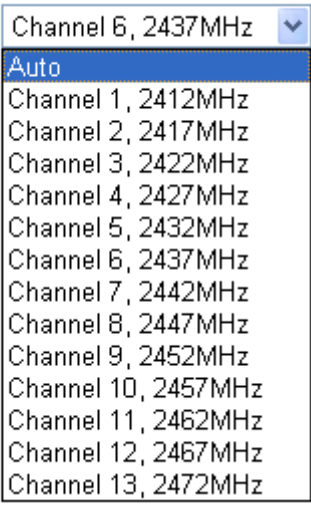
Note: Channel setting should not be changed while Wireless WAN mode is in use.

OK

Cancel

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, 11b Only, Mixed (11b+11g), Mixed (11g+11n), Mixed and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode. 
Channel	Means the channel of frequency of the wireless LAN. The

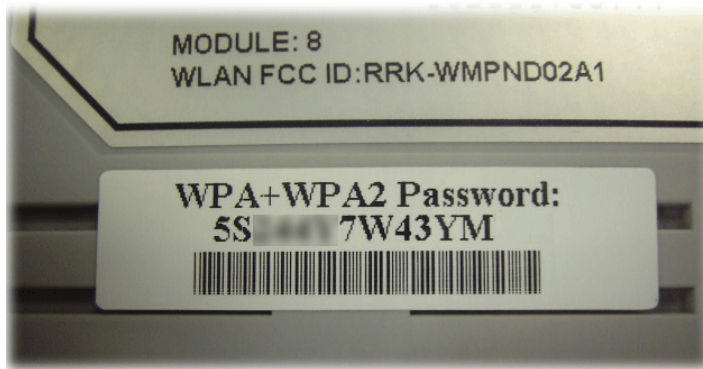
	<p>default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.</p> <p>Channel: </p>
Hide SSID	<p>Check it to prevent from wireless sniffing and make it harder for 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.</p>
SSID	<p>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.</p>
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>
Rate Control	<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>
Schedule	<p>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.</p>

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

3.13.3 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.



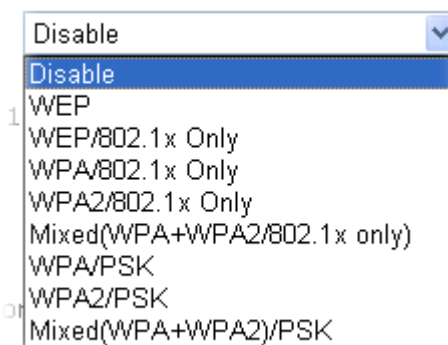
By clicking the **Security Settings**, a new web page will appear so that you could configure the settings of WPA and WEP.

Wireless LAN >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
<p>Mode: Mixed(WPA+WPA2)/PSK</p> <p><u>WPA</u></p> <p>Encryption Mode: TKIP for WPA/AES for WPA2</p> <p>Pre-Shared Key(PSK): *****</p> <p>Type 8~63 ASCII character or 64 Hexadecimal digits leading by "0x", for example "cfgs01a2..." or "0x655abcd....".</p> <p><u>WEP</u></p> <p>Encryption Mode: 64-Bit</p> <p><input checked="" type="radio"/> Key 1 : *****</p> <p><input type="radio"/> Key 2 : *****</p> <p><input type="radio"/> Key 3 : *****</p> <p><input type="radio"/> Key 4 : *****</p> <p>Note:</p> <p>Please configure the RADIUS Server if 802.1x is used.</p> <p>For 64 bit WEP key configurations, please insert 5 ASCII characters or 10 Hexadecimal digits leading by "0x". Examples are "AB312" or "0x4142333132".</p> <p>For 128 bit WEP key configurations, please insert 13 ASCII characters or 26 Hexadecimal digits leading by "0x".</p> <p>OK Cancel</p>			

Available settings are explained as follows:

Item	Description
Mode	There are several modes provided for you to choose.



Note: You should also set **RADIUS Server** simultaneously if 802.1x mode is selected.

Disable - Turn off the encryption mechanism.

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

WEP/802.1x Only - Accepts only WEP clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.

WPA/802.1x Only- Accepts only WPA clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.

WPA2/802.1x Only- Accepts only WPA2 clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.

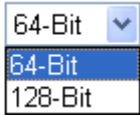
Mixed (WPA+WPA2/802.1x only) - Accepts WPA and WPA2 clients simultaneously and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.

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

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

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

WPA	<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 as "0x321253abcde...").</p>
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.

3.13.4 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

Add

Delete

Edit

Cancel

OK

Clear All

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.

3.13.5 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.



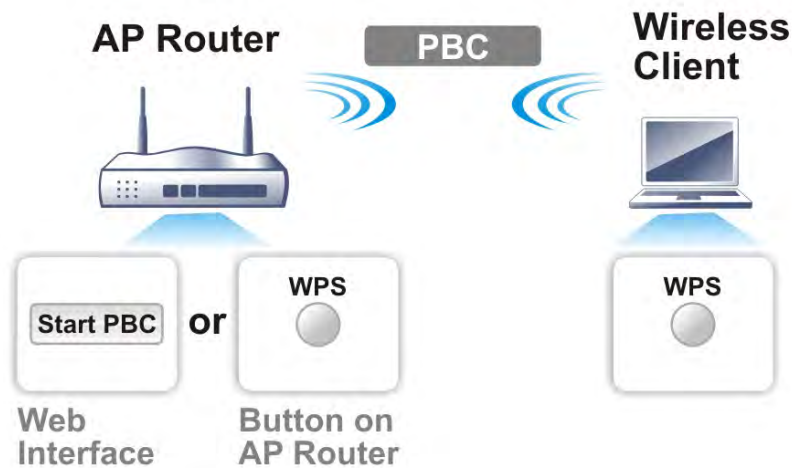
Note: Such function is available for the wireless station with WPS supported.

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.

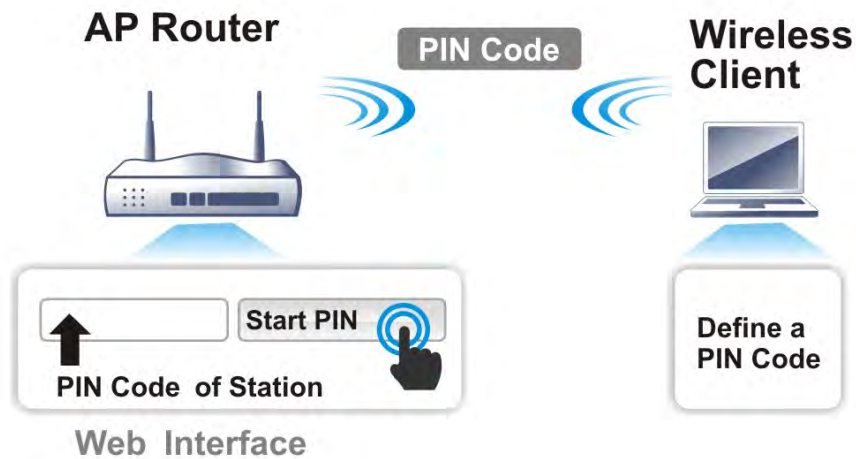
There are two methods to do network connection through WPS between AP and Stations: pressing the **Start PBC** button or using **PIN Code**.

- On the side of Vigor 2830 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

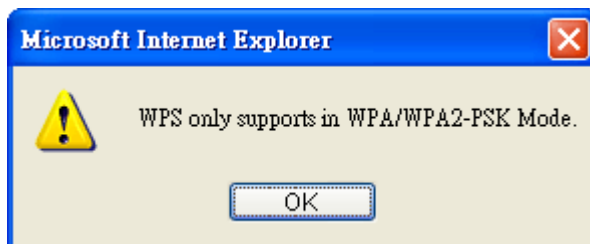
of a station with network card installed, press **Start PBC** button of network card.



- 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)

3.13.6 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:

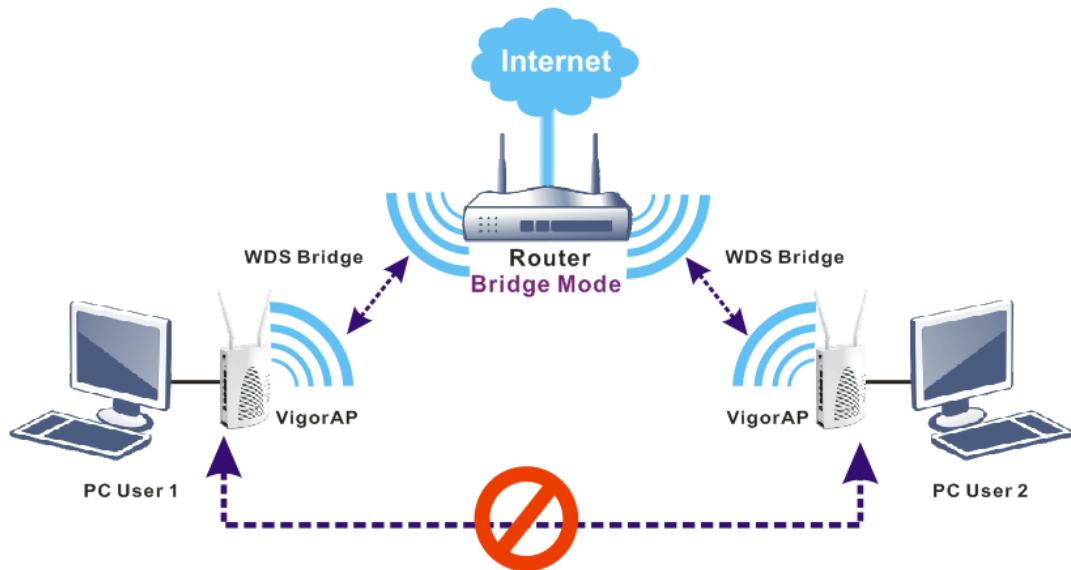
- Provide bridge traffic between two LANs through the air.
- Extend the coverage range of a WLAN.

Refer to the following table:

WDS Mode	Wireless Signal	Comparisons
Bridge	Limited	<ul style="list-style-type: none">● Wireless stations (clients) within the effective range of wireless signal can access into Internet through the router /AP.● Wireless stations (clients) out of the effective range of wireless signal cannot access into Internet through the router /AP with Bridge mode configured.● The packets received from a WDS link will only be forwarded to local wired or wireless hosts.
Repeater	Extended	<ul style="list-style-type: none">● Wireless stations (clients) within the effective range of wireless signal can access into Internet through the router /AP.● Wireless stations (clients) out of the effective range of wireless signal can access into Internet through the router /AP with Repeater mode configured.● The packets received from one Vigor router can be repeated to another AP (remotely) through WDS links.● Only Repeater mode can do WDS-to-WDS packet forwarding.

Bridge Mode

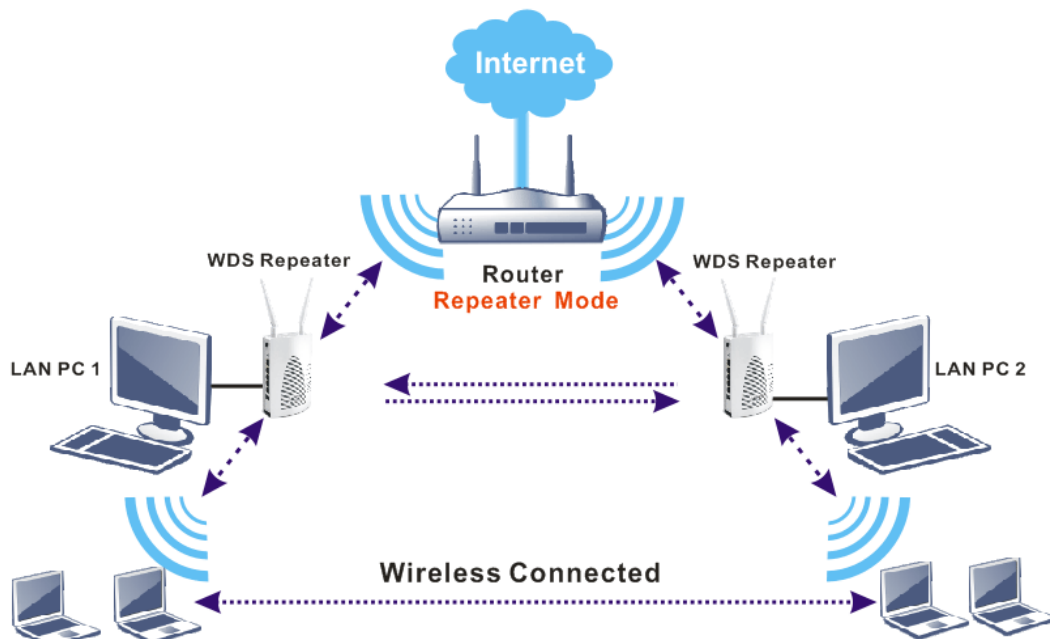
Vigor routers (and / or Vigor APs) with WDS Bridge link established can communicate with each other. Wireless stations (clients) within the effective range of wireless signal can access into Internet through the router /AP. However, PC users under VigorAPs without WDS Bridge link established cannot communicate with each other (refer to the following figure, PC User 1 and PC Users 2).



Repeater Mode

Vigor routers (and / or Vigor APs) with WDS Repeater link established can communicate with each other, and communicate with wireless stations (clients) due to the coverage range of a wireless connection extended.

The wireless signal from the root router (AP) **can be received and extended** by other router (AP), therefore the coverage range of wireless signal can be expanded which is convenient for remote wireless stations which require to access Internet via the Vigor router (AP).



To configure the WDS web page settings, open **Wireless LAN>>WDS** to get the following page:

WDS Settings
[Set to Factory Default](#)

<p>Mode: Bridge</p> <hr/> <p>Security:</p> <p> <input checked="" type="radio"/> Disable <input type="radio"/> WEP <input type="radio"/> Pre-shared Key </p> <hr/> <p>WEP:</p> <p>Use the same WEP key set in Security Settings.</p> <hr/> <p>Pre-shared Key:</p> <p>Type:</p> <p> <input type="radio"/> WPA <input checked="" type="radio"/> WPA2 </p> <p>Key : *****</p> <p>Note: WPA and WPA2 are not compatible with DrayTek WPA.</p> <p>Type 8~63 ASCII characters or 64 hexadecimal digits leading by "0x", for example "cfs01a2..." or "0x655abcd....".</p>	<p>Bridge</p> <p>Enable <input type="checkbox"/></p> <p>Peer MAC Address</p> <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td></tr> </table> <p>Note: Disable unused links to get better performance.</p> <hr/> <p>Repeater</p> <p>Enable <input type="checkbox"/></p> <p>Peer MAC Address</p> <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td></tr> </table> <hr/> <p>Access Point Function:</p> <p> <input checked="" type="radio"/> Enable <input type="radio"/> Disable </p> <hr/> <p>Status:</p> <p><input type="checkbox"/> Send "Hello" message to peers.</p> <p style="text-align: center;">Link Status</p> <p>Note: The status is valid only when the peer also supports this function.</p>																																																

Note: Channel Bandwidth will affect the connection of WDS. If failed, please check [Channel Bandwidth](#) setting.

OK
Cancel

Available settings are explained as follows:

Item	Description
Mode	<p>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.</p> <div style="border: 1px solid black; padding: 5px; width: fit-content;"> Disable <div style="border: 1px solid black; padding: 2px;"> Disable Bridge Repeater </div> </div>
Security	<p>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.</p>
WEP	<p>When WEP is selected as Security above, Vigor router will use the same WEP key set in Wireless LAN>>Security Settings page.</p> <p>All you have to do is to make sure WEP mode and WEP key setting have been configured properly in Wireless LAN>>Security Settings.</p> <p>Note: If Security mode configured in Wireless LAN>>Security Settings page is not the same as the security mode set here, a warning message will appear and</p>

	ask you to make the same configuration.
Pre-shared Key	<p>When Pre-Shared Key is selected as Security above, configure the following settings if required.</p> <p>Type – There are some types for you to choose. WPA and WPA2 are used for WDS devices (e.g. 2925n 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 – Set the encryption key in this field. Type 8 ~ 63 ASCII characters or 64 hexadecimal digits leading by “0x”.</p>
Bridge	<p>If you choose Bridge as the connecting mode, please type in the peer MAC address (of VigorAP/Vigor router required to make connection with such Vigor router) in these fields.</p> <p>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.</p>
Repeater	<p>If you choose Repeater as the connecting mode, please type in the peer MAC address (of VigorAP/Vigor router required to make connection with such Vigor router and used to extend the wireless signal) in these fields.</p> <p>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.</p>
Access Point Function	Click Enable to make this router serve as an access point.
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.

3.13.7 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

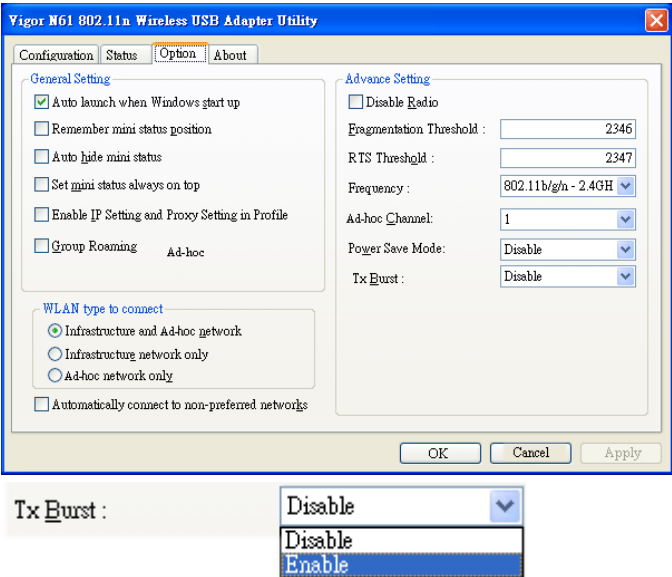
HT Physical Mode

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 <input type="radio"/> 40
Guard Interval	<input type="radio"/> long <input checked="" type="radio"/> auto
Aggregation MSDU(A-MSDU)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Long Preamble	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Packet-OVERDRIVE™ TX Burst	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Antenna	<input checked="" type="radio"/> 2T2R <input type="radio"/> 1T1R
Tx Power	<input checked="" type="radio"/> 100% <input type="radio"/> 80% <input type="radio"/> 60% <input type="radio"/> 30% <input type="radio"/> 20% <input type="radio"/> 10%
WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Rate Adaptation Algorithm	<input checked="" type="radio"/> New <input type="radio"/> Old
Fragment Length (256 - 2346)	<input type="text" value="2346"/> bytes
RTS Threshold (1 - 2347)	<input type="text" value="2347"/> bytes

OK

Available settings are explained as follows:

Item	Description
Operation Mode	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. 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.
Channel Bandwidth	20- the router will use 20Mhz for data transmission and receiving between the AP and the stations. 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.
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 .
Long Preamble	This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b

	<p>wireless network devices only support long preamble. Click Enable to use Long Preamble if needed to communicate with this kind of devices.</p>
Packet-OVERDRIVE	<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>
Antenna	<p>Vigor router can be attached with two antennas to have good data transmission via wireless connection. However, if you have only one antenna attached, please choose 1T1R.</p>
TX Power	<p>Set the power percentage for transmission signal of access point. The greater the value is, the higher intensity of the signal will be.</p>
WMM Capable	<p>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.</p> <p>To apply WMM parameters for wireless data transmission, please click the Enable radio button.</p>
APSD Capable	<p>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</p>

	by minimizing transmission latency. The default setting is Disable .
Rate Adaptation Algorithm	Wireless transmission rate is adapted dynamically. Usually, performance of “new” algorithm is better than “old”.
Fragment Length (256 – 2346)	Set the Fragment threshold. Do not modify default value if you don’t know what it is, default value is 2346.
RTS Threshold (1 – 2347)	Minimize the collision (unit is bytes) between hidden stations to improve wireless performance. Set the RTS threshold. Do not modify default value if you don’t know what it is, default value is 2347.

3.13.8 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	<p>It displays the statistics for the channels used by APs.</p> <p>Wireless LAN >> Site Survey Statistics</p> <div><p>Recommended channels for usage: 1 2 3 4 5 6 7 8 9 10 11 12 13</p><div><p>AP number v.s. Channel</p><table><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td></tr></table></div><p>Channel</p><p>Cancel</p></div>															1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	2	3	4	5	6	7	8	9	10	11	12	13	14																
Add to	<p>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.</p>																												

3.13.9 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

GeneralAdvanced

Index	Status	MAC Address	Associated with
-------	--------	-------------	-----------------

Refresh

Status Codes :
C: Connected, No encryption.
E: Connected, WEP.
P: Connected, WPA.
A: Connected, WPA2.
B: Blocked by Access Control.
N: Connecting.
F: Fail to pass WPA/PSK authentication.

Add to Access Control :

Client's MAC address : : : : :

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

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 .

3.14 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.



3.14.1 General Setup

This page determines the general configuration for SSL VPN Server and SSL Tunnel.

[Web Access Control >> General Setup](#)

SSL VPN General Setup

Bind to WAN	<input checked="" type="checkbox"/> WAN1 <input checked="" type="checkbox"/> WAN2 <input checked="" type="checkbox"/> WAN3
Port	<input type="text" value="443"/> (Default: 443)
Server Certificate	<input type="text" value="self-signed"/>

Note: The settings will act on all SSL applications.

Please go to [System Maintenance >> Management](#) to enable SSLv3.0 .

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.

3.14.2 SSL Web Proxy

SSL Web Proxy will allow the remote users to access the internal web sites over SSL.

[Web Access Control >> 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

Each item is 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.

[Web Access Control >> SSL Web Proxy](#)

Profile Index : 1

Name	<input type="text"/>
URL	<input type="text"/>
Host IP Address	<input type="text"/>
Access Method	<div>SSL Disable Secured Port Redirection SSL</div>

Note:

1. URL format must be entered as `http://[IP address]/[Port]/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. The length of the name is limited to 15 characters.
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 field. 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.

3.14.3 SSL Application

It provides a secure and flexible solution for network resources, including VNC (Virtual Network Computer) /RDP (Remote Desktop Protocol) to any remote user with access to Internet and a web browser.

Web Access Control >> SSL Application

SSL Applications Profiles:				Set to Factory Default
Index	Name	Host Address	Service	Active
1.				×
2.				×
3.				×
4.				×
5.				×
6.				×
7.				×
8.				×
9.				×
10.				×

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 path.
Service	Display the type of the service selected, e.g., VNC/RDP.
Active	Display current status (active or inactive) of the selected profile.

To create a new SSL application profile:

1. Click number link under Index field to set detailed configuration.

Web Access Control >> SSL Application

SSL Applications Profiles:

Index	Name	
1.		
2.		
3.		

2. The following page will appear.

Web Access Control >> SSL Application

Profile Index : 1

☐ Enable Application Service

Application Name

Application

Remote Desktop Protocol (RDP)
 ---Please Select---
 Virtual Network Computing (VNC)
 Remote Desktop Protocol (RDP)
 SMB Application

IP Address

Port

Screen Size

OK

Clear

Cancel

Available settings are explained as follows:

Item	Description
Enable Application Server	Check the box to enable such profile.
Application Name	Type a name for such application. The length of the name is limited to 23 characters.
Application	<p>There are three types offered for you to create an application profile.</p> <p>Virtual Network Computing (VNC) – It allows you to access and control a remote PC through VNC protocol.</p> <p>Remote Desktop Protocol (RDP) – It allows you to access and control a remote PC through RDP protocol.</p> <p>SMB Application – It allows you to access and control a remote PC through SMB service.</p>
IP Address	If you choose VNC or RDP, you have to type the IP address for this protocol.
Port	If you choose VNC or RDP, you have to specify the port used for this protocol. The default setting is 5900.
Idle Timeout	If you choose VNC, you have to specify the time for disconnecting the SSL VPN tunnel.
Scaling	If you choose VNC, you have to choose the percentage (100%, 80%, 60%) for such application.
Screen Size	If you choose RDP, you have to choose the screen size for such application.

SMB Path	If you choose SMB, you have to specify the path of the SMB service.
-----------------	---

3. Enter the required information.
4. After finished the above settings, click **OK** to save the configuration.

Web Access Control >> SSL Application

SSL Applications Profiles:

[Set to Factory Default](#)

Index	Name	Host Address	Service	Active
<u>1.</u>	VNC_1	192.168.1.54:5900	VNC	<input checked="" type="checkbox"/>
<u>2.</u>				<input type="checkbox"/>
<u>3.</u>				<input type="checkbox"/>
<u>4.</u>				<input type="checkbox"/>
<u>5.</u>				<input type="checkbox"/>

3.14.4 User Account

With SSL VPN, Vigor2830 series let teleworkers have convenient and simple remote access to central site VPN. The teleworkers do not need to install any VPN software manually. From regular web browser, you can establish VPN connection back to your main office even in a guest network or web cafe. The SSL technology is the same as the encryption that you use for secure web sites such as your online bank. The SSL VPN can be operated in either full tunnel mode or proxy mode. Now, Vigor2830 series allows up to 10 simultaneous incoming users.

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 will guide to access into **VPN and Remote Access>>Remote Dial-in user**.

Web Access Control >> Remote Dial-in User

Remote Access User Accounts:

[Set to Factory Default](#)

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"/>	---

Note: User Accounts need to be added into User Group to enable SSL Portal Login.

OK

Cancel

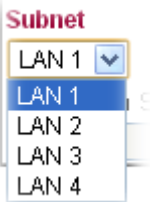
Click each index to edit one remote user profile.

Index No. 1

User account and Authentication <input type="checkbox"/> Enable this account Idle Timeout <input type="text" value="300"/> second(s)		Username <input type="text" value="???"/> Password(Max 19 char) <input type="text"/> <input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP) PIN Code <input type="text"/> Secret <input type="text"/>
Allowed Dial-In Type <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input checked="" type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/> <input type="button" value="v"/> <input checked="" type="checkbox"/> SSL Tunnel <input type="checkbox"/> Specify Remote Node Remote Client IP <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.)		IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key <input type="text" value="IKE Pre-Shared Key"/> <input type="checkbox"/> Digital Signature(X.509) <input type="text" value="None"/> <input type="button" value="v"/>
Subnet <input type="text" value="LAN 1"/> <input type="button" value="v"/> <input type="checkbox"/> Assign Static IP Address <input type="text" value="0.0.0.0"/>		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) <input type="text"/>

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. <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.,</p>

Item	Description
	<p>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) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node.

Item	Description
	<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.

3.14.5 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.

[Web Access Control >> 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
Set to Factory Default	Click to clear all indexes.
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.

[Web Access Control >> User Group](#)

Index No. 1

☐ Enable

Group Name

Access Authority

☐ SSL Web Proxy

☐ SSL Application

☐ VNC_1

Authentication Methods

☐ Local User DataBase

Available User Accounts

Selected User Accounts

☐ RADIUS

☐ LDAP / Active Directory

☐ rd1

☐ shrd

OK

Clear

Cancel

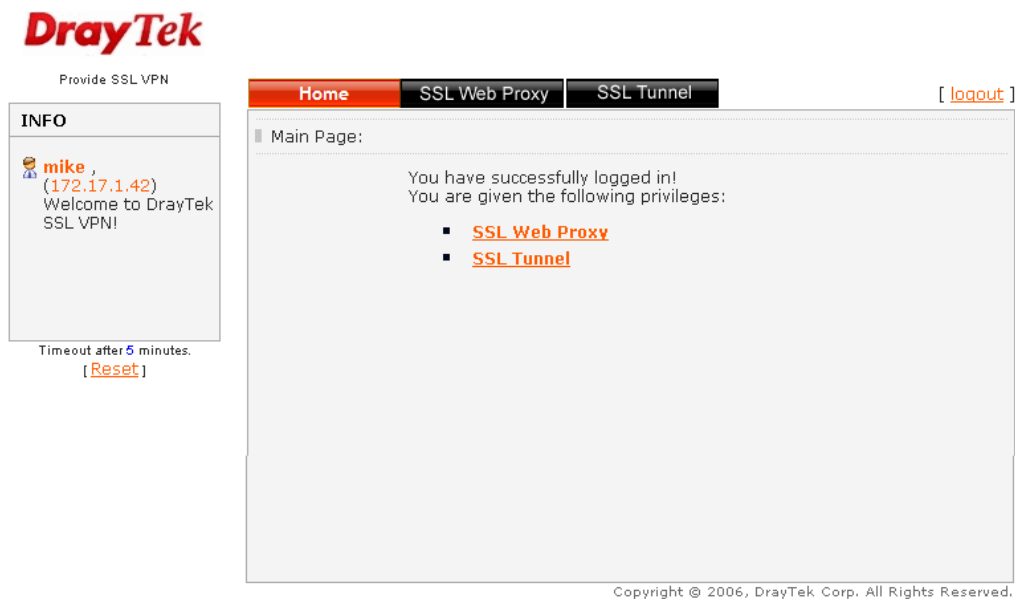
Available settings are explained as follows:

Item	Description
Enable	Check this box to enable such profile.
Group Name	Type a name for such profile. The length of the name is limited to 23 characters.
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> <div> <p>Access Authority</p> <div> <input checked="" type="checkbox"/> SSL Web Proxy <input checked="" type="checkbox"/> SSL Application <input type="checkbox"/> SSL_WP_1 <input type="checkbox"/> Game_APP </div> </div>
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.

3.14.6 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.



Next, users can open **SSL VPN>> Online Status** to view logging status of SSL VPN.

Web Access Control >> Online User Status

Refresh Seconds : <input type="text" value="10"/> <input type="button" value="refresh"/>			
Active User	Host IP	Time out(seconds)	Action
Kate	192.168.30.14	299	<input type="button" value="Drop"/>

Available settings are 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.

3.15 USB Application

USB storage disk connected on Vigor router can be regarded as a server. By way of Vigor router, clients on LAN can access, write and read data stored in USB storage disk 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 storage disk) or share the Samba service through Vigor router.



3.15.1 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

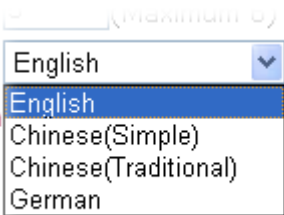
General Settings	
Simultaneous FTP Connections	5 (Maximum 6)
Default Charset	English
SMB File Sharing Service (Network Neighborhood)	
<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Access Mode	
<input checked="" type="radio"/> LAN Only <input type="radio"/> LAN And WAN	
NetBios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

Note: 1. If character set 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 has a multi-connection mechanism, such as FileZilla, you should limit client connections to 1 to improve performance.
3. A workgroup name must be different from the host name. The workgroup name can have up to 15 characters and the host name can have up to 15 characters. Names cannot contain any of the following: . ; : " < > * + = / \ | ?.

OK

Available settings are explained as follows:

Item	Description
General Settings	Simultaneous FTP Connections - This field is used to specify the quantity of the FTP sessions. The router allows up to 6 FTP sessions connecting to USB storage disk at one time.

	<p>Default Charset - At present, Vigor router supports four types of character sets. Default Charset is for English based file name.</p> 
SMB File Sharing Service	Click Enable to invoke SMB service (file sharing) via the router.
Access Mode	<p>LAN Only – Users coming from internet cannot connect to the SMB server of the router.</p> <p>LAN And WAN - Both LAN and WAN users can access SMB 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>
Printer Server	Enable – Click it to make Vigor router act as a printer server (with USB printer attached).

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

3.15.2 USB User Management


This page allows you to set profiles for FTP/Samba users. Any user who wants to access into the USB storage disk must type the same username and password configured in this page. Before adding or modifying settings in this page, please insert a USB storage disk 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.		

Click index number to access into configuration page.


Profile Index: 8

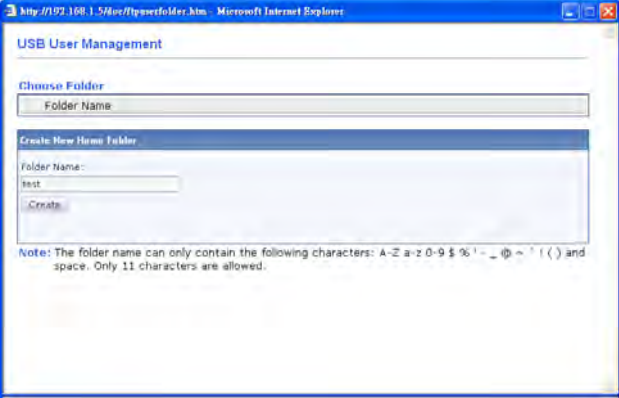
FTP/SMB User	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Username	<input type="text"/>
Password	<input type="text"/> (Maximum 11 Characters)
Confirm Password	<input type="text"/>
Home Folder	<input type="text"/> 
Access Rule	
File	<input type="checkbox"/> Read <input type="checkbox"/> 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.

OK Clear Cancel

Available settings are explained as follows:

Item	Description
FTP/SMB 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> <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. Please disable the mode on the FTP client.</p>
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	<p>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 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.

3.15.3 File Explorer

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

USB Application >> File Explorer

File Explorer



File Explorer interface showing the current path and file management options.

Current Path: /




Name	Size	Delete	Rename
------	------	--------	--------

Upload File

Select a file:

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 diskette can be shared for other user through FTP.

3.15.4 USB Device Status

This page is to monitor the status for the users who accessing into FTP or Samba server (USB storage disk) via the Vigor router. In addition, the status of the USB modem or USB printer connecting to Vigor router can be checked from such page. If you want to remove the storage disk from USB port in router, please click **Disconnect USB Disk** first. And then, remove the USB storage disk later.

[USB Application >> USB Device Status](#)

Disk	Modem	Printer	Refresh
-------------	--------------	----------------	-------------------------

USB Mass Storage Device Status

Connection Status: No Disk Connected [Disconnect USB Disk](#)

Disk Capacity: 0 MB

Free Capacity: 0 MB [Refresh](#)

USB Disk Users Connected

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.

Available settings are 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	It displays the total capacity of the USB storage disk.
Free Capacity	It displays the free space of the USB storage disk. Click Refresh at any time to get new status for free capacity.
Index	It displays the number of the client which connecting to FTP server.
IP Address	It displays the IP address of the user’s host which connecting to the FTP server.
Username	It displays the username that user uses to login to the FTP server.





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

3.15.5 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 test lists 3.5G/LTE modems **supported by Vigor router under certain environment or countries**. If the LTE modem you have is on the list but cannot work properly, please write an e-mail to support@draytek.com or consult your dealer for further information.

PPP mode	DHCP mode		
Brand	Model	LTE	Status
Aiko	Aiko 83D		Y
Alcatel	Alcatel L100V		Y
Alcatel	Alcatel W100		Y
BandRich	Bandlux C170		Y
BandRich	Bandlux C270		Y
BandRich	Bandlux C321		Y
BandRich	Bandlux C330		Y
BandRich	Bandlux C331		Y
BandRich	Bandlux C502		Y
Huawei	Huawei E169u		Y
Huawei	Huawei E220		Y
Huawei	Huawei E303D		Y
Huawei	Huawei E3131		Y
Huawei	Huawei E392		Y
Huawei	Huawei E398		Y
Huawei	Huawei K3772		Y
SpinCom	SpinCom GPRS Modem(2.5G)		Y
Sony Ericsson	Sony Ericsson MD300		Y
TP-LINK	TP-LINK MA180		Y

3.15.6 SMB Client Support List

SMB Client Support List provides the test status information for applications with file sharing operated under different platforms.

[USB Application >> SMB Client Support List](#)



The following compatibility test lists suggested SMB clients supported by Vigor router.

Platform	Application	Status
Microsoft® Windows® XP	Built in	I
Microsoft® Windows Vista™	Built in	Y
Microsoft® Windows® 7	Built in	Y
Microsoft® Windows® 8	Built in	M
Microsoft® Windows® 10	Built in	Y
OS X® 10.7.5	Built in	Y
OS X® 10.10	Built in	Y
Ubuntu 14.04	Built in	Y
Android™	AndSMB	Y
Android™	ES File Explorer	Y
Android™	File Expert	Y
Android™	File Manager	Y
Android™	Solid Explorer	Y
Android™	SharesFinder	Y
iOS	eXPlayer	Y
iOS	nPlayer	Y

Y: Tested and is supported.

I: Supported but has some issue.

M: Has not been tested but might be supported.

3.16 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: Status, TR-069, Admin Password, User Password, Login Page Greeting, Configuration Backup, Syslog/Mail Alert, Time and Date, SNMP, Management, Reboot System, Firmware Upgrade and Activation.

Below shows the menu items for System Maintenance.

USB Application
System Maintenance
▶ System Status
▶ TR-069
▶ Admin Setting
▶ User Password
▶ Login Page Greeting
▶ Configuration Backup
▶ SysLog / Mail Alert
▶ Time and Date
▶ SNMP
▶ Management
▶ Reboot System
▶ Firmware Upgrade
▶ Modem Code Upgrade
▶ Activation
Diagnostics

3.16.1 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 : Vigor2830n v2
Firmware Version : 3.8.1
Build Date/Time : Apr 11 2016 12:38:30

LAN					
	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-1D-AA-00-00-00	192.168.1.1	255.255.255.0	ON	8.8.8.8
LAN2	00-1D-AA-00-00-00	192.168.2.1	255.255.255.0	ON	8.8.8.8
LAN3	00-1D-AA-00-00-00	192.168.3.1	255.255.255.0	ON	8.8.8.8
LAN4	00-1D-AA-00-00-00	192.168.4.1	255.255.255.0	ON	8.8.8.8
IP Routed Subnet	00-1D-AA-00-00-00	192.168.0.1	255.255.255.0	ON	8.8.8.8

Wireless LAN			
MAC Address	Frequency Domain	Firmware Version	SSID
00-1D-AA-00-00-00	Europe	2.7.1.5	DrayTek

WAN					
	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Disconnected	00-1D-AA-00-00-01	PPPoE	---	---
WAN2	Disconnected	00-1D-AA-00-00-02	---	---	---
WAN3	Disconnected	00-1D-AA-00-00-03	---	---	---

IPv6			
	Address	Scope	Internet Access Mode
LAN	FE80::21D:AAFF:FE00:0/64	Link	---

User Mode is OFF now.

Available settings are 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	MAC Address - Display the MAC address of the LAN Interface. IP Address - Display the IP address of the LAN interface. Subnet Mask - Display the subnet mask address of the LAN interface. DHCP Server - Display the current status of DHCP server of the LAN interface DNS - Display the assigned IP address of the primary DNS.
Wireless LAN	MAC Address - Display the MAC address of the wireless LAN. Frequency Domain - It can be Europe (13 usable channels), USA (11 usable

	<p>channels) etc. The available channels supported by the wireless products in different countries are various.</p> <p>Firmware Version</p> <ul style="list-style-type: none"> - 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>SSID - Display the SSID of the router.</p>
WAN	<p>Link Status</p> <ul style="list-style-type: none"> - Display current connection status. <p>MAC Address</p> <ul style="list-style-type: none"> - Display the MAC address of the WAN Interface. <p>Connection</p> <ul style="list-style-type: none"> - Display the connection type. <p>IP Address</p> <ul style="list-style-type: none"> - Display the IP address of the WAN interface. <p>Default Gateway</p> <ul style="list-style-type: none"> - Display the assigned IP address of the default gateway.
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>

3.16.2 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"/> Wizard
Username	<input type="text"/>
Password	<input type="password"/>
	Test With Inform Event Code
	PERIODIC ▼
Last Inform Response Time :(NA) ●	
CPE Client	
<input checked="" type="radio"/> Disable	
<input type="radio"/> Enable	
<input checked="" type="radio"/> Http <input type="radio"/> Https	
URL	<input type="text"/>
Port	8069
Username	vigor
Password	<input type="password"/>

Periodic Inform Settings

<input checked="" type="radio"/> Disable	
<input 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)

Apply Settings to APs

<input checked="" type="radio"/> Disable	
<input type="radio"/> Enable	
AP Password	<input type="password"/>

OK Clear

Available settings 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>

CPE Client	<p>Such information is useful for Auto Configuration Server.</p> <p>Enable/Disable – Allow/Deny the CPE Client to connect with Auto Configuration Server.</p> <p>Port – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE.</p> <p>Username and Password – Type the username and password that VigorACS can use to access into such CPE.</p>
Periodic Inform Settings	<p>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.</p>
STUN Settings	<p>The default is Disable. If you click Enable, please type the relational settings listed below:</p> <p>Server IP – Type the IP address of the STUN server.</p> <p>Server Port – Type the port number of the STUN server.</p> <p>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”.</p> <p>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.</p>
Apply Settings to APs	<p>This feature is able to apply TR-069 settings (including STUN and ACS server settings) to all of APs managed by Vigor2830n at the same time.</p> <p>Disable – Related settings will not be applied to VigorAP.</p> <p>Enable – Above settings will be applied to VigorAP after clicking OK to save the configuration. If such feature is enabled, you have to type the password for accessing VigorAP.</p> <ul style="list-style-type: none"> ● AP Password – Type the password of the VigorAP that you want to apply Vigor2830n’s TR-069 settings.

3.16.3 Admin Setting

This page allows you to set new password.

[System Maintenance >> Admin Setting](#)

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 ; , . " < > * + = \ | ? @ # ^ ! ()

Administrator Local User

☐ Local User

Local User List

Index	User Name
-------	-----------

Specific User

User Name:

Password:

Confirm Password:

☒ Enable 'Admin' Login From Wan

Administrator LDAP Setting

☐ Enable LDAP/AD login for Admin users

☒ Enable 'Admin' Login From Wan

LDAP Server Profiles

[LDAP Profile Setup](#)

Note: Please select 'Admin' from group select box on login UI.

OK

Available settings are explained as follows:

Item	Description
Administrator Password	Old Password - Type in the old password. The factory default setting for password is “admin”. New Password -Type in new password in this field. The length of the password is limited to 23 characters. Confirm Password -Type in the new password again.
Administrator Local User	The administrator can login web user interface of Vigor router to modify all of the settings to fit the requirements. This feature allows other user in LAN who can access into the web user interface with the same privilege of the administrator. Local User – Check the box to enable the local user configuration. Local User List – It displays the username of the local user. User Name – Give a user name for the local user.

	<p>Password – Type the password for the local user.</p> <p>Confirm Password – Type the password again for confirmation.</p> <p>Add – After typing the user name and password above, simply click it to create a new local user. The new one will be shown on the Local User List immediately.</p> <p>Edit – If the username listed on the box above is not satisfied, simply click the username and modify it on the field of User Name. Later, click Edit to update the information.</p> <p>Delete – If the local user listed on the box above is not satisfied, simply click the username and click Delete to remove it.</p> <p>Enable Admin Login From Wan – The default setting is enabled. It can ensure any user accessing into web user interface of Vigor router through Internet by username/password of “admin/admin”.</p>
Administrator LDAP Setting	<p>Enable LDAP/AD login for Admin users – If it is enabled, any user can access into the web user interface of Vigor router through the LDAP server authentication.</p> <p>LDAP Server Profiles – Available profiles will be displayed here under the link of LDAP Profile Setup.</p> <p>LDAP Profile Setup – It allows you to create a new LDAP profile.</p>

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

3.16.4 User Password

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

System Maintenance >> User Password

☒ Enable User Mode for simple web configuration

User Password

[Set to Factory Default](#)

Password	<input type="text"/>	(Max. 23 characters allowed)
Confirm Password	<input type="text"/>	(Max. 23 characters allowed)

Note: 1.Password can contain a-z A-Z 0-9 , ; : . " < > * + = \ | ? @ # ^ ! ()
2.Password can't be all asterisks(*). For example, '*' or '****' is illegal, but '123*' or '*45' is OK.
3.To login as User, leave the Username field blank.

OK

Available settings are explained as follows:

Item	Description
Enable User Mode for simple web configuration	After checking this box, you can access into the web user interface with the password typed here for simple web configuration. The settings on simple web user interface will be different with full web user interface accessed by using the administrator password.
Password	Type in new password in this field.
Confirm Password	Type in the new password again.
Set to Factory Default	Click to return to the factory default setting.

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 , ; : . " < > * + = \ | ? @ # ^ ! ()

OK

3. The following screen will appear. Simply click **OK**.

System Maintenance >> User Password

Active Configuration

Password	: *****
----------	---------

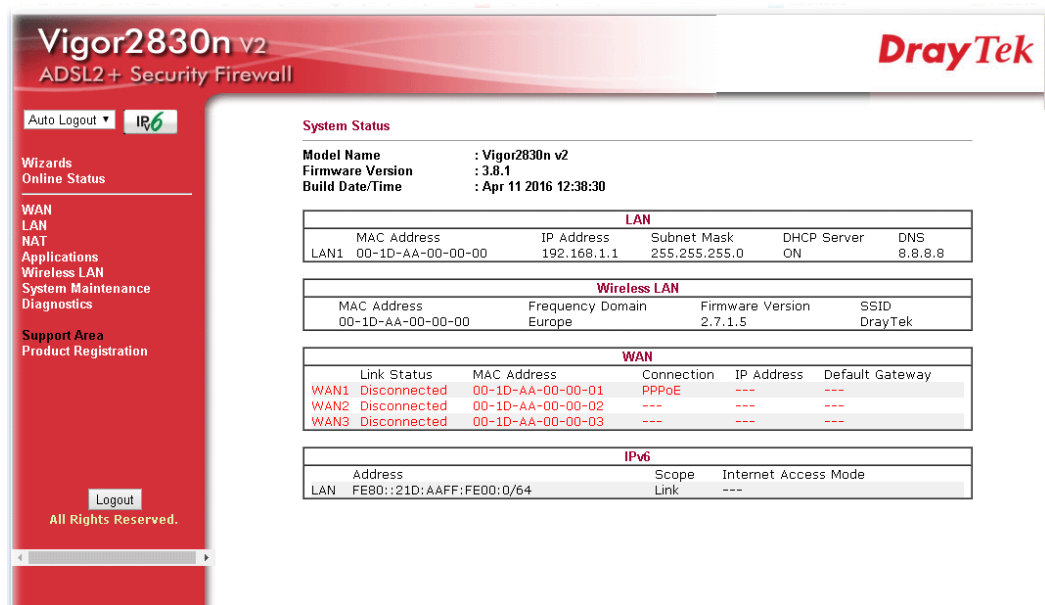
4. Log out Vigor router Web user interface.



5. The following window will be open to ask for username and password. Type the new user password in the field of **Password** and click **Login**.

A login window with a light gray background and rounded corners. It has two input fields: "Username" and "Password". The "Password" field is filled with black dots. To the right of the "Password" field is a "Login" button. At the bottom, there is a red banner with the text "Copyright©, DrayTek Corp. All Rights Reserved." and the "DrayTek" logo in white.

6. The main screen with User Mode will be shown as follows.



Vigor2830n v2
ADSL2+ Security Firewall

DrayTek

Auto Logout **IPv6**

Wizards
Online Status

WAN
LAN
NAT
Applications
Wireless LAN
System Maintenance
Diagnostics

Support Area
Product Registration

Logout
All Rights Reserved.

System Status

Model Name : Vigor2830n v2
Firmware Version : 3.8.1
Build Date/Time : Apr 11 2016 12:38:30

LAN					
	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-1D-AA-00-00-00	192.168.1.1	255.255.255.0	ON	8.8.8.8

Wireless LAN			
	MAC Address	Frequency Domain	Firmware Version
	00-1D-AA-00-00-00	Europe	2.7.1.5

WAN				
	Link Status	MAC Address	Connection	IP Address
WAN1	Disconnected	00-1D-AA-00-00-01	PPPoE	---
WAN2	Disconnected	00-1D-AA-00-00-02	---	---
WAN3	Disconnected	00-1D-AA-00-00-03	---	---

IPv6		
	Address	Scope
LAN	FE80::21D:AAFF:FE00:0/64	Link

Settings to be configured in User Mode will be less than settings in Admin Mode. Only basic configuration settings will be available in User Mode and can be configured as same as in Admin Mode.

3.16.5 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>Welcome Message</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.

Login for Test

Username

Password

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

Vigor:

This is an example of Bulletin feature of Vigor Routers

- 1. John, please pay your rent
- 2. Mary, please collect your electricity bill in the mailbox
- 3. Josh, couldn't manage to reach you but your parents were looking for you urgently

3.16.6 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

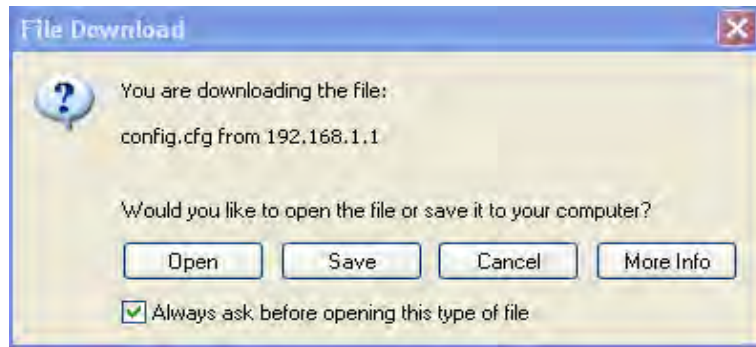
Click Backup to download current running configurations as a file.

Note: Configuration restoration from other models supported, but verification after restoration is recommended as it's not guaranteed that every setting will map across perfectly.

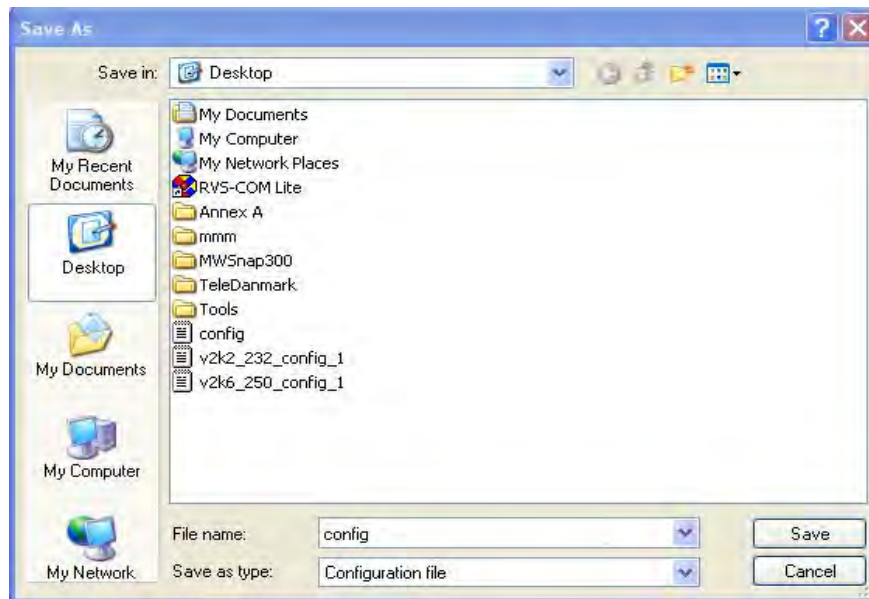
Support Model List

Model	Firmware Version
Vigor2830	3.6.6.2

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.

Configuration Backup / Restoration

<p>Restore</p> <p>Restore settings from a configuration file.</p> <p><input type="button" value="Select"/></p> <p>Click Restore to upload the file.</p> <p><input type="button" value="Restore"/></p>
<p>Backup</p> <p>Back up the current settings into a configuration file.</p> <p><input type="button" value="Backup"/></p>

Note: When loading a configuration file from a model in the Supported Model List please note that features and functionality can vary between models so please manually verify the settings after the restoration.

Supported Model List

Model	Firmware Version
Vigor2830	3.6.6.2

Available settings are explained as follows:

Item	Description
Restore	<p>Select – Click it to specify a file to be restored.</p> <p>Click Restore to restore the configuration. If the file is encrypted, the system will ask you to type the password to decrypt the configuration file.</p>
Backup	Click Backup to perform the configuration backup of this router.
Supported Model List	<p>Web configuration file from <i>other</i> Vigor router can be applied to Vigor2830n V2 series. At present, the configuration file of Vigor2830 is accepted for Vigor 2830n V2.</p> <p>This field displays model name(s) and firmware which web configuration file saved can be used by such router.</p>

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

3.16.7 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

SysLog Access Setup <input checked="" type="checkbox"/> Enable Syslog Save to: <input checked="" type="checkbox"/> Syslog Server <input type="checkbox"/> USB Disk Router Name <input type="text"/> Server IP Address <input type="text"/> Destination Port <input type="text" value="514"/> Mail Syslog <input type="checkbox"/> Enable Enable syslog message: <input checked="" type="checkbox"/> Firewall Log <input checked="" type="checkbox"/> VPN Log <input checked="" type="checkbox"/> User Access Log <input checked="" type="checkbox"/> Call Log <input checked="" type="checkbox"/> WAN Log <input checked="" type="checkbox"/> Router/DSL information AlertLog Setup <input type="checkbox"/> Enable AlertLog Port <input type="text" value="514"/>	Mail Alert Setup <input checked="" type="checkbox"/> Enable <input type="button" value="Send a test e-mail"/> SMTP Server <input type="text"/> SMTP Port <input type="text" value="25"/> Mail To <input type="text"/> Return-Path <input type="text"/> <input type="checkbox"/> Use SSL <input type="checkbox"/> Authentication Username <input type="text"/> Password <input type="text"/> Enable E-Mail Alert: <input checked="" type="checkbox"/> DoS Attack <input checked="" type="checkbox"/> IM-P2P <input checked="" type="checkbox"/> VPN LOG
---	--

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 settings are explained as follows:

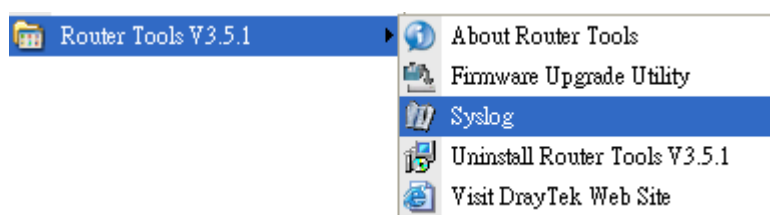
Item	Description
SysLog Access Setup	Enable - Check Enable to activate function of syslog. Syslog Save to – Check Syslog Server to save the log to Syslog server. Check USB Disk to save the log to the attached USB storage disk.
Router Name	Display the name for such router configured in System Maintenance>>Management . If there is no name here, simply lick the link to access into System Maintenance>>Management to set the router name. Server IP Address -The IP address of the Syslog server. Destination Port - Assign a port for the Syslog protocol. Mail Syslog – Check the box to recode the mail event on Syslog. Enable syslog message - Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to

	Syslog.
AlertLog Setup	<p>Check “Enable” to activate function of alert log.</p> <p>AlertLog Port - Type the port number for alert log. The default setting is 514.</p>
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 - The IP address 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>Authentication - Check this box to activate this function while using e-mail application.</p> <p>User Name - Type the user name for authentication.</p> <p>Password - Type the password for authentication.</p> <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>

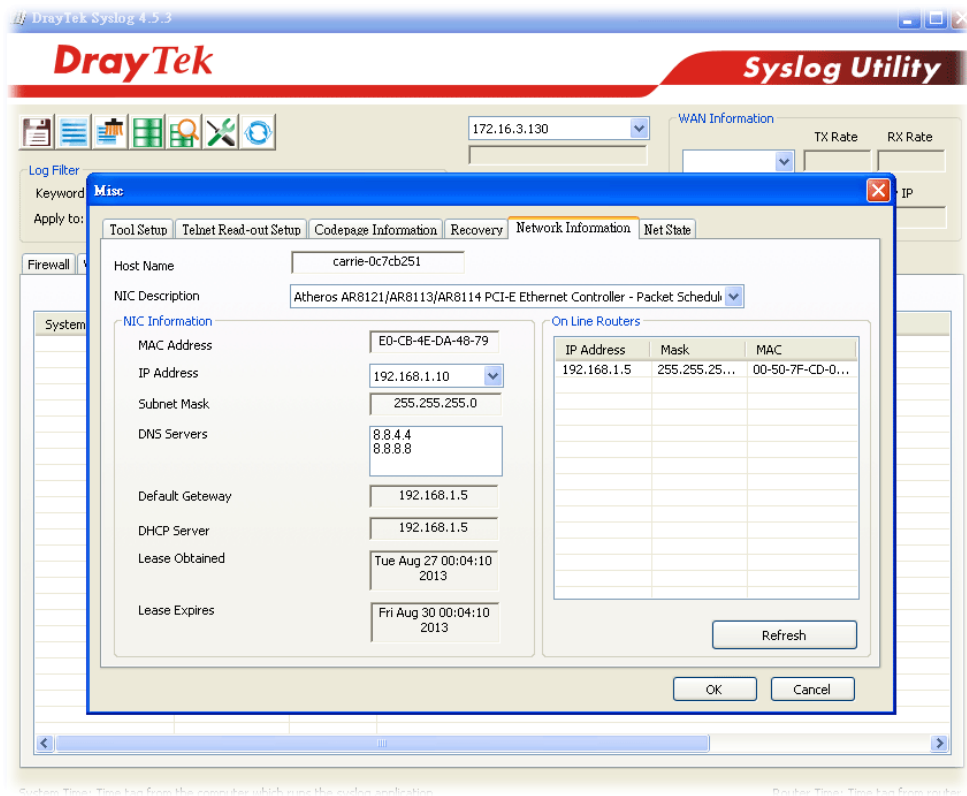
Click **OK** to save these settings.

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.



3.16.8 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 14 Fri 0 : 36 : 41	Inquire Time
---------------------	-----------------------------	---------------------

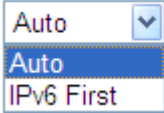
Time Setup

<input type="radio"/> Use Browser Time <input checked="" type="radio"/> Use Internet Time	
Time Server	pool.ntp.org
Priority	Auto
Time Zone	(GMT) Greenwich Mean Time : Dublin
Enable Daylight Saving	<input type="checkbox"/> Advanced
Automatically Update Interval	30 min

OK **Cancel**

Available settings are explained as follows:

Item	Description
Current System Time	Click Inquire Time to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the

	Internet using assigned protocol.
Time Server	Type the IP address of the time server.
Priority	<p>Choose Auto or IPv6 First 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> <div data-bbox="711 658 1394 990"> <p>Daylight Saving Advanced</p> <p><input checked="" type="radio"/> Default Start: No Daylight Saving End: No Daylight Saving</p> <p><input type="radio"/> Date Range Start: Year Month Day 00:00 End: Year Month Day 00:00</p> <p><input type="radio"/> Yearly Start: Yearly On Januai First Sunda 00:00 End: Yearly On Januai First Sunda 00:00</p> <p>OK Close</p> </div> <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.

3.16.9 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.

SNMP Setup

☒ Enable SNMP Agent

Get Community

Set Community

Manager Host IP(IPv4)	Index	IP	Subnet Mask
	1	<input type="text"/>	<input type="text" value="255.255.255.0"/>
	2	<input type="text"/>	<input type="text" value="255.255.255.0"/>
	3	<input type="text"/>	<input type="text" value="255.255.255.0"/>

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

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

☐ Enable SNMPV3 Agent

USM User

Auth Algorithm

Auth Password

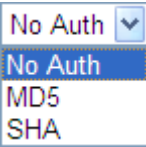
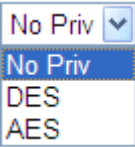
Privacy Algorithm

Privacy Password

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.

3.16.10 Management

This page allows you to manage the settings for Internet Access Control, Access List from the Internet, Management Port Setup, and External Device Control.

The management pages for IPv4 and IPv6 protocols are different.

For IPv4

System Maintenance >> Management



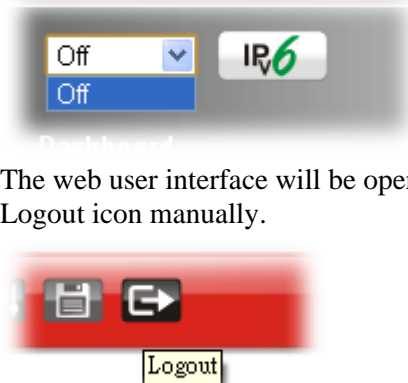
IPv4 Management Setup	IPv6 Management Setup
Router Name <input type="text"/>	
<input type="checkbox"/> Default: Disable Auto-Logout	
Internet Access Control	
<input type="checkbox"/> Allow management from the Internet	
Domain name allowed <input type="text"/>	
<input type="checkbox"/> FTP Server	
<input 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"/> IP Routed Subnet	
Access List from the Internet	
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"/> (Default: 23)
HTTP Port	<input type="text"/> (Default: 80)
HTTPS Port	<input type="text"/> (Default: 443)
FTP Port	<input type="text"/> (Default: 21)
TR069 Port	<input type="text"/> (Default: 8069)
SSH Port	<input type="text"/> (Default: 22)
TLS/SSL Encryption Setup	
<input type="checkbox"/> Enable SSL 3.0	
<input checked="" type="checkbox"/> Device Management	
<input type="checkbox"/> Respond to external device	

Note: Subnet LAN1 is always allowed to access all the router services regardless of "LAN Access Control" settings.

OK

Available settings are explained as follows:

Item	Description
Router Name	Type in the router name provided by ISP.
Default: Disable Auto-Logout	If it is enabled, the function of auto-logout for web user interface will be disabled.

	 <p>The web user interface will be open until you click the Logout icon manually.</p>
Internet Access Control	<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>
LAN Access Control	<p>Allow management from LAN - Enable the checkbox to allow system administrators to access from LAN. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.</p> <p>Apply To – Choose the subnet(s) for the administrator to access.</p>
Access List from the Internet	<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.</p> <p>Subnet Mask - Represent a subnet mask allowed to login to the router.</p>
Management Port Setup	<p>User Defined Ports - Check to specify user-defined port numbers for the Telnet, HTTP and FTP servers.</p> <p>Default Ports - Check to use standard port numbers for the Telnet and HTTP servers.</p>
TLS/SSL Encryption Setup	<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 Vigor2860.</p> <p>Respond to external device – If it is enabled, Vigor2860 will be regarded as slave device. When the external device</p>

(master device) sends request packet to Vigor2860, Vigor2860 would send back information to respond the request coming from the external device which is able to manage Vigor2860.

For IPv6

System Maintenance >> Management



IPv4 Management Setup	IPv6 Management Setup
Management Access Control <input type="checkbox"/> Allow management from the Internet <input type="checkbox"/> Telnet Server (Port : 23) <input type="checkbox"/> HTTP Server (Port : 80) <input type="checkbox"/> HTTPS Server (Port : 443) <input type="checkbox"/> SSH Server (Port : 22) <input checked="" type="checkbox"/> Disable PING from the Internet	
Access List List IPv6 Address / Prefix Length 1. <input type="text"/> / <input type="text"/> 2. <input type="text"/> / <input type="text"/> 3. <input type="text"/> / <input type="text"/> Note : Telnet / Http server port is the same as IPv4.	

OK

Available settings are explained as follows:

Item	Description
Management Access Control	Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify. Enable PING from the Internet - Check the checkbox to enable all PING packets from the Internet. For security issue, this function is disabled by default.
Access List	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed. IPv6 Address /Prefix Length - Indicate the IP address(es) allowed to login to the router.

3.16.11 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. Click **OK** to save the schedule setting.

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 5 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.

3.16.12 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](ftp://DrayTek.com).

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

System Maintenance >> Firmware Upgrade



Firmware Version Status

Current Firmware Version: 3.8.1

Check The Latest Firmware

Web Firmware Upgrade

Select a firmware file.

選擇檔案 未選擇任何檔案

Click Upgrade to upload the file.

Upgrade

TFTP Firmware Upgrade from LAN

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 ?

OK

Note: Upgrade using the ALL file will retain existing router configuration, whereas using the RST file will reset the configuration to factory defaults.

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.

3.16.13 Modem Code Upgrade

This function is used to upgrade modem code if you find built-in modem code is not suitable for Vigor router. Contact with your dealer for further assistance if required.

System Maintenance >> Modem Code Upgrade

Web DSL Modem Code Upgrade

Select a modem code file.

Select

Click Upgrade to upload the file.

Upgrade

3.16.14 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 2014-08-05 01:18:19

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 settings are explained as follows:

Item	Description
Activate via Interface	Choose WAN interface used by such device for activating Web Content Filter. <div style="text-align: right;"> Activate via interface : <div style="border: 1px solid black; padding: 2px; display: inline-block;"> auto-selected ▼ auto-selected WAN 1 WAN 2 WAN 3 </div> </div>
Activate	The Activate link brings you accessing into www.vigorpro.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: **2014-07-27** Expire Date: **2014-08-27**]

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.

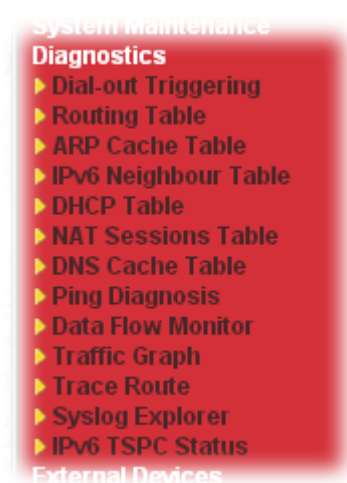
OK

Cancel

3.17 Diagnostics

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

Below shows the menu items for Diagnostics.



3.17.1 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

Decoded Format:

0.0.0.0 -> 0.0.0.0
Pr 0 len 0 (0)

Available settings are 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.

3.17.2 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	WAN2	
C~	192.168.1.0/ 255.255.255.0	directly connected	LAN1	
C	172.16.0.0/ 255.255.0.0	directly connected	WAN2	

or

[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	

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

3.17.3 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](#)

LAN

WAN

Show:

ALL LANs

 and

ALL VLANs

Ethernet ARP Cache Table

Clear

Refresh

IP Address	MAC Address	Netbios Name	Interface	VLAN	Port
192.168.1.5	00-05-5D-E4-D8-EE	A1000351	LAN1	---	P1

☐ Show Comment

Available settings are explained as follows:

Item	Description
Show	Specify LAN and VLAN to display related information. In default, this page will display all of the information about LAN and VLAN.
Clear	Click it to clear the whole table.
Refresh	Click it to reload the page.

3.17.4 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	

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

3.17.5 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	10:10:54.970	carrie-0c7cb251
2	192.168.1.1	00-1D-AA-00-00-00		

or

DHCP IP Assignment Table		DHCPv6 IP Assignment Table		Refresh
DHCPv6 server binding client:				
Index	IPv6 Address	MAC Address	Leased Time	

Each item is 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.

3.17.6 NAT Sessions Table

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

NAT Active Sessions Table						Refresh
Private IP	:Port	#Pseudo Port	Peer IP	:Port	Interface	
192.168.1.11	2491	52078	24.9.93.189	443	WAN1	
192.168.1.11	2493	52080	207.46.25.2	80	WAN1	
192.168.1.10	3079	52665	207.46.5.10	80	WAN1	

Available settings are 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.

3.17.7 DNS Cache Table

Click **Diagnostics** and click **DNS Cache Table** to pen 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)	
onead.onevision.com.tw	202.153.196.35	7679	
edm.contineomedia.com	103.244.8.140	11181	
mms.digitimes.com	122.255.90.181	10716	
reflexoptin.com	213.186.33.18	7482	
www.taipeitimes.com	61.63.34.204	10846	
www.ubot.com.tw	219.87.63.162	867	
shop-ze-deal.com	178.32.65.200	19459	
www.taca-subn.com	120.136.46.142	9726	
www.nlhs.tyc.edu.tw	203.68.75.51	14656	
nl-score.nlhs.tyc.edu.tw	203.68.75.17	19979	
www.mis.yzu.edu.tw	140.138.154.3	2755	
ml0-fr.com	178.32.13.203	10149	
www.ee.yzu.edu.tw	140.138.180.205	6077	
www.cse.yzu.edu.tw	140.138.144.1	441	
www.crc.yzu.edu.tw	140.138.181.217	1269	
www.comm.yzu.edu.tw	140.138.181.109	862	

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.

OK

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....	<p>Check the box the type the value of TTL (time to live) for each entry. Click OK to enable such function.</p> <p>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.</p>

3.17.8 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: Unspecified

Ping to: Host / IP IP Address:

Run

Result

Host / IP

DNS

Gateway 1

Gateway 2

Gateway 3

| Clear |

or

[Diagnostics >> Ping Diagnosis](#)

Ping Diagnosis

☐ IPV4 ☒ IPV6

Ping IPv6 Address:

Run

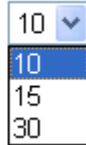
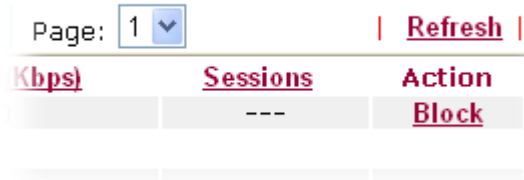

Result

| Clear |

Available settings are explained as follows:

Item	Description
IPV4 /IPV6	Choose the interface for such function.
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.

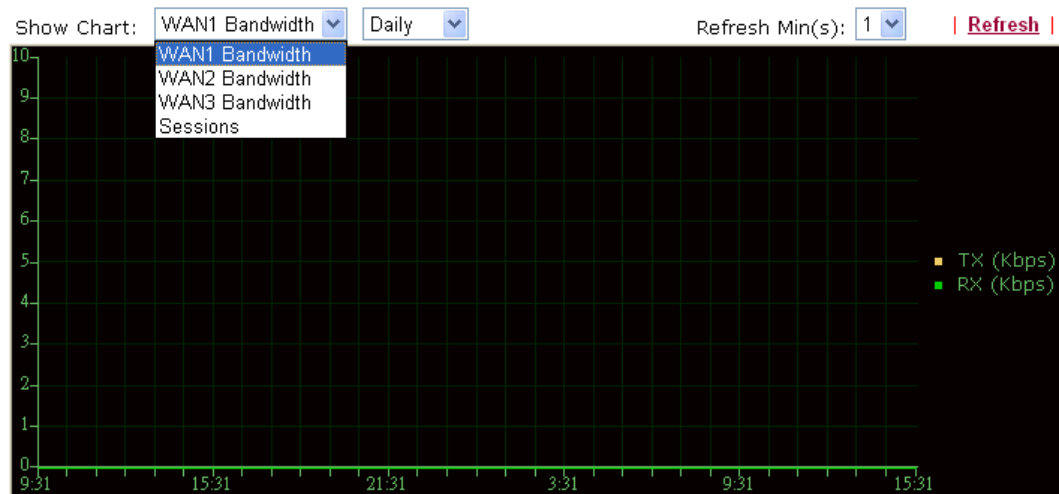
Available settings are explained as follows:

Item	Description
Enable Data Flow Monitor	Check this box to enable this function.
Refresh Seconds	<p>Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically.</p> <p>Refresh Seconds: </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> 
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>

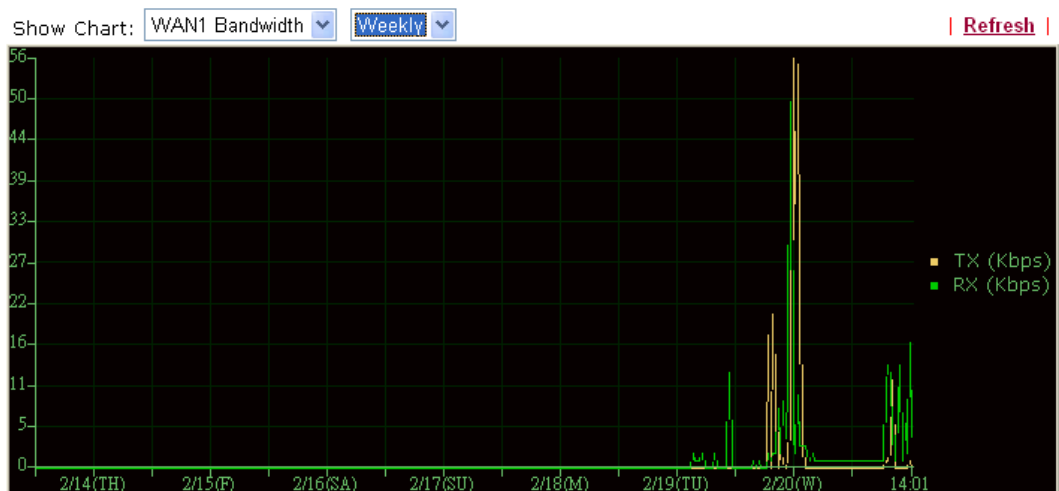
3.17.10 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to pen the web page. Choose WAN1/WAN2/WAN3 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. 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 Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

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

3.17.11 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](#)

or

[Diagnostics >> Trace Route](#)

Trace Route

☐ IPv4 ☒ IPv6

Trace Host / IP Address:

Result [Clear](#)

Available settings are explained as follows:

Item	Description
IPv4 / IPv6	Click one of them to display corresponding information for it.
Trace through	Use the drop down list to choose the 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.
Trace Host/IP Address	It indicates the IPv6 address of the host.
Run	Click this button to start route tracing work.
Clear	Click this link to remove the result on the window.

3.17.12 Syslog Explorer

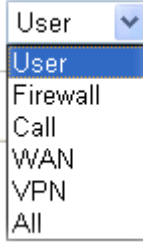
Such page provides real-time syslog and displays the information on the screen.

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.

[USB Application >> 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. 
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> <div>Stop record when fulls</div> <div>Stop record when fulls</div> <div>Always record the new event</div> </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.

[USB Application >> Syslog Explorer](#)

Web Syslog	USB Syslog
------------	------------

Folder: n/a	File: n/a	Page: n/a	Log Type: n/a
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.

3.17.13 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 >> TSPC Status

WAN1	WAN2	WAN3	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.

3.17.14 DoS Flood Table

This page can display content of IP connection detected by DoS Flooding Defense mechanism. It is useful and convenient for network engineers (e.g., MIS engineer) to inspect the network environment to find out if there is any abnormal connection.

Information of IP traced and destination port used for SYN Flood, UDP Flood and ICMP Flood attacks will be detected and shown respectively on different pages.

Moreover, IP address detected and suspected to attack the network system can be blocked shortly by clicking the **Block** button shown on pages of SYN Flood, UDP Flood and ICMP Flood.

Diagnostics >> DoS Flood Table

IPv4

SYN Flood

UDP Flood

ICMP Flood

Blocking IP List

| [Refresh](#) |

Tracing IP

Destination Port

IPv6

SYN Flood

UDP Flood

ICMP Flood

Blocking IP List

| [Refresh](#) |

Tracing IP

Destination Port

3.18 External Devices

This page allows you to enable or disable the function of detecting external devices.

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 properly. Click the **Clear** button to Clear the off-line information and account information.

OK

Available settings are explained as follows:

Item	Description
External Device Auto Discovery	Check this box to detect the external device automatically and display on this page.

This page is left blank.

4

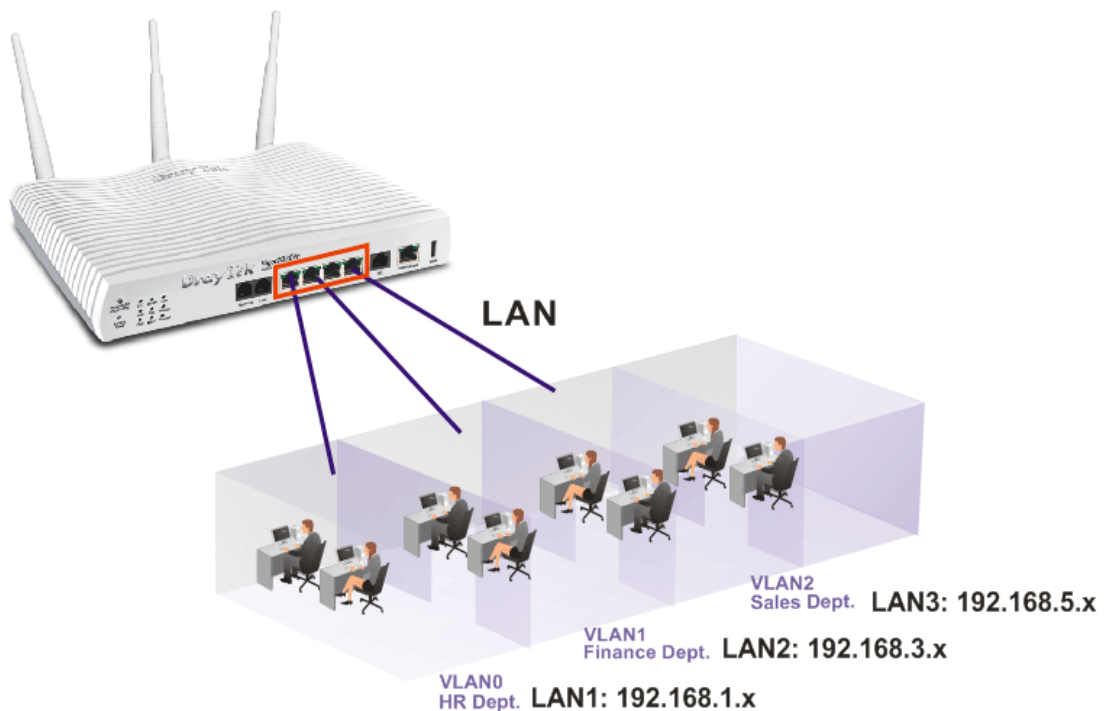
Application and Examples

4.1 How to Configure Multi-Subnet in Vigor2830

There are two types of VLAN. One is Port Based VLAN; the other is Tag Based VLAN. Refer to the following sections for learning the usage of VLAN.

I. Port Based VLAN

Vigor2830 can divide the physical LAN ports into several groups. For example, it can divide the internal departments of a company into three different groups. Each group uses different network segment. See the following graphic for an example.



Group 0 (VLAN0)(Human Resource): LAN Port 1 IP: 192.168.1.0/24

Group 1 (VLAN1)(Finance Dept): LAN Port 2 IP: 192.168.3.0/24

Group 2 (VLAN2)(Sales Dept.): LAN Port 3 、 Port 4 IP: 192.168.5.0/24

Configuration:

1. In the page of **LAN >> VLAN Configuration**, check the box of **Enable** to enable the function of VLAN Configuration.
2. For VLAN0 setting, check **P1** and set **LAN1** as the **Subnet**.
3. For VLAN1 setting, check **P2** and set **LAN2** as the **Subnet**.
4. For VLAN2 setting, check **P3** and **P4**, and set **LAN3** as the **Subnet**.

LAN >> VLAN Configuration

VLAN Configuration

☒ Enable

	LAN				Wireless LAN				Subnet	VLAN Tag		
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4		Enable	VID	Priority
VLAN0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 2	<input type="checkbox"/>	0	0
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 3	<input type="checkbox"/>	0	0
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0

☒ Permit untagged device in P1 to access router

1. Tag based VLAN only applied for LAN Ports;
2. The checked Wireless LAN SSID will not has VLAN tagging function but regarded as joining VLAN group;
3. The set VLAN ID (VID) must be unique and not duplicate.

OK Clear Cancel

5. In the page of **LAN >> General Setup**, check the **Status** box of LAN2 and LAN3 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	IPv6
LAN 2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.3.1	Details Page	
LAN 3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.5.1	Details Page	
LAN 4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.7.1	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

After finishing the above configuration, the equipment connecting to Vigor2830 LAN Port can get the corresponding IP address of the network segment.

The equipment connecting to Vigor2830 LAN Port 1 (LAN1) can get the IP address of 192.168.1.0/24

The equipment connecting to Vigor2830 LAN Port 2 (LAN2) can get the IP address of 192.168.3.0/24

The equipment connecting to Vigor2830 LAN Port 3 and Port 4 (LAN3) can get the IP address of 192.168.5.0/24

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	LAN 1 IPv6 Setup
Network Configuration For NAT Usage IP Address: <input type="text" value="192.168.1.1"/> Subnet Mask: <input type="text" value="255.255.255.0"/> RIP Protocol Control: <input type="button" value="Disable"/>	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="192.168.1.10"/> IP Pool Counts: <input type="text" value="200"/> Gateway IP Address: <input type="text" value="192.168.1.1"/> Lease Time: <input type="text" value="86400"/> (s) <input checked="" type="checkbox"/> Retrieve IPs from inactive clients periodically
DNS Server IP Address Primary IP Address: <input type="text"/> Secondary IP Address: <input type="text"/>	

OK

6. 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.

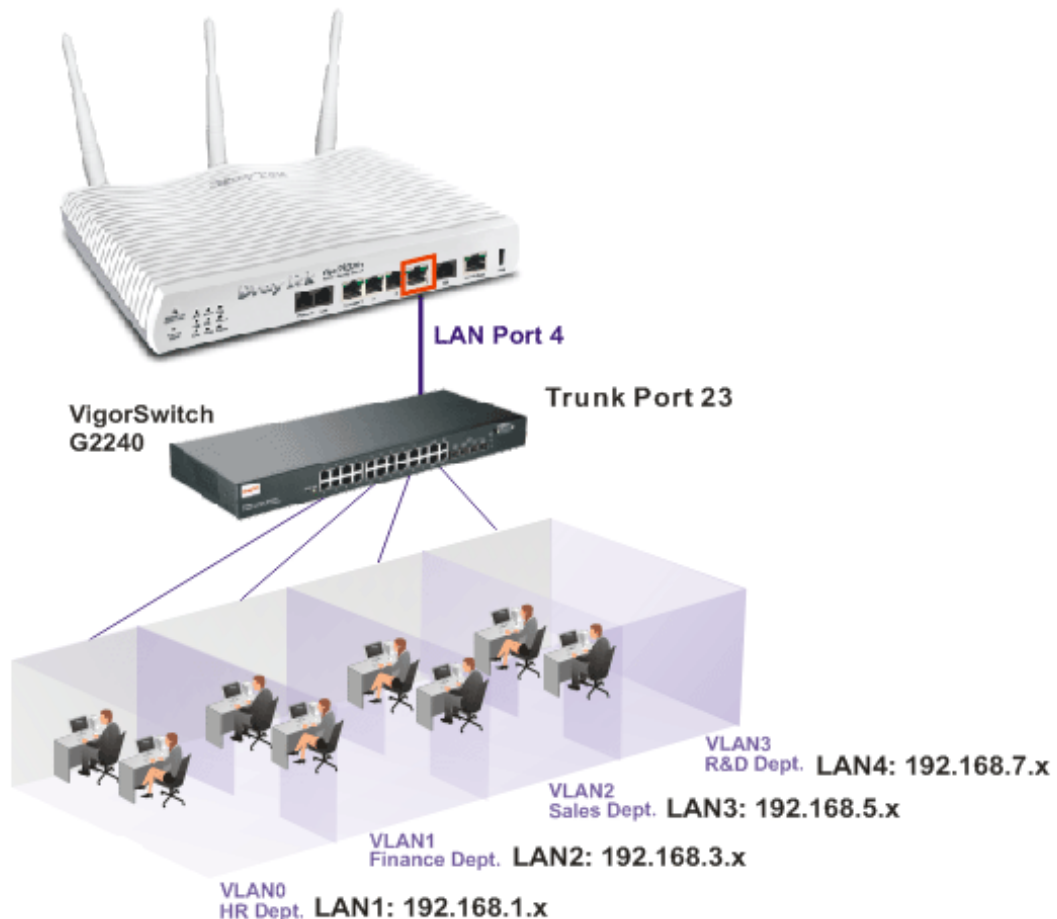
Inter-LAN Routing

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

II. Tag Based VLAN

By identifying the tagged message, Vigor2830 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, Vigor2830 can divide the internal departments of a company into four different groups by using VigorSwitch 2240. Each group uses different network segment and does not link for each other. VigorSwitch 2240 Trunk Port 23 and Vigor2830 LAN Port 4 are connected with network cable. See the following graphic for an example.



Group 0 (VLAN0)(Human Resource): LAN Port 4 IP: 192.168.1.0/24

Group 1 (VLAN1)(Finance Dept): LAN Port 4 IP: 192.168.3.0/24

Group 2 (VLAN2)(Sales Dept.): LAN Port 4 IP: 192.168.5.0/24

Group 3 (VLAN3)(R&D): LAN Port 4 IP: 192.168.7.0/24

Configuration for Vigor2830:

1. In the page of **LAN >> VLAN Configuration**, check the box of **Enable** to enable the function of VLAN Configuration.
2. To activate the function of VLAN Tag for VLAN0 setting, check the box of **Enable** and type the value (7) for VID setting. Then check **P4** and set **LAN1** as the **Subnet**.
3. To activate the function of VLAN Tag for VLAN1 setting, check the box of **Enable** and type the value (8) for VID setting. Then check **P4** and set **LAN2** as the **Subnet**.
4. To activate the function of VLAN Tag for VLAN2 setting, check the box of **Enable** and type the value (9) for VID setting. Then check **P4** and set **LAN3** as the **Subnet**.

5. To activate the function of VLAN Tag for VLAN3 setting, check the box of **Enable** and type the value (10) for VID setting. Then check **P4** and set **LAN4** as the **Subnet**.

LAN >> VLAN Configuration

VLAN Configuration

☒ Enable

	LAN				Wireless LAN				Subnet	VLAN Tag		
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4		Enable	VID	Priority
VLAN0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LAN 1	<input checked="" type="checkbox"/>	7	0
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 2	<input checked="" type="checkbox"/>	8	0
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 3	<input checked="" type="checkbox"/>	9	0
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 4	<input checked="" type="checkbox"/>	10	0
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0

☒ Permit untagged device in P1 to access router

1. Tag based VLAN only applied for LAN Ports;

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

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

OK

Clear

Cancel

6. In the page of **LAN >> General Setup**, check the **Status** box of LAN2, LAN3 and 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	IPv6
LAN 2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.3.1	Details Page	
LAN 3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.5.1	Details Page	
LAN 4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.7.1	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

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	LAN 1 IPv6 Setup
Network Configuration For NAT Usage IP Address: <input type="text" value="192.168.1.1"/> Subnet Mask: <input type="text" value="255.255.255.0"/> RIP Protocol Control: <input type="text" value="Disable"/>	
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="192.168.1.10"/> IP Pool Counts: <input type="text" value="200"/> Gateway IP Address: <input type="text" value="192.168.1.1"/> Lease Time: <input type="text" value="86400"/> (s) <input type="checkbox"/> Retrieve IPs from inactive clients periodically	
DNS Server IP Address Primary IP Address: <input type="text"/> Secondary IP Address: <input type="text"/>	

OK

Configuration for VigorSwitch 2240:

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

Tag-Based VLAN Memberships Configuration

Del	VID	IGMP-A	P-VLAN	GVRP-P	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	Disable	Disable	Disable	1																							24
	7	Disable	Disable	Disable															15								23	
	8	Disable	Disable	Disable															16								23	
	9	Disable	Disable	Disable																17							23	
	10	Disable	Disable	Disable																18							23	

VLAN Name 2830-VID7, Port Members = 15 、 23

VLAN Name 2830-VID8, Port Members = 16 、 23

VLAN Name 2830-VID9, Port Members = 17 、 23

VLAN Name 2830-VID10, Port Members = 18 、 23

3. Open **Vlan>> Ports** and set the VID value with role for each Port:

Port 15 VID = 7 Role = Access

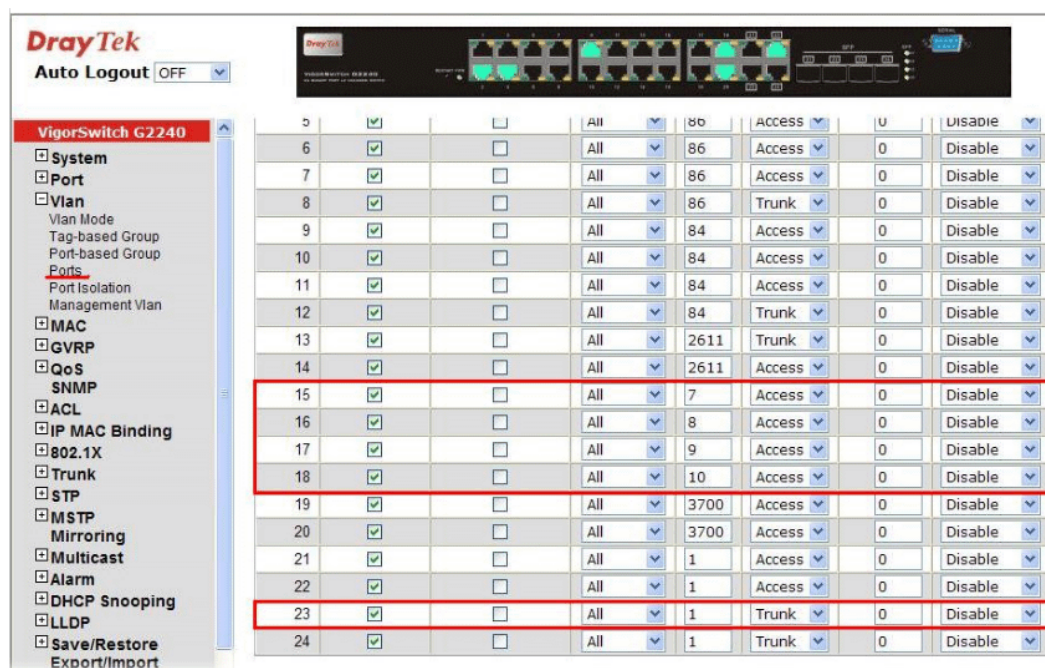
Port 16 VID = 8 Role = Access

Port 17 VID = 9 Role = Access

Port 18 VID = 10 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 7, 8, 9 and 10 will be transferred to Vigor2830 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 192.168.3.0/24

The equipment connecting to VigorSwitch Port 17 can get the IP address of 192.168.5.0/24

The equipment connecting to VigorSwitch Port 18 can get the IP address of 192.168.7.0/24

- To make any two of VLAN groups of Tag Based VLAN linked with each other, just check the boxes of the ones in the field of **Inter-LAN Routing** in the page of **LAN >> General Setup**. Refer to the following figure. LAN2 and LAN3 are linked.

Inter-LAN Routing

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

4.2 How Can I Use FTP to Get the Files from USB Storage Device Connecting to Vigor Router?

There are three methods to get files from USB devices connecting to router.

- File Explorer – Under Administration operation, the administrator can control the files on USB storage device through USB Application>>File Explorer.
- FTP – Use common FTP utility.

Files on USB storage device can be reviewed by opening **USB Application>>File Explorer**. Below shows the example of getting files from FTP:

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	

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

USB Application >> USB User Management

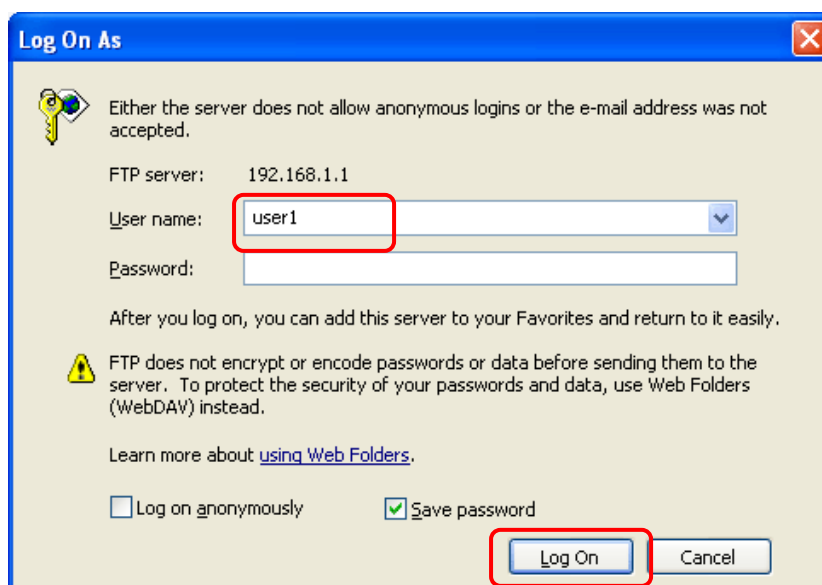
Profile Index: 1

FTP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	<input type="text" value="user1"/>
Password	<input type="password" value="....."/> (Maximum 11 Characters)
Confirm Password	<input type="password" value="....."/>
Home Folder	<input type="text"/>
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

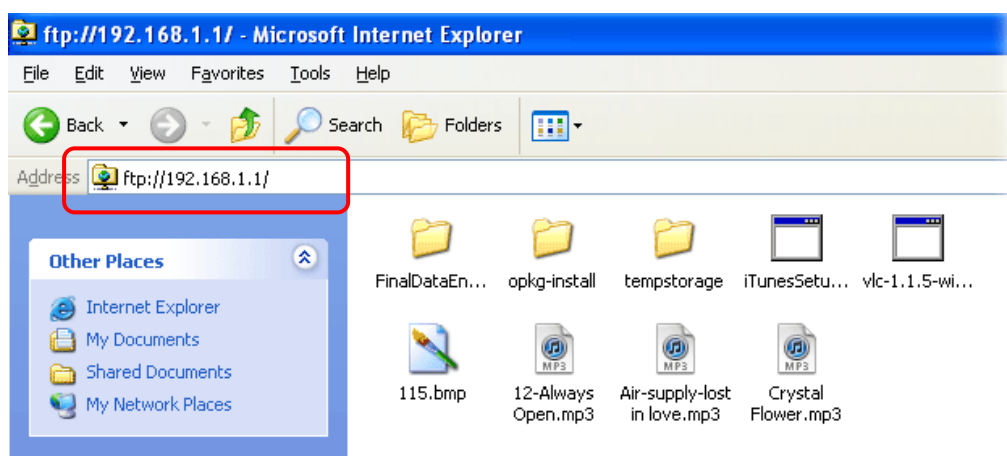
Note: The folder name can only contain the following characters: A-Z a-z 0-9 \$ % ' - _ @ ~ ` ! () / and space.

[OK](#) [Clear](#) [Cancel](#)

3. 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.



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



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

USB Application >> USB Disk Status

USB Mass Storage Device Status

Connection Status: **Disk Connected** Disconnect USB Disk

Write Protect Status: **No**

Disk Capacity: 2009 MB

Free Capacity: 0 MB [Refresh](#)

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

Index	Service	IP Address(Port)	Username
1.	FTP	192.168.1.10(1963)	user1 Drop

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

Now, users in LAN of Vigor2830 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**.

4.3 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection

Follow the steps listed below:

1. Log into the web user interface of Vigor router.
2. Configure relational objects first. Open **Object Settings>>SMS/Mail Server Object** to get the following page.

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			

Index 1 to Index 8 allows you to choose the built-in SMS service provider. If the SMS service provider is not on the list, you can configure Index 9 and Index 10 to add the new service provider to Vigor router.

3. Choose any index number (e.g., Index 1 in this case) to configure the SMS Provider setting. In the following page, type the username and password and set the quota that the router can send the message out.

Object Settings >> SMS / Mail Service Object

Profile Index: 1

Profile Name	<input type="text" value="Local number"/>
Service Provider	<input type="text" value="kotsms.com.tw (TW)"/>
Username	<input type="text" value="abc5026"/>
Password	<input type="password" value="..."/>
Quota	<input type="text" value="10"/>
Sending Interval	<input type="text" value="3"/> (seconds)

4. After finished the settings, click **OK** to return to previous page. Now you have finished the configuration of the SMS Provider profile setting.

Object Settings >> SMS / Mail Service Object

SMS Provider		Mail Server	Set to Factory Default	
Index	Profile Name	SMS Provider		
1.	Local Number	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			

5. Open **Object Settings>>Notification Object** to configure the event conditions of the notification.

Object Settings >> Notification Object

			Set to Factory Default	
Index	Profile Name	Settings		
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				

6. Choose any index number (e.g., Index 1 in this case) to configure conditions for sending the SMS. In the following page, type the name of the profile and check the Disconnected and Reconnected boxes for WAN to work in concert with the topic of this paper.

Object Settings >> Notification Object

Profile Index: 1

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

OK Clear
Cancel

- After finished the settings, click **OK** to return to previous page. You have finished the configuration of the notification object profile setting.

Object Settings >> Notification Object

Set to Factory Default		
Index	Profile Name	Settings
1.	WAN_Notify	WAN
2.		
3.		
4.		
5.		
6.		
7.		
8.		

- Now, open **Application >> SMS / Mail Alert Service**. Use the drop down list to choose SMS Provider and the Notify Profile (specify the time of sending SMS). Then, type the phone number in the field of Recipient (the one who will receive the SMS).

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 - Local Number	0912345678	1 - WAN_Notify		
2 <input type="checkbox"/>	1 - Local Number		1 - WAN_Notify		
3 <input type="checkbox"/>	1 - Local Number		1 - WAN_Notify		
4 <input type="checkbox"/>	1 - Local Number		1 - WAN_Notify		
5 <input type="checkbox"/>	1 - Local Number		1 - WAN_Notify		
6 <input type="checkbox"/>	1 - Local Number		1 - WAN_Notify		
7 <input type="checkbox"/>	1 - Local Number		1 - WAN_Notify		
8 <input type="checkbox"/>	1 - Local Number		1 - WAN_Notify		
9 <input type="checkbox"/>	1 - Local Number		1 - WAN_Notify		
10 <input type="checkbox"/>	1 - Local Number		1 - WAN_Notify		

OK
Cancel

- Click **OK** to save the settings. Later, if one of the WAN connections fails in your router, the system will send out SMS to the phone number specified. If the router has only one WAN interface, the system will send out SMS to the phone number while reconnecting the WAN interface successfully.

10. Configure the settings as the following figure. Choose one of the SMS profiles. In this example, the profile “For warning” is selected. Then, click **OK** to save the settings.

WAN >> General Setup

WAN 2

Enable: Yes ▾

Display Name:

Physical Mode: Ethernet

Physical Type: Auto negotiation ▾

Line Speed(Kbps):

DownLink

UpLink

VLAN Tag insertion : Disable ▾

Tag value: (0~4095)

Priority: (0~7)

Send **SMS** if line drops out 1-For warning ▾

Send **Mail Alert** if line drops out ☐

Active Mode: Backup ▾

☐ WAN 1 ☐ WAN 2 ☐ WAN 3

Backup Type

(Only if acting as backup for multiple WAN):

☒ When any of selected WAN disconnect

☐ When all of selected WAN disconnect

OK Cancel

When such WAN (e.g., WAN2 in this example) disconnects due to some reason, the system will use other WAN for connection instead and send SMS to notify the user (destination number #123456789). However, if there is no available WAN for connection, the system will send SMS to inform the user after reconnecting WAN2 successfully.

4.4 Web Portal Log-In Application for Wireless Client

With the increase of hotspot deployed via Wi-Fi technology in the world, we may easily get Internet connection with the served wireless connection facility provided by the campus, chain store, the coffee shop, the airport, department store, municipal...etc.. Such hotspot deployment contributes to seamless Internet connection which enables the remote workers or wireless users to get onto the cyber space anywhere at anytime.

In contrast to the real wireless user's advantage earn from hotspot, the Wi-Fi connection providers may also earn placement marketing advantage via Vigor2830n as offering wireless connection service at its hotspot. With the smart, easy configuration of WLAN on Vigor2830n, the free riders of Wi-Fi connection at hotspot would be automatically directed to dedicated web site. In a department store with Vigor2830n deployed, the mobile users will be directed to its own company web site or dedicated special promotion program web page as firstly get wireless connection to the Internet. The Internet surfers would have a glance at least on the dedicated web site and related contents.

Direct Marketing via Web Portal Log-in



Wireless General Setup

1. From Vigor router web configuration page, select **Wireless LAN>>General Setup**.
2. Check **Enable Wireless LAN** and set the SSID. Then click **OK** to save the settings.

Vigor2830 Series
ADSL2+ Security Firewall

Wireless LAN >> General Setup

General Setting (IEEE 802.11)

☒ Enable Wireless LAN

Mode: Mixed(11b+11g+11n)

Channel: Channel 6, 2437MHz

Enable	Hide	SSID	Isolate Member	Isolate VPN
<input type="checkbox"/>	<input type="checkbox"/>	DrayTek	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	DrayTek_Guest	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>

Wireless Portal Log-in Setting

1. Open **LAN>>Web Portal Setup**.
2. Click **Redirect to URL** and type the URL in the field below. User's first HTTP request will be redirected to the URL defined here. (Here we take www.draytek.com for an example.)

LAN >> Web Portal Setup

Profile Index: 1

Profile Index: 1

☐ Disable

☒ URL Redirect

☐ Message

Applied Interfaces

www.draytek.com

e.g. http://www.draytek.com

Note : If the User Management application is enabled, it will override the Web Portal settings seen here.

<h1>Vigor</h1><h2> - Reliable connectivity</h2><h2> - Robust firewall protection</h2><h2> - Multi-site secure communication</h2>

(Max 255 characters)

☐ LAN1 ☐ LAN2 ☐ LAN3 ☐ LAN4

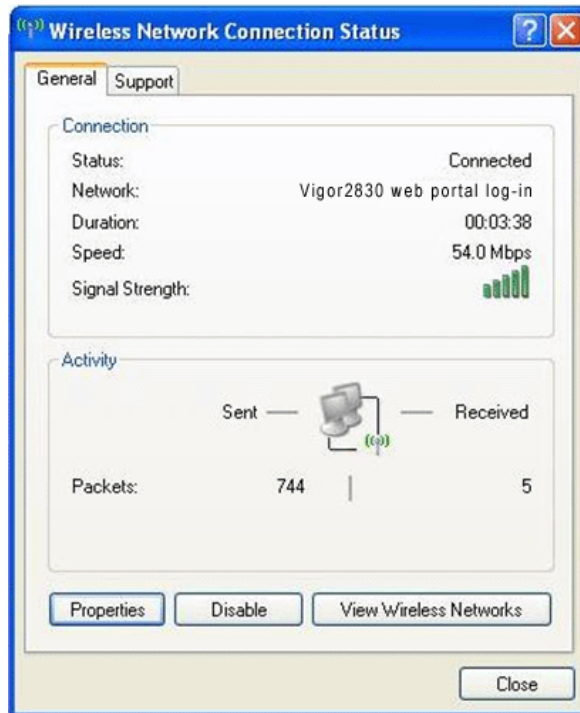
☐ SSID1 ☐ SSID2 ☐ SSID3 ☐ SSID4

OK Cancel

3. Click **OK** to save the settings. Note that do not choose **Redirect to URL** for this page if you have already enabled the user-based mode under **User Management**. For such case, choosing **Show the message** will be accepted.

Note: This feature is useful for restaurant, hotel, shopping store and so on. Wireless clients will be redirected to the specified web sites when they open the browser through the wireless environment set by the restaurant, hotel, shopping store, and so on. It can gain the result of advertisement effectively.

4. Use a Notebook or mobile device supporting Wireless function to connect Vigor2830 via Wireless LAN.



5. Try to open a new tab in the same browser (for IE 7.0/FireFox and above) or open a new web browser.
6. The first connection session will be redirected to DrayTek Website (specified in step 2) automatically.



However, if open another new tab again in the same browser, the browser will open default page based on the default setting.

4.5 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.

Vigor2830 Series
ADSL2+ Security Firewall

DrayTek

Off **IR6**

Wizards
Online Status

WAN
LAN
Load-Balance/Route Policy
NAT
Firewall
User Management
 General Setup
 User Profile
 User Group
 User Online Status
 Objects Setting
 CSM
Bandwidth Management
Applications
VPN and Remote Access
Certificate Management
VoIP
Wireless LAN
SSL VPN
USB Application
System Maintenance
Diagnostics
External Devices

Admin mode
Status: Ready

User Management >> General Setup

General Setup

Mode: Rule-Based
Display IP Address: Rule-Based
Checking window: Off

Web Authentication: HTTPS

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>
```

OK Clear Cancel

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.	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.	

- 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

Profile Index 3

<input checked="" type="checkbox"/> Enable this account	
Username	carrie
Password	*****
Confirm Password	*****
Idle Timeout	10 min(s) 0:Unlimited
Max User Login	0 0:Unlimited
External Server Authentication	None
Log	None
Pop Browser Tracking Window	<input checked="" type="checkbox"/>
Authentication	<input checked="" type="checkbox"/> Web <input checked="" type="checkbox"/> Alert Tool <input checked="" type="checkbox"/> Telnet
Landing Page	<input type="checkbox"/>
Index(1-15) in Schedule Setup:	
<input type="checkbox"/> Enable Time Quota	0 min. + - 0 min.
<input type="checkbox"/> Enable Data Quota	0 MB + - 0 MB
Reset quota to default when scheduling time expired	
<input type="checkbox"/> Enable	Default Time Quota 0 min. Default Data Quota 0 MB

OK Refresh Clear Cancel

- 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 Page Title** which will be shown on the heading of the login dialog. Next, click **OK**.

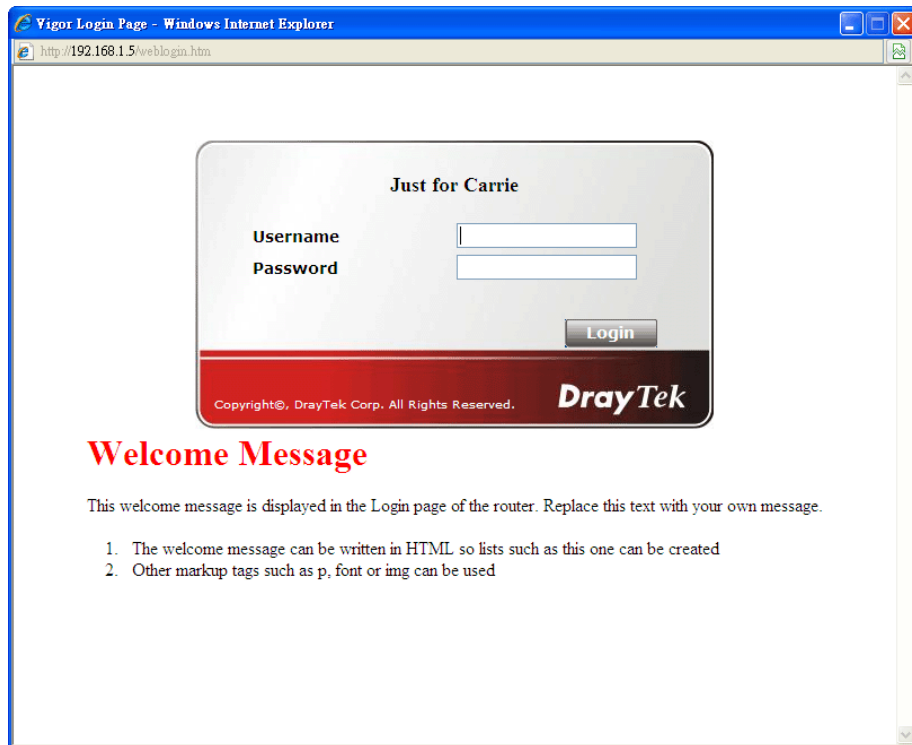
System Maintenance >> Login Page Greeting

Login Page Greeting

<input checked="" type="checkbox"/> Enable
Login Page Title Just for Carrie (31 char max.)
Welcome Message and Bulletin (Max 511 characters) Preview Set to Factory Default
<pre><h1>Welcome Message</h1><p>This welcome message is displayed in the Login page of the router. Replace this text with your own message. </p>The welcome message can be written in HTML so lists such as this one can be created Other markup tags such as p, font or img can be used</pre>
<p>Examples of Welcome Message and Bulletin:</p> <pre><h1>Welcome Message</h1> <p>Message</p></pre>

OK Cancel

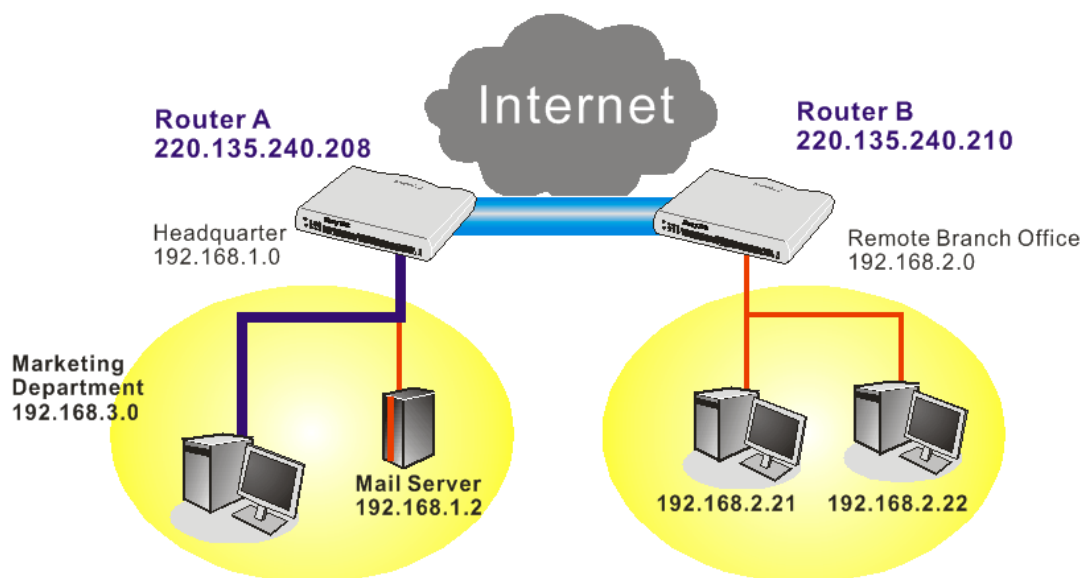
- Open a new tab in the same browser (for IE 7.0/FireFox and above) or open a new web browser.
- Try to access into the web user interface (e.g., 192.168.1.1) of Vigor router. Please note “*Just for Carrie*” is displayed as a heading on the login dialog box.



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

4.6 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/CHAP/MS-CHAP/MS-CHAPv2
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="password"/>	
IP Address Assignment for Dial-In Users (When DHCP Disable set)	
Assigned IP start	LAN 1 192.168.1.200
	LAN 2 192.168.3.200
	LAN 3 192.168.5.200
	LAN 4 192.168.7.200
LDAP Server Profiles for PPP Authentication PPTP LDAP Profile Note: Please select 'PAP Only' in 'Dial-In PPP Authentication', if you want to use AD/LDAP for PPP Authentication!!	

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	
Certificate for Dial-in	None ▾
Pre-Shared Key	
Pre-Shared Key	<input type="text"/>
Confirm Pre-Shared Key	<input type="text"/>
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 **LAN-to-LAN**. Click on one index number to edit a profile.
4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name	Branch 1	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	WAN1 First ▾	Idle Timeout	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"/>
(for some IGMP,IP-Camera,DHCP Relay..etc.)			

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	
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <input type="text" value="220.135.240.210"/>	
Username <input style="width: 100px;" type="text" value="???"/>	
Password(Max 15 char) <input style="width: 100px;" type="password"/>	
PPP Authentication PAP/CHAP/MS-CHAP/MS-CHAPv2	
VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off	
IKE Authentication Method	
<input checked="" type="radio"/> Pre-Shared Key	
IKE Pre-Shared Key <input style="width: 100px;" type="text"/>	
<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	
Local Certificate None	
IPsec Security Method	
<input checked="" type="radio"/> Medium(AH)	
<input type="radio"/> High(ESP) DES without Authentication	
Advanced	
Index(1-15) in Schedule Setup:	
<input style="width: 30px;" type="text"/> , <input style="width: 30px;" type="text"/> , <input style="width: 30px;" type="text"/> , <input style="width: 30px;" 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	
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <input type="text" value="220.135.240.210"/>	
Username <input style="width: 100px;" type="text" value="draytek"/>	
Password(Max 15 char) <input style="width: 100px;" type="password"/>	
PPP Authentication PAP/CHAP/MS-CHAP/MS-CHAPv2	
VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off	
IKE Authentication Method	
<input checked="" type="radio"/> Pre-Shared Key	
IKE Pre-Shared Key <input style="width: 100px;" type="text"/>	
<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	
Local Certificate None	
IPsec Security Method	
<input checked="" type="radio"/> Medium(AH)	
<input type="radio"/> High(ESP) DES without Authentication	
Advanced	
Index(1-15) in Schedule Setup:	
<input style="width: 30px;" type="text"/> , <input style="width: 30px;" type="text"/> , <input style="width: 30px;" type="text"/> , <input style="width: 30px;" type="text"/>	

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

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

3. Dial-In Settings

Allowed Dial-In Type	
<input type="checkbox"/> PPTP	Username <input data-bbox="1182 495 1414 528" type="text" value="???"/>
<input checked="" type="checkbox"/> IPSec Tunnel	Password <input data-bbox="1182 535 1398 568" type="text"/>
<input type="checkbox"/> L2TP with IPSec Policy <input data-bbox="679 584 820 618" type="text" value="None"/>	VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
<input checked="" type="checkbox"/> Specify Remote VPN Gateway	
Peer VPN Server IP <input data-bbox="400 752 628 786" type="text" value="220.135.240.210"/>	
or Peer ID <input data-bbox="504 792 735 826" type="text"/>	
IKE Authentication Method	
<input checked="" type="checkbox"/> Pre-Shared Key	
<input data-bbox="919 707 1174 741" type="text" value="IKE Pre-Shared Key"/> <input data-bbox="1182 707 1398 741" type="text"/>	
<input type="checkbox"/> Digital Signature(X.509)	
<input data-bbox="919 786 999 819" type="text" value="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	Username <input data-bbox="1182 1167 1414 1200" type="text" value="draytek"/>
<input type="checkbox"/> IPSec Tunnel	Password <input data-bbox="1182 1207 1398 1240" type="text" value="*****"/>
<input type="checkbox"/> L2TP with IPSec Policy <input data-bbox="679 1256 820 1290" type="text" value="None"/>	VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
<input checked="" type="checkbox"/> Specify Remote VPN Gateway	
Peer VPN Server IP <input data-bbox="400 1424 628 1458" type="text" value="220.135.240.210"/>	
or Peer ID <input data-bbox="504 1464 735 1498" type="text"/>	
IKE Authentication Method	
<input checked="" type="checkbox"/> Pre-Shared Key	
<input data-bbox="919 1379 1174 1413" type="text" value="IKE Pre-Shared Key"/> <input data-bbox="1182 1379 1398 1413" type="text"/>	
<input type="checkbox"/> Digital Signature(X.509)	
<input data-bbox="919 1458 999 1491" type="text" value="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	

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

4. TCP/IP Network Settings

My WAN IP	0.0.0.0	RIP Direction	Disable
Remote Gateway IP	0.0.0.0	From first subnet to remote network, you have to do	
Remote Network IP	192.168.2.0		Route
Remote Network Mask	255.255.255.0		
Local Network IP	192.168.1.1	<input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)	
Local Network Mask	255.255.255.0		
	More		

OK Clear Cancel

Settings in Router B in the remote office:

- 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

PPP General Setup PPP/MP Protocol Dial-In PPP Authentication: PAP/CHAP/MS-CHAP/MS-CHAPv2 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="password"/> IP Address Assignment for Dial-In Users (When DHCP Disable set) Assigned IP start: <table border="1"> <tr> <td>LAN 1</td> <td>192.168.2.200</td> </tr> <tr> <td>LAN 2</td> <td>192.168.3.200</td> </tr> <tr> <td>LAN 3</td> <td>192.168.5.200</td> </tr> <tr> <td>LAN 4</td> <td>192.168.7.200</td> </tr> </table>		LAN 1	192.168.2.200	LAN 2	192.168.3.200	LAN 3	192.168.5.200	LAN 4	192.168.7.200	LDAP Server Profiles for PPP Authentication PPTP LDAP Profile Note: Please select 'PAP Only' in 'Dial-In PPP Authentication', if you want to use AD/LDAP for PPP Authentication!!
LAN 1	192.168.2.200									
LAN 2	192.168.3.200									
LAN 3	192.168.5.200									
LAN 4	192.168.7.200									

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	
Certificate for Dial-in	None
Pre-Shared Key	
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

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

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name	Branch 1	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	WAN1 First	Idle Timeout	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	
(for some IGMP,IP-Camera,DHCP Relay..etc.)			

- 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		Username ??? Password(Max 15 char) PPP Authentication PAP/CHAP/MS-CHAP/MS-CHAPv2 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) 220.135.240.208		IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE 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 Local Certificate None
		IPsec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) DES without Authentication Advanced
		Index(1-15) in Schedule Setup: , , ,

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

2. Dial-Out Settings

Type of Server I am calling <input checked="" type="radio"/> PPTP <input type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy None		Username draytek Password(Max 15 char) ***** PPP Authentication PAP/CHAP/MS-CHAP/MS-CHAPv2 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) 220.135.240.208		IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE 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 Local Certificate None
		IPsec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) DES without Authentication Advanced
		Index(1-15) in Schedule Setup: , , ,

- 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 ??? Password(Max 11 char) VJ Compression On Off
<input checked="" type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP 220.135.240.208 or Peer ID 		IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <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

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 draytek Password(Max 11 char) ***** VJ Compression On Off
<input checked="" type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP 220.135.240.208 or Peer ID 		IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <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

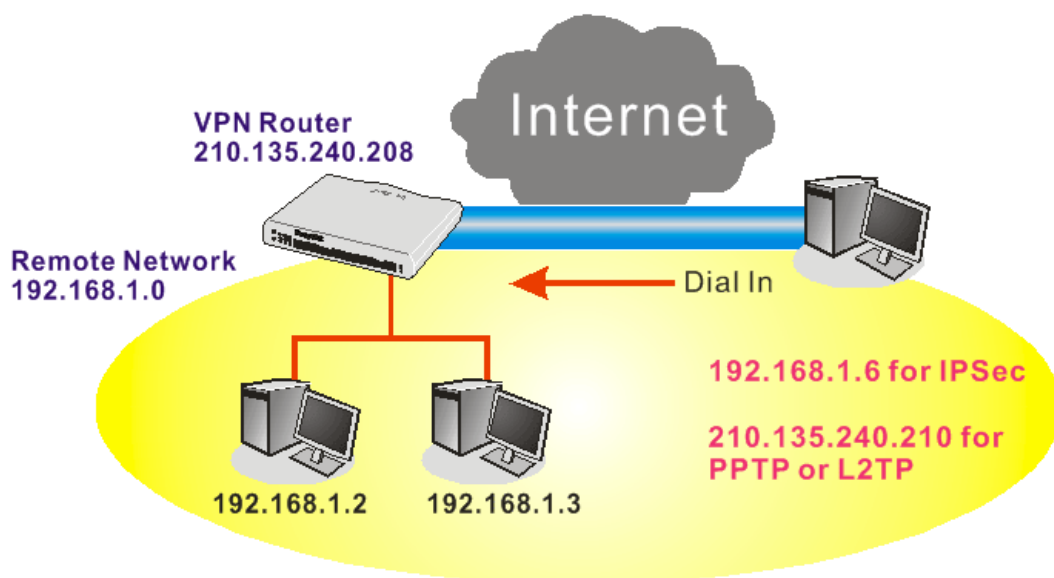
- At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router B can direct the packets destined to the remote network to Router A via the VPN connection.

4. TCP/IP Network Settings

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

4.7 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	
Password	
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	Username	???	
<input type="checkbox"/> Enable this account	Password		
Idle Timeout	300	second(s)	
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
IKE Authentication Method			
<input checked="" type="checkbox"/> Pre-Shared Key			
IKE 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
Local ID (optional)			

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.

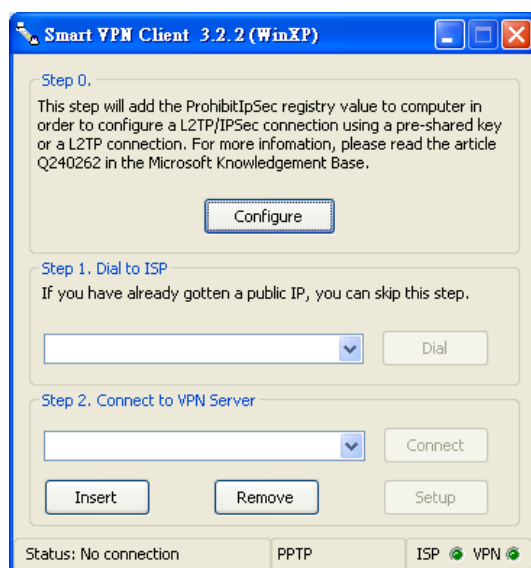
VPN and Remote Access >> Remote Dial-in User

Index No. 1

User account and Authentication <input type="checkbox"/> Enable this account Idle Timeout <input type="text" value="300"/> second(s)		Username <input type="text" value="???"/> Password <input type="password"/>
Allowed Dial-In Type <input checked="" type="checkbox"/> PPTP <input type="checkbox"/> IPSec Tunnel <input type="checkbox"/> L2TP with IPSec Policy <input type="text" value="None"/>		IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="text"/> <input type="checkbox"/> Digital Signature(X.509) <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		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) <input type="text"/>

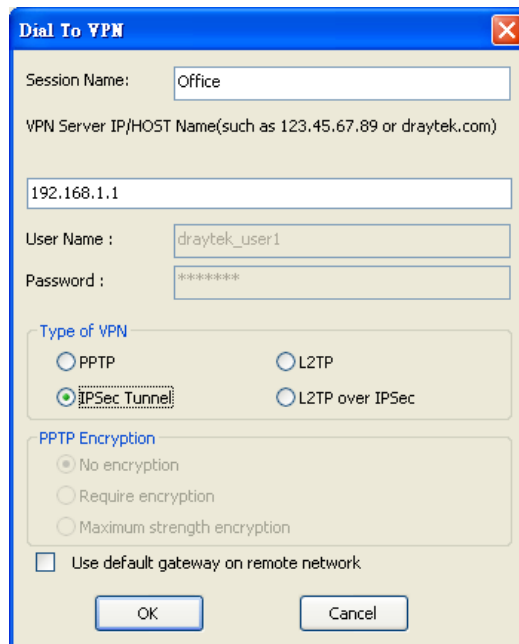
Settings in the remote host:

- 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.
- After successful installation, for the first time user, you should click on the **Step 0. Configure** button. Reboot the host.



- 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:

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

User Name :

Password :

Type of VPN

☐ PPTP ☐ L2TP

☒ IPsec Tunnel ☐ L2TP over IPsec

PPTP Encryption

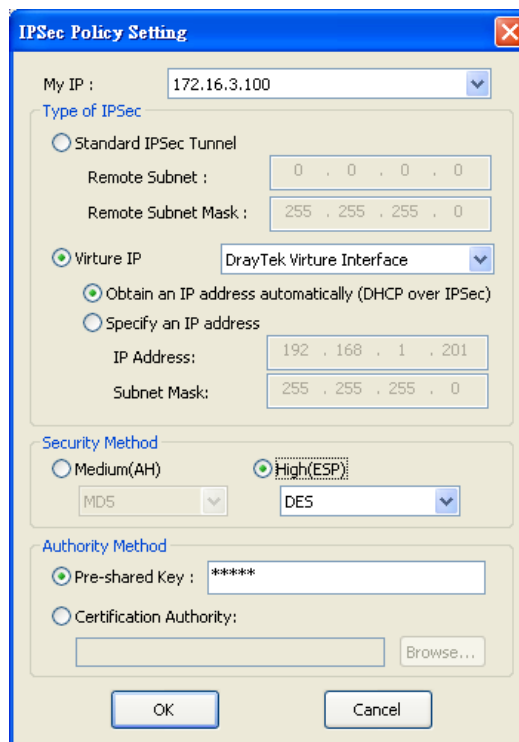
☒ No encryption

☐ Require encryption

☐ Maximum strength encryption

☐ Use default gateway on remote network

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 :

Type of IPSec

☐ Standard IPSec Tunnel

Remote Subnet :

Remote Subnet Mask :

☒ Virture IP

☒ Obtain an IP address automatically (DHCP over IPSec)

☐ Specify an IP address

IP Address:

Subnet Mask:

Security Method

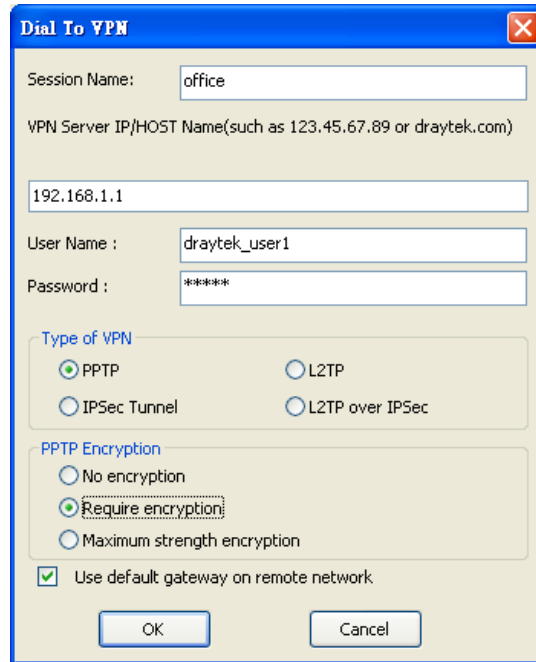
☐ Medium(AH) ☒ High(ESP)

Authority Method

☒ Pre-shared Key :

☐ Certification Authority:

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

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

4.8 QoS Setting Example

Assume a teleworker sometimes works at home and takes care of children. When working time, he would use Vigor router at home to connect to the server in the headquarter office downtown via either HTTPS or VPN to check email and access internal database. Meanwhile, children may chat on Skype in the restroom.

- 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	Enable	--Kbps/--Kbps	Outbound	25%	25%	25%	25%	Inactive	Status	Setup
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Status	Setup
WAN3	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	

- Click **Setup** link of WAN(1/2/3). Make sure the QoS Control on the left corner is checked. And select **BOTH** in **Direction**.

Bandwidth Management >> Quality of Service

WAN2 General Setup

☒ Enable the QoS Control OUT

WAN Inbound Bandwidth

WAN Outbound Bandwidth

Index Class Name

- Set Inbound/Outbound bandwidth.

Bandwidth Management >> Quality of Service

WAN2 General Setup

☒ Enable the QoS Control BOTH

WAN Inbound Bandwidth Kbps

WAN Outbound Bandwidth 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	<input type="radio"/> 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

WAN2 General Setup

☒ Enable the QoS Control BOTH

WAN Inbound Bandwidth	10000	Kbps	
WAN Outbound Bandwidth	10000	Kbps	

Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	25 %
Class 2		25 %
Class 3		25 %
	Others	25 %

☒ Enable UDP Bandwidth Control
☐ Outbound TCP ACK Prioritize

Limited_bandwidth Ratio 25 %

OK
Clear
Cancel

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

Bandwidth Management >> Quality of Service

Class Index #2

Name HTTPS

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

Add
Edit
Delete

OK
Cancel

- Click **Setup** link for WAN2.

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	Enable	--Kbps/--Kbps	Outbound	25%	25%	25%	25%	Inactive	Status Setup
WAN2	Enable	10000Kbps/10000Kbps	Both	25%	25%	25%	25%	Active	Status Setup
WAN3	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status Setup

Class Rule

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

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

Bandwidth Management >> Quality of Service

WAN2 General Setup

☒ Enable the QoS Control BOTH

WAN Inbound Bandwidth		10000	Kbps
WAN Outbound Bandwidth		10000	Kbps

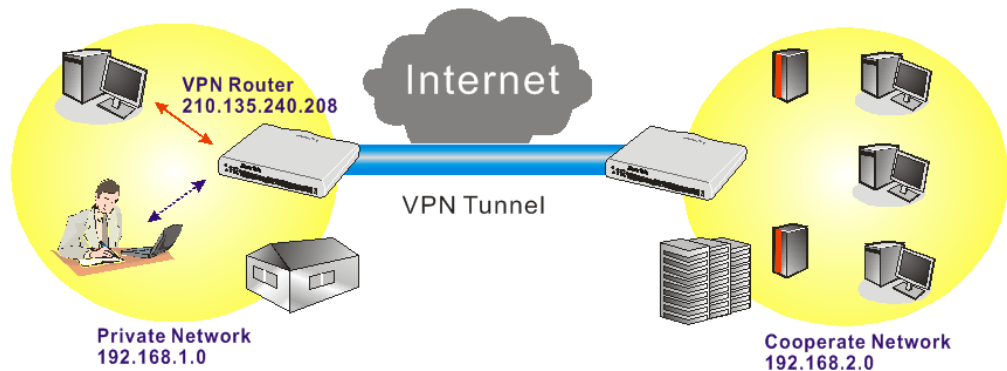
Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	25 %
Class 2	HTTPS	25 %
Class 3		25 %
	Others	25 %

☒ Enable UDP Bandwidth Control Limited_bandwidth Ratio 25 %

☐ Outbound TCP ACK Prioritize

OK Clear Cancel

9. If the worker has connected to the headquarter using host to host VPN tunnel. (Please refer to Chapter 3 VPN for detail instruction), he may set up an index for it. Enter the Class Name of Index 3. In this index, he will set reserved bandwidth for 1 VPN tunnel.



10. Click **Edit** to open a new window.

Bandwidth Management >> Quality of Service

Class Index #3

Name VPN

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

Add Edit Delete

OK Cancel

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

Bandwidth Management >> Quality of Service

Rule Edit

<input checked="" type="checkbox"/> ACT		
Local Address	<input type="text" value="Any"/>	<input type="button" value="Edit"/>
Remote Address	<input type="text" value="Any"/>	<input type="button" value="Edit"/>
DiffServ CodePoint	<input type="text" value="IP precedence 4"/>	<input type="button" value="v"/>
Service Type	<input type="text" value="SYSLOG(UDP:514)"/>	<input type="button" value="v"/>
Note: Please choose/setup the <u>Service Type</u> first.		
<input type="button" value="OK"/> <input type="button" value="Cancel"/>		

12. Then click **Edit** of **Local Address** to set a worker's subnet address. Click **Edit** of **Remote Address** to set headquarter's IP address. Leave other fields and click **OK**.

4.9 Upgrade Firmware for Your Router

Using Firmware Upgrade Utility

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

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

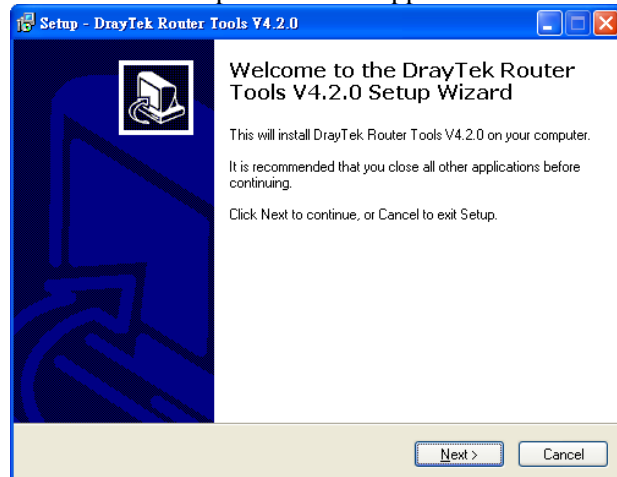
Model Name	Firmware Version	Release Date
Vigor120 series	3.2.2.1	26/06/2009
Vigor2100 series	2.6.2	26/02/2008
Vigor2104 series	2.5.7.3	13/02/2008
Vigor2110 series	3.3.0	25/06/2009
Vigor2200/X/W/E	2.3.11	22/09/2004
Vigor2200Eplus	2.5.7	18/02/2009
Vigor2200USB	2.3.10	16/03/2005

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

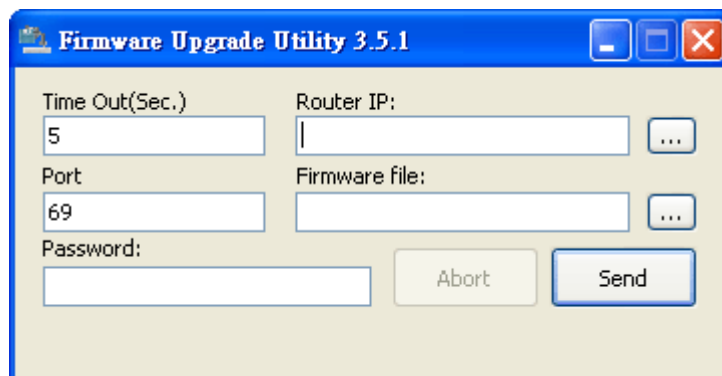
Tools Name	Release Date	Version	OS	Support Model
Router Tools	2009/06/18	4.2.0	MS-Windows	All Modules
Syslog Tools	2009/06/18	4.2.0	MS-Windows XP MS-Vista	All Modules
VigorPro Alert Notice Tools	2009/06/03	1.1.0 (Multi-language)	MS-Windows XP MS-Vista	VigorPro 100 series VigorPro 5500 series VigorPro 5510 series VigorPro 5300 series
Smart VPN Client	2009/05/25	3.6.3 (Multi-language)	MS-Windows XP MS-Vista	All Modules
Smart Monitor	2009/03/25	2.0	MS-Windows XP	Vigor2950 series VigorPro 5510 series

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

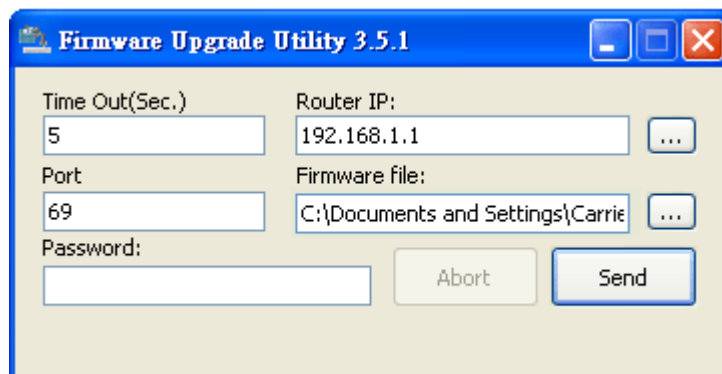
5. Double click on the icon of router tool. The setup wizard will appear.



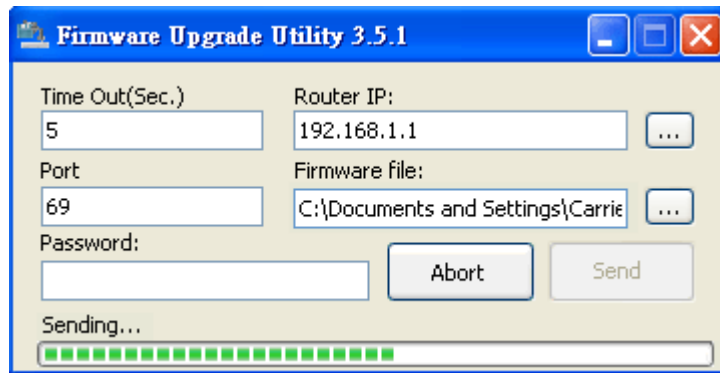
6. Follow the onscreen instructions to install the tool. Finally, click **Finish** to end the installation.
7. From the **Start** menu, open **Programs** and choose **Router Tools XXX >> Firmware Upgrade Utility**.



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



10. Click **Send**.



11. Now the firmware update is finished.

Using Web Page

The web page also can guide you to upgrade firmware. Note that this example is running over Windows OS (Operating System).

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

System Maintenance >> Firmware Upgrade

Web Firmware Upgrade

Select a firmware file.

未選擇檔案

Click Upgrade to upload the file.

TFTP Firmware Upgrade from LAN

Current Firmware Version: 3.6.6.1_db_RC1

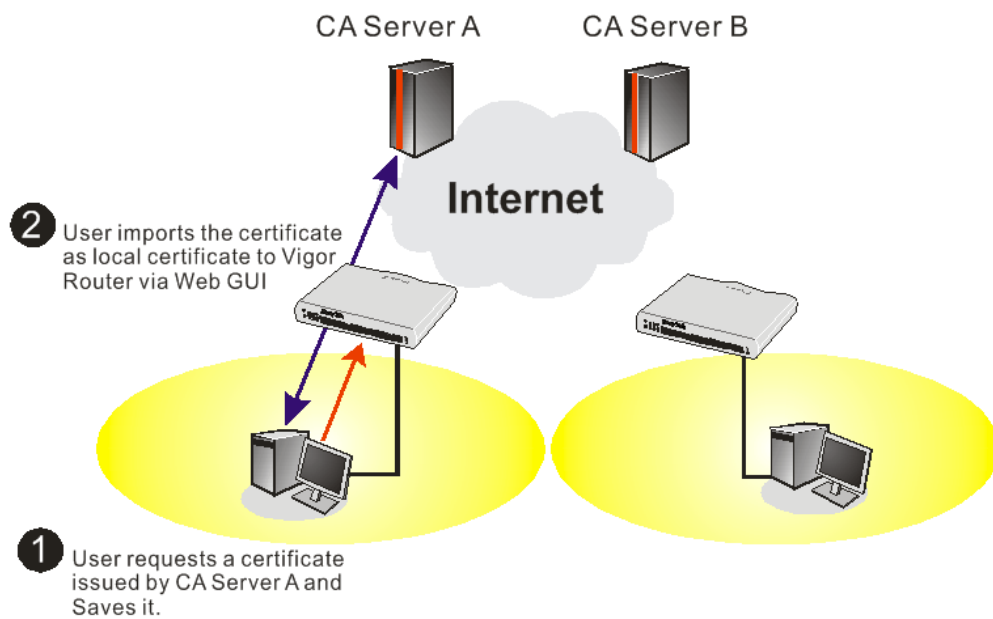
Firmware Upgrade Procedures:

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 ?

3. Select a firmware file by clicking **Browse**.
4. Click **Upgrade** to perform the firmware upgrade.

4.10 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	---	---	View Delete

[GENERATE](#) [IMPORT](#) [REFRESH](#)

X509 Local Certificate

- Certificate Management >> Local Certificate**

Generate

- Certificate Management >> Local Certificate**

X509 Local Certificate Request

- 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

Next >

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:

Base64 Encoded Certificate Request (PKCS #10 or #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARCAQAwQTELMAkGA1UEBhMCVFcxEDAO
BgkqhkiG9w0BCQEWEXByZXNzQG9yYX10ZWsuY29t
A4GNADCB1QKBgQDQYB7wmZFfFhN9/ IeQnG03Xk++
hX4bp89cUF9d1oACGG1M/tcBOckdcZdPFFvIXcP3
x/G0A7CTvO/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.

- 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	View Delete

[GENERATE](#)
[IMPORT](#)
[REFRESH](#)

X509 Local Certificate Request

```

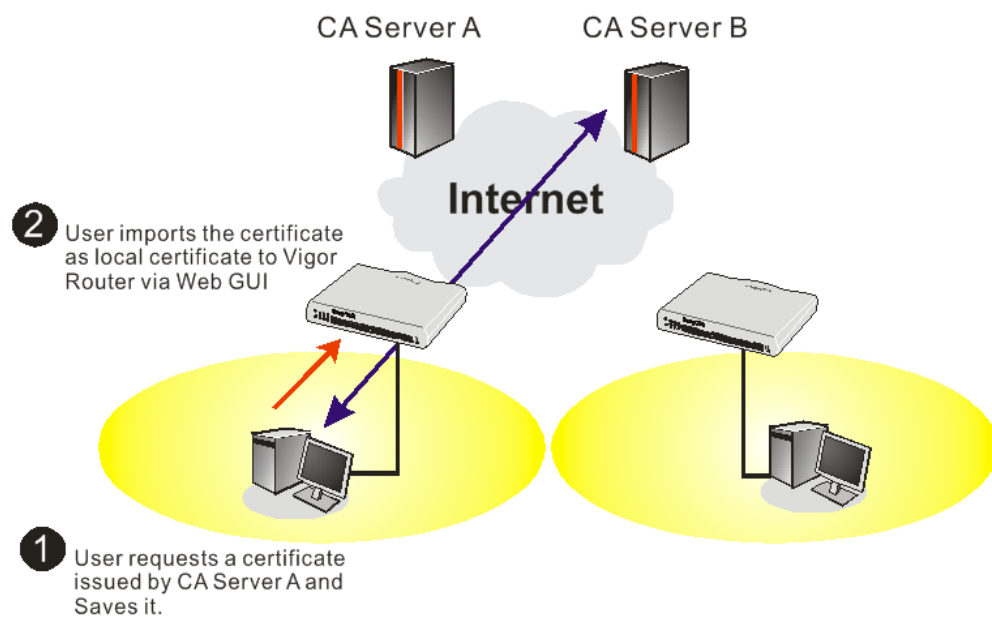
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCAQAwQTElMAkGA1UEBhMCVFcxEDAOBgNVBAAoTBORyYX10ZWsxID Ae
BgkqhkiG9wOBCQEWEXByZXNzQGRyYX10ZWsuY29tMIGfMAOGCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDPioahu/gFQaYB1ce5OERSDfWknIdHb1o1kt9cTdLUDaFk6s8d
3wDeQytoV1LBjz2IDFOxjX6ip7evl87twwTsg4lgZ6Qk/rGhuVTKd9j6PlcrnkP7
du84t23tWBdMD4W5c8VmSyDjShLhjdXVYPWpNKVlrOT2RZjkrMaHEWpVpwIDAQAB
oCkwJwYJKoZIhvcNAQkOMRowGDAWBgNVHREEDzANggtkcmF5dGVrLmNvbTANBgkq
hkiG9wOBAQUFAAOBgQAuSBRUGt4W1hH9N6/HwToem1tHQbcwjXvg/t7kFlzTJiHh
uRLq4CiEi6nV4hMRytcxZpE26sMarSgRREr86RoO8JxOI45560xCZ/N1Gh9VQ9I1
I9FgkjJNihp4TCjecSNNZjmQo5WU+Bce8TG+SCBCyejqu/fo/AJQFajB7Gviw==
-----END CERTIFICATE REQUEST-----

```

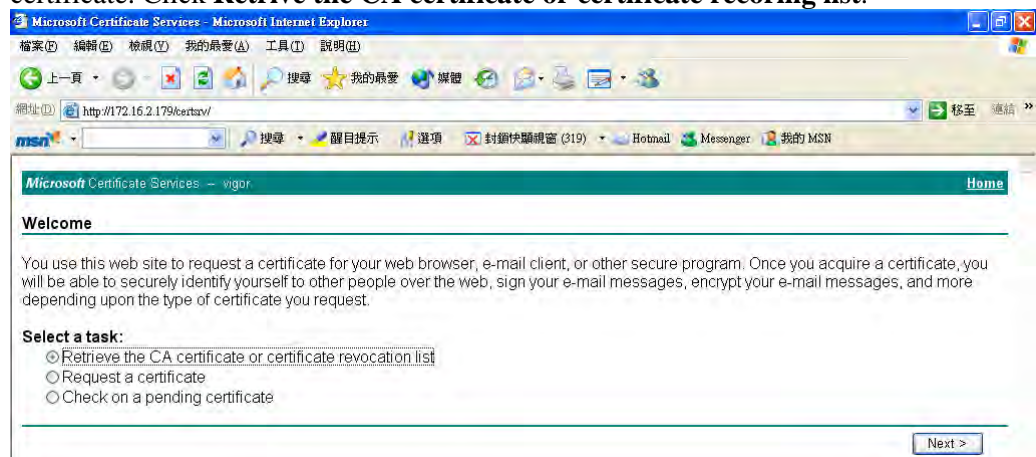
- You may review the detail information of the certificate by clicking **View** button.

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

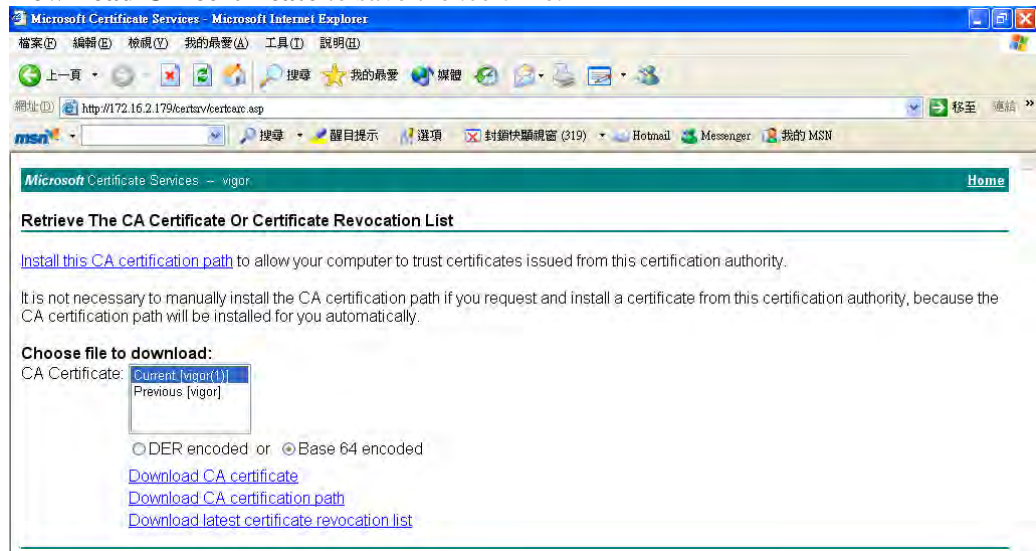
4.11 Request a CA Certificate and Set as Trusted on Windows CA Server



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	View	Delete
Trusted CA-2	---	---	View	Delete
Trusted CA-3	---	---	View	Delete

[IMPORT](#)

[REFRESH](#)

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

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

[Close](#)

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

4.12 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 filtering the web pages for the sake of protecting your system.

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

4.12.1 Creating an Account via Vigor Router

1. Click **CSM>> Web Content Filter Profile**. The following page will appear.

CSM >> Web Content Filter Profile

Web-Filter License
[Status:Not Activated]

[Activate](#)

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.	

Or

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

System Maintenance >> Activation

Activate via interface :

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 :

AYi GXZ

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

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 modifications 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

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

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: *
(3 ~ 20 characters)

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

Confirm Password: *

Personal Information

First Name: *

Last Name: *

Company Name:

Email Address: *
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: -

Country: *

Career: *

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?

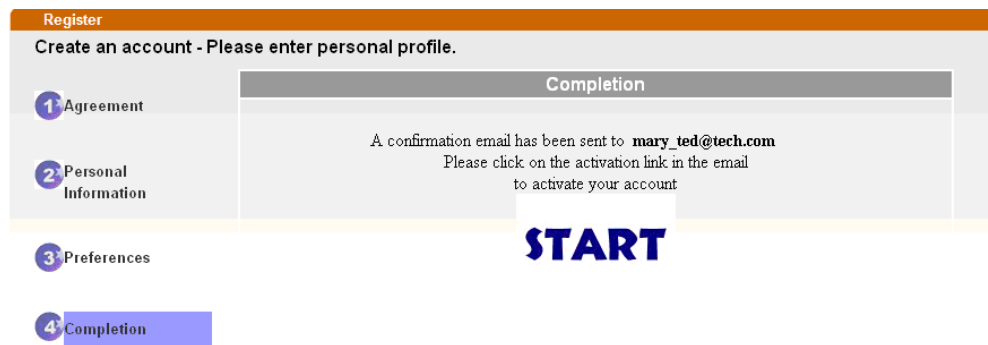
What kind of anti-virus do you use?

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.

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



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

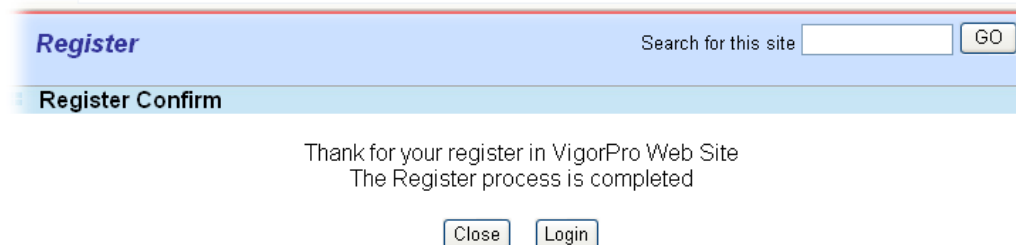
***** This is an automated message from myvigor.draytek.com.*****

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**.



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 : (886) 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.

4.12.2 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](#)

[About Us](#)
[Product](#)
[My Information](#)
[VigorPro](#)

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 trial 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.

Login

UserName

Password

AuthCode

QbkqVd

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 modifications 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

☒ 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: * ****

(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

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**.

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

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**.

Register Search for this site

Register Confirm

The Confirm message of New Owner(Mary) maybe timeout
Please try again or contact to draytek.com

Close Login

8. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**. Then type the code in the box of Auth Code according to the value displayed on the right side of it.

**This service is available for MyVigor member only. Please login to access MyVigor.
If you are not one of the members of MyVigor, please create an account first.**

LOGIN

UserName :

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.

4.13 How to Implement the LDAP/AD 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 Address

172.16.2.8

Destination Port

389

☐ Use SSL

Regular DN

uid=vpntest,ou=vpnuser,dc=ms,dc=dr

Regular Password

OK

Cancel

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.

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"/>	
Additional Filter	<input type="text" value="cn=rd1,ou=group,dc=ms,dc=draytek,dc=com"/>	
Note: Please type in your additional filter for BaseDN search request. For example, 1) For OpenLDAP: (gidNumber=500) 2) For AD: (msNPAllowDialin=TRUE)		
Group Distinguished Name	<input type="text"/>	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>		

and

Applications >> Active Directory /LDAP>>Server Profiles

Index No. 1

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"/>	
Additional Filter	<input type="text" value="cn=shrd,ou=group,dc=ms,dc=draytek,dc=com"/>	
Note: Please type in your additional filter for BaseDN search request. For example, 1) For OpenLDAP: (gidNumber=500) 2) For AD: (msNPAllowDialin=TRUE)		
Group Distinguished Name	<input type="text"/>	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>		

4. Click **OK** to save the settings above.

Applications >> Active Directory /LDAP

Active Directory /LDAP

General Setup		Active Directory / LDAP Profiles
Index	Name	Display Name
<u>1.</u>	rd1	
<u>2.</u>	shrd	
<u>3.</u>		
<u>4.</u>		

5. Open **User Management>>General Setup**. Select **User-Based** as the **Mode** option.

User Management >> General Setup

General Setup

Mode Selection:

- ☐ **Rule-Based** is a management method based on IP address. Administrator may set different firewall rules to different IP address.
- ☒ **User-Based** is a management method based on user profiles. Administrator may set different firewall rules to different user profiles.

Notice for User-Based mode:

- In User-Based mode, **Active Rules** in Firewall will be applied to all LAN clients, packets that matches the Active Rules will be blocked or pass immediately, no user authentication is required.
- Only **Inactive Rules** in Firewall can be set for individual user profile. In User-Based mode, packets that do not match Active Rules will need authentication, and the Inactive Rule applied to the specific user profile will then take effect.

Authentication page:

Web Authentication: ☒ HTTPS ☐ HTTP

☐ Display IP address on the dialog box pops up after successful login.

Landing page:

(Max 255 characters)

[Preview](#) [Set to Factory Default](#)

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

OK

Clear

Cancel

6. Then open **User Management>>User Profile**. Click index 3 to create a new user profile.

User Management >> User Profile

User Profile Table

Profile	Name
<u>1.</u>	admin
<u>2.</u>	Dial-In User
<u>3.</u>	

7. Check **Enable this account**; choose **LDAP** as **External Server Authentication**; and check the user profile you want.

Profile Index 3

<input checked="" type="checkbox"/> Enable this account	
Username	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
Idle Timeout	<input type="text" value="10"/> min(s) 0:Unlimited
Max User Login	<input type="text" value="0"/> 0:Unlimited
External Server Authentication	LDAP <input type="button" value="v"/>
<input checked="" type="checkbox"/> rd1	<input checked="" type="checkbox"/> shrd
Log	None <input type="button" value="v"/>
Pop Browser Tracking Window	<input checked="" type="checkbox"/>
Authentication	<input checked="" type="checkbox"/> Web <input checked="" type="checkbox"/> Alert Tool <input checked="" type="checkbox"/> Telnet
<u>Landing Page</u>	<input type="checkbox"/>
Index(1-15) in <u>Schedule</u> Setup:	<input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>
<hr/>	
<input type="checkbox"/> Enable Time Quota	0 min. <input type="button" value="+"/> <input type="button" value="-"/> 0 min.
<input type="checkbox"/> Enable Data Quota	0 MB <input type="button" value="+"/> <input type="button" value="-"/> 0 MB
Reset quota to default when scheduling time expired	
<input type="checkbox"/> Enable	Default Time Quota <input type="text" value="0"/> min. Default Data Quota <input type="text" value="0"/> MB

8. After finished above configurations, click OK to save the settings. Now, users belong to either “rd1” or “shrd” group can access Internet after inputting their credentials on LDAP server.

4.14 How to Implement the LDAP/AD Authentication for VPN?

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 Address

172.16.2.8

Destination Port

389

☐ Use SSL

Regular DN

uid=vpntest,ou=vpnuser,dc=ms,dc=dr

Regular Password

OK

Cancel

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.

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"/>	
Additional Filter	<input type="text" value="cn=rd1,ou=group,dc=ms,dc=draytek,dc=com"/>	
Note: Please type in your additional filter for BaseDN search request. For example, 1) For OpenLDAP: (gidNumber=500) 2) For AD: (msNPAllowDialin=TRUE)		
Group Distinguished Name	<input type="text"/>	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>		

and

Applications >> Active Directory /LDAP>>Server Profiles

Index No. 1

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"/>	
Additional Filter	<input type="text" value="cn=shrd,ou=group,dc=ms,dc=draytek,dc=com"/>	
Note: Please type in your additional filter for BaseDN search request. For example, 1) For OpenLDAP: (gidNumber=500) 2) For AD: (msNPAllowDialin=TRUE)		
Group Distinguished Name	<input type="text"/>	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>		

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

User Management >> General Setup

General Setup

Mode Selection:

- ☐ **Rule-Based** is a management method based on IP address. Administrator may set different firewall rules to different IP address.
- ☒ **User-Based** is a management method based on user profiles. Administrator may set different firewall rules to different user profiles.

Notice for User-Based mode:

- In User-Based mode, **Active Rules** in Firewall will be applied to all LAN clients, packets that matches the Active Rules will be blocked or pass immediately, no user authentication is required.
- Only **Inactive Rules** in Firewall can be set for individual user profile. In User-Based mode, packets that do not match Active Rules will need authentication, and the Inactive Rule applied to the specific user profile will then take effect.

Authentication page:

Web Authentication: ☒ HTTPS ☐ HTTP

☐ Display IP address on the dialog box pops up after successful login.

- Then open **VPN and Remote Access>>PPP General Setup** to **check** the profile(s) that will be authenticated with LDAP server. Choose **PAP Only** as **Dial-In PPP Authentication**.

VPN and Remote Access >> PPP General Setup

PPP General Setup

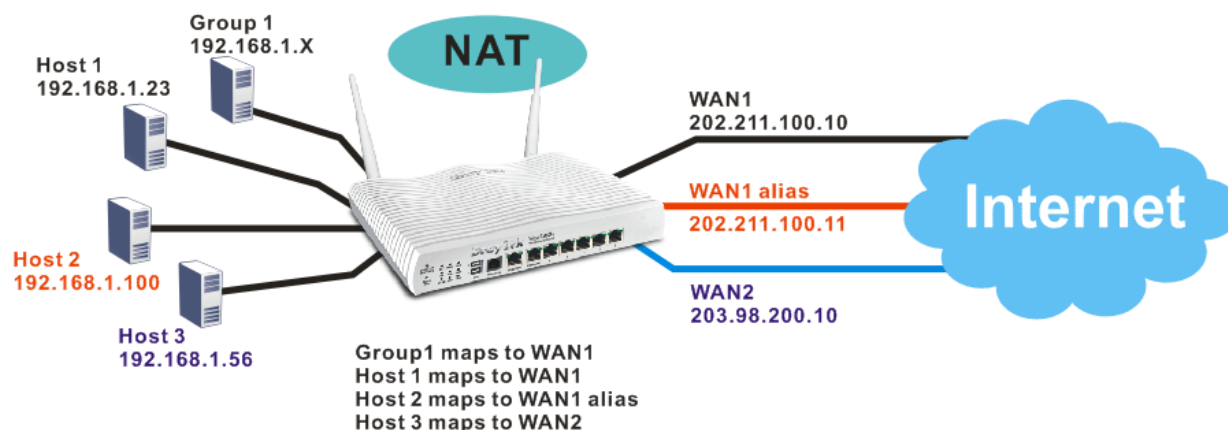
<p>PPP/MP Protocol</p> <p>Dial-In PPP Authentication: PAP Only</p> <p>Dial-In PPP Encryption(MPPE): Optional MPPE</p> <p>Mutual Authentication (PAP): <input type="radio"/> Yes <input checked="" type="radio"/> No</p> <p>Username: <input type="text"/></p> <p>Password: <input type="text"/></p> <p>IP Address Assignment for Dial-In Users (When DHCP Disable set)</p> <table><tr><td>Assigned IP start</td><td>LAN 1</td><td>192.168.1.200</td></tr><tr><td></td><td>LAN 2</td><td>192.168.2.200</td></tr><tr><td></td><td>LAN 3</td><td>192.168.3.200</td></tr><tr><td></td><td>LAN 4</td><td>192.168.4.200</td></tr></table>	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	<p>LDAP Server Profiles for PPP Authentication</p> <table><tr><td><input checked="" type="checkbox"/></td><td>rd1</td></tr><tr><td><input checked="" type="checkbox"/></td><td>shrd</td></tr></table> <p>Note: Please select 'PAP Only' in 'Dial-In PPP Authentication', if you want to use AD/LDAP for PPP Authentication!!</p>	<input checked="" type="checkbox"/>	rd1	<input checked="" type="checkbox"/>	shrd
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															
<input checked="" type="checkbox"/>	rd1																
<input checked="" type="checkbox"/>	shrd																

OK

- After finished above configurations, click OK to save the settings. Now, users belong to either “rd1” or “shrd” group can access Internet after inputting their credentials on LDAP server.

4.15 How to Setup Address Mapping

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



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

WAN1: 202.211.100.10, WAN1 alias: 202.211.100.11

WAN2: 203.98.200.10

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

With address mapping feature, you can manually configure any host mapping to any WAN interface to fit the request. In the above example, you can configure NAT Host 1 to always map to 202.211.100.10 (WAN1); Host 2 to always map to 202.211.100.11 (WAN1 alias); Host 3 always map to 203.98.200.10 (WAN2) and Group 1 to always map to 202.211.100.10 (WAN1).

NAT Address Mapping function lets you specify the outgoing IP address(es) for one internal IP address or a block of internal IP addresses.

We will take an example to introduce how to make use of this feature.

1. Log into the web user interface of Vigor2830.
2. Open **WAN>>Internet Access**. For WAN1, choose **MPoA/Static or Dynamic IP** as the **Access Mode**.

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode		
WAN1		ADSL	MPoA (RFC1483/2684)	Details Page	IPv6
WAN2		Ethernet	Static or Dynamic IP	Details Page	IPv6
WAN3		USB	None	Details Page	IPv6

Note : Only one WAN can support IPv6.

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

- Click the **Details Page** of WAN 1 to open the following page. From the above figure, set main WAN IP address as 202.211.100.10.

WAN >> Internet Access

WAN 1

PPPoE / PPPoA **MPoA (RFC1483/2684)** **IPv6**

☐ Enable ☒ Disable

DSL Modem Settings

Multi-PVC channel: Channel 2

Encapsulation: 1483 Bridged IP LLC

VPI: 8

VCI: 88

Modulation: Multimode

WAN Connection Detection

Mode: ARP Detect

Ping IP:

TTL:

RIP Protocol

☐ Enable RIP

Bridge Mode

☐ Enable Bridge Mode

WAN IP Network Settings **WAN IP Alias**

☐ Obtain an IP address automatically

Router Name: Vigor *

Domain Name: *

* : Required for some ISPs

DHCP Client Identifier for some ISP

☐ Enable

Username:

Password:

☒ Specify an IP address

IP Address: 202.211.100.10

Subnet Mask: 255.255.255.0

Gateway IP Address:

☐ Default MAC Address

☐ Specify a MAC Address

MAC Address: 00 1D AA A8 42 59

DNS Server IP Address

Primary IP Address: 8.8.8.8

Click the **WAN IP Alias** button to configure the other IP address which is 202.211.100.11. Make sure **Join IP NAT Pool** is not checked. Click **OK** to save the settings.

WAN1IP Alias - Google Chrome

192.168.1.1/doc/wipalias.htm

WAN1 IP Alias (Multi-NAT)

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	<input checked="" type="checkbox"/>	---	<input checked="" type="checkbox"/>
2.	<input checked="" type="checkbox"/>	202.211.100.11	<input type="checkbox"/>
3.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
4.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
5.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
6.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
7.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
8.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>

OK Clear All Close

4. After finished configuration for WAN1, open **Load-Balance/Route Policy**.

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

<< 1-1011-2021-3031-4041-50 >>

Next >>

<< [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

5. Click Index number 1 and 2 to configure the details. After finished the settings, click **OK** to save the settings respectively.

Load-Balance/Route Policy

Index: 1

☒ Enable

Criteria

Protocol: Any

Source IP:

☐ Any

☒ Src IP Start: 192.168.1.16 ~ Src IP End: 192.168.1.31

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

Interface Address: 1----

Gateway IP:

☒ Default Gateway

☐ Specific Gateway:

More Options

☐ Auto Failover to the Other WAN

Packet Forwarding to WAN via:

☒ Force NAT

☐ Force Routing

And

Load-Balance/Route Policy

Index: 2

☒ Enable

Criteria

Protocol Any

Source IP

☐ Any
 ☒ Src IP Start

Src IP End
 192.168.1.100 ~ 192.168.1.100

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

Interface Address 2-202.211.100.11

Gateway IP

☒ Default Gateway
 ☐ Specific Gateway

More Options

☐ Auto Failover to the Other WAN

Packet Forwarding to WAN via

☒ Force NAT
 ☐ Force Routing

- Upon completing the above configuration, you have specified the outgoing IP address(es) for some specific computers.

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 checked="" type="checkbox"/>	Any	WAN1	---	192.168.1.16	192.168.1.31	Any	Any	Any	Any		Down
2	<input checked="" type="checkbox"/>	Any	WAN1	202.211.100.11	192.168.1.100	192.168.1.100	Any	Any	Any	Any	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 >>

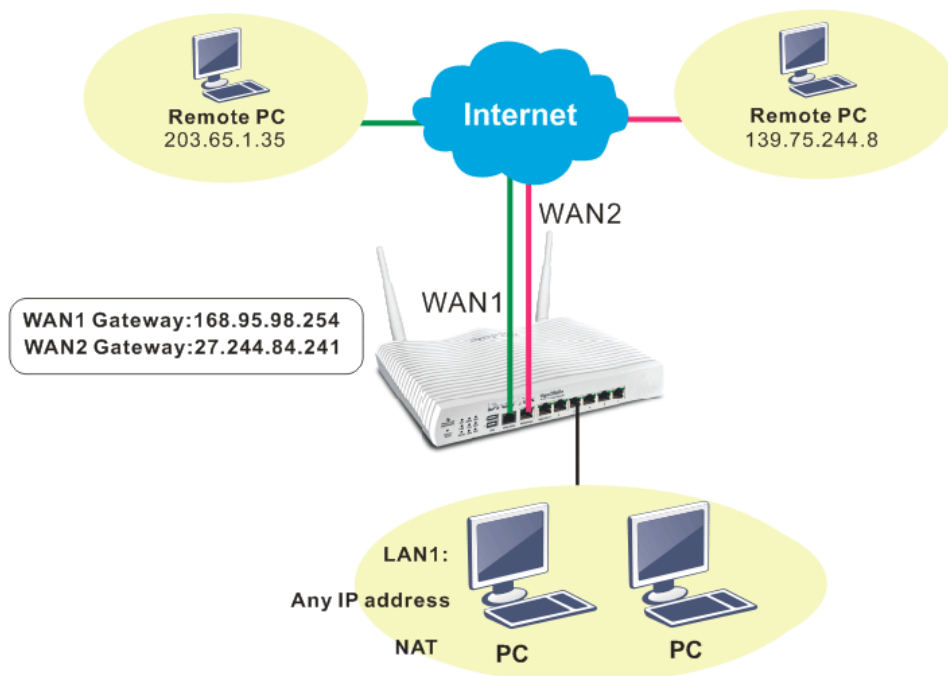
- ☐ Wizard Mode: most frequently used settings in three pages
- ☒ Advance Mode: all settings in one page

OK

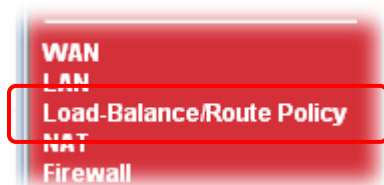
- Now, you bind some specific computers to some WAN IP alias for outgoing traffic.

4.16 How to setup Load Balance for Packets?

The following figure shows a simple application of load balance. WAN1 and WAN2 can be used to access into Internet. The PC in LAN1 can send the data to the remote PC through the specified WAN1.



1. Access into web user interface of Vigor2830 series. Open **Load-Balance/Route Policy**.



2. From the following web page, simply click index number #1.

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

- In the following page, check **Enable**; set Dest IP Start and Dest IP End with 203.65.1.35 and 203.65.1.35; choose WAN1 as the **Interface**; click **default gateway**; do not check **Auto Failover To The Other WAN**.

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 203.65.1.35 ~ 203.65.1.35 Dest IP End

Destination Port: ☐ Any ☐ Dest Port Start ~ Dest Port End

Send to if Criteria Matched

Interface: WAN1

Interface Address: 1----

Gateway IP: ☒ Default Gateway ☐ Specific Gateway

More Options

☐ Auto Failover to the Other WAN

Packet Forwarding to WAN via: ☒ Force NAT ☐ Force Routing

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



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 checked="" type="checkbox"/>	Any	WAN1	---	Any	Any	203.65.1.35	203.65.1.35	Any	Any		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

Now, the packets sent to the remote PC (IP address: 203.65.1.35) will be forcefully to pass through WAN1.

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

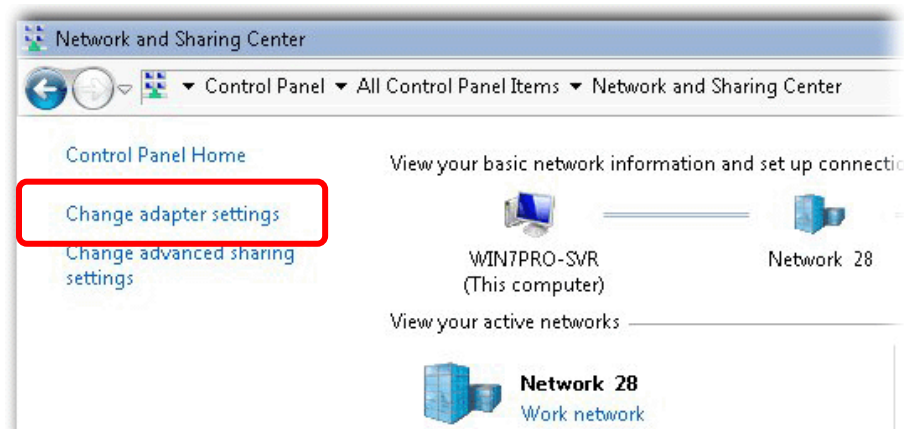


The example is based on Windows 7 (Professional Edition). As to the examples for other operation systems, please refer to the similar steps or find support notes in www.DrayTek.com.

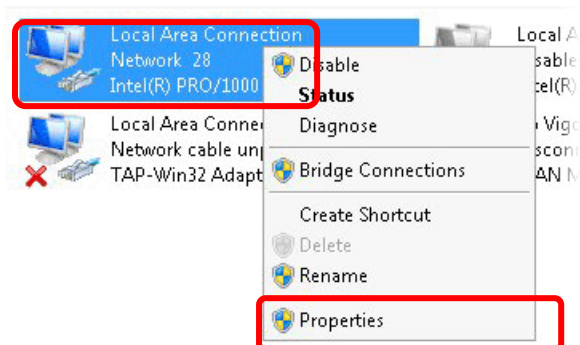
1. Open **All Programs>>Getting Started>>Control Panel**. Click **Network and Sharing Center**.



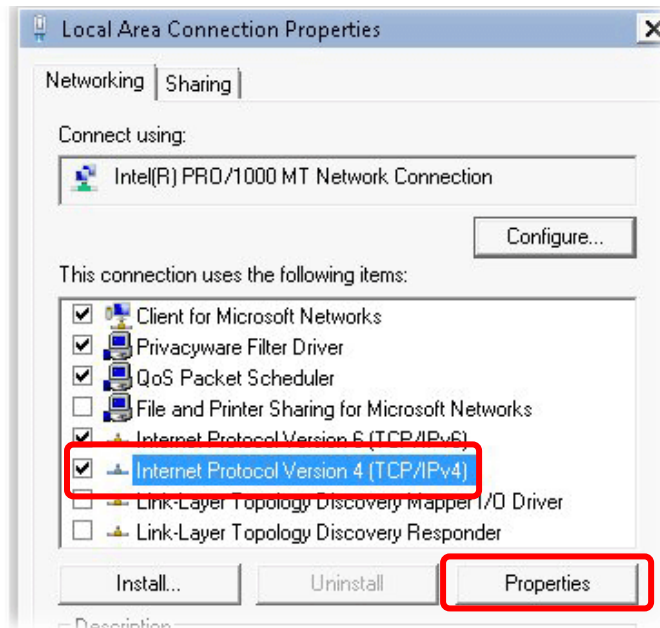
2. In the following window, click **Change adapter settings**.



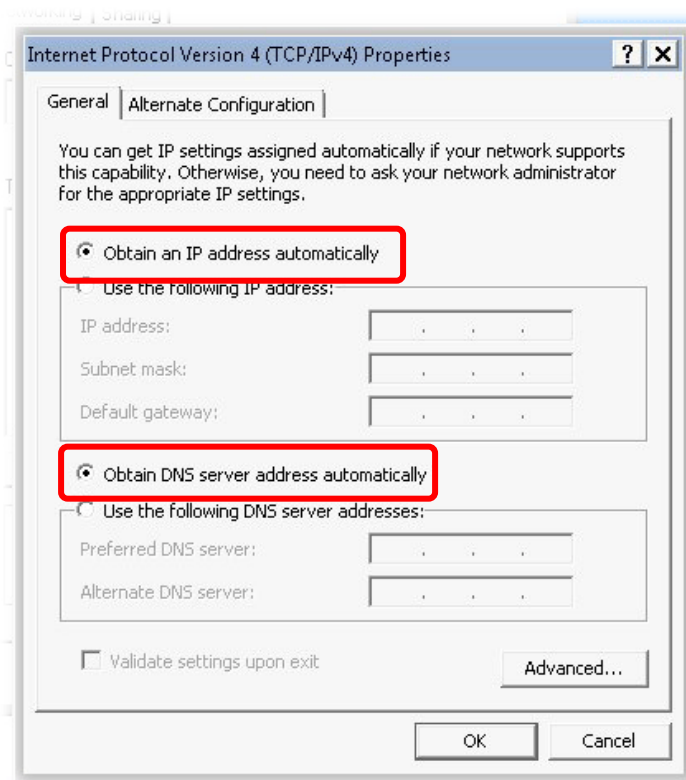
3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



4. Select **Internet Protocol Version 4 (TCP/IP)** and then click **Properties**.

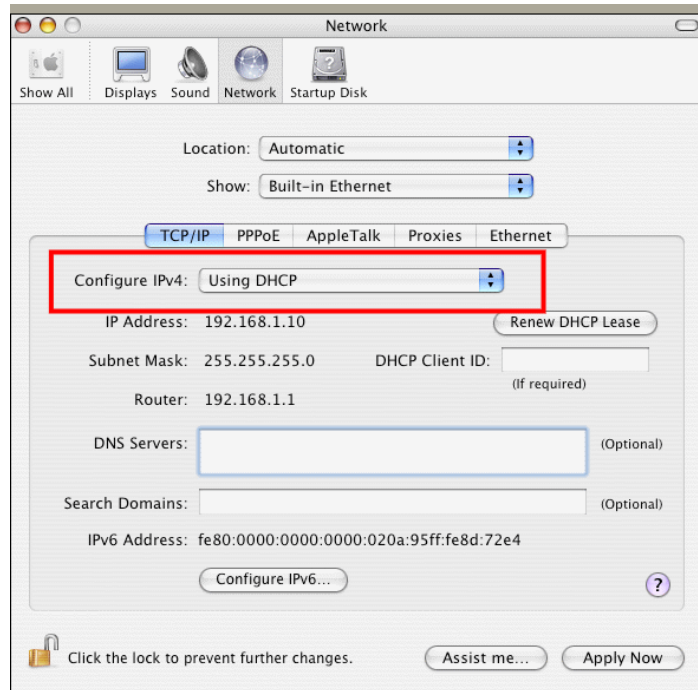


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



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.



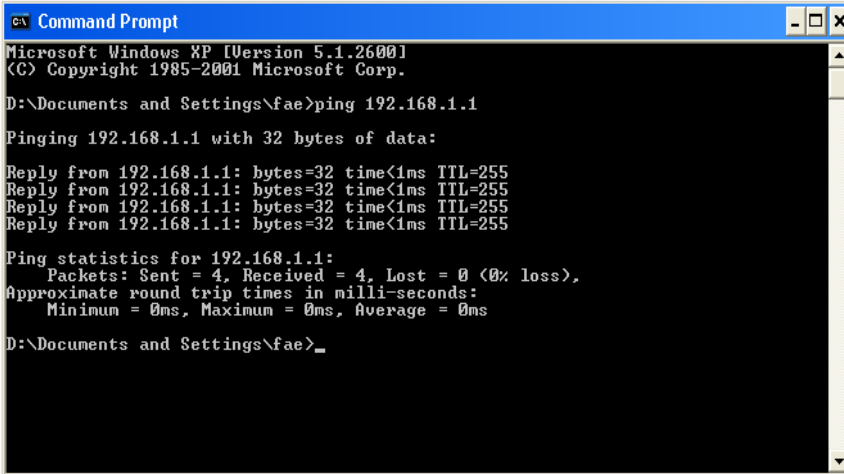
5.3 Pinging the Router from Your Computer

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.



```

C:\ Command Prompt
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 WAN1/WAN2 to review the settings that you configured previously.

WAN >> Internet Access

Internet Access			
Index	Display Name	Physical Mode	Access Mode
WAN1		ADSL	<div> <div>PPPoE / PPPoA</div> <div>Details Page</div> </div>
WAN2		Ethernet	<div> <div>Static or Dynamic IP</div> <div>Details Page</div> </div>
WAN3		USB	<div> <div>None</div> <div>Details Page</div> </div>

5.5 Problems for 3G/4G Network Connection

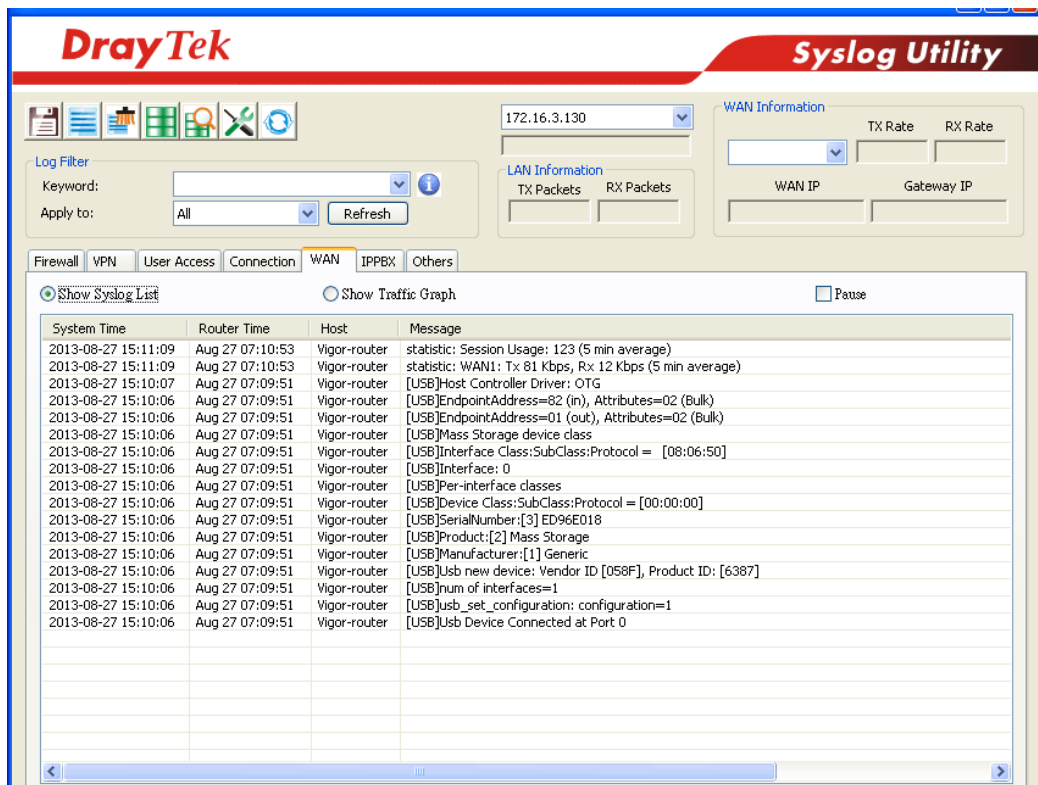
When you have trouble in using 3G/4G network transmission, please check the following:

Check if USB LED lights on or off

You have to wait about 15 seconds after inserting 3G/4G USB Modem into your Vigor2830. 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 Vigor2830.

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/4G 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.



Transmission Rate is not fast enough

Please connect your Notebook with 3G/4G USB Modem to test the connection speed to verify if the problem is caused by Vigor2830. 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. Such function is available in **Admin Mode** only.



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. The password of factory default is null.

Software Reset

You can reset the router to factory default via Web page. Such function is available in **Admin Mode** only.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **Reboot Now**. After few seconds, the router will return all the settings to the factory settings.

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

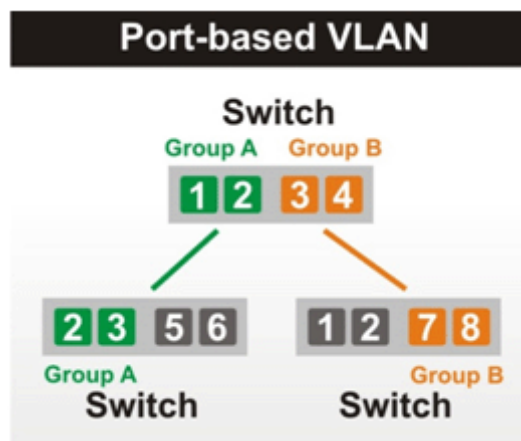
If the router still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@DrayTek.com.

Appendix I: VLAN Applications on Vigor Router

Virtual Local Area Network is so-called VLAN. It offers the logical grouping technique to separate the physical ports of Ethernet switches, thus we can management our local network easier, more flexible and secure. For instance, you're a networking administrator in your company and you're planning to isolate the visitors' traffics from your private network for security considerations because you cannot ensure that visitors' computer is clean. Or you want to separate your private network into several parts by divisions because there are too many computers in the same network segment and it results in the local traffics heavily. VLAN helps you to solve these situations, and DrayTek's products support bellow two popular types:

Port-based

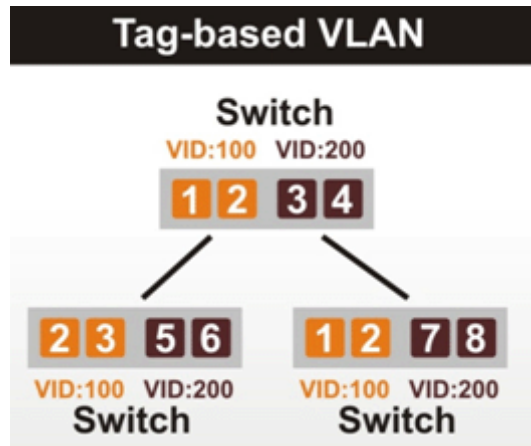
It uses a matrix table of the physical ports to define the traffics how to exchange between each port, and the traffics will be isolated from the ports are not being ticked in the same line. It is the easiest way to setup an isolate network, but not a flexible way to maintain a growing network. Because the idea of port-based VLAN is grouping by physical ports, but the difficulty is how to handle the traffics between two or more Ethernet switches. Thus, VLAN is suitable for some circumstances, for example, the rental apartment, SOHO office...and so on. These clients may need two or three isolated networks only and setup a network in a simple way.



Tag-based

The idea of tag-based VLAN is to identify a virtual LAN with a specific ID, therefore, **VLAN ID** introduced by tag-based VLAN. Through VLAN ID, ports with different **VID (VLAN ID)** will be identified as in different LANs, so the traffics also will be isolated from each of VLANs. Many administrators who manage an enterprise network or even the internet service providers (ISP) adopt Tag-based VLAN popularly because it is convenient to maintenance and management a distributed network. Setting a large-scale network is easy by giving each of them with different VID and isolating the traffics at the same time. Besides the VLAN ID, there is another feature, **Trunk**, introduced. While the role of a port on an Ethernet switch is setup as a Trunk port, it means the VLAN ID will be kept while forwarding the packets between switches. By this feature, VLANs are able to distribute over two or more Ethernet

switches easily, moreover design a large and secured network is possible through Trunk port. When VLAN is being enabled on Vigor routers, the LAN ports are being turned into Trunk mode automatically. Therefore, a VLAN supported switch, like VigorSwitch G2260/P2261, or VigorSwitch G1240, is needed.



Vigor routers^[Note] support Tag-based feature both on LAN and WAN interfaces. The next we'll demonstrate our web design and how to configure the settings by introducing the functionalities of Vigor router.

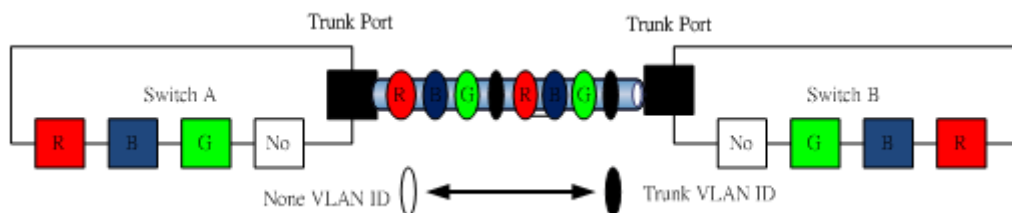
[Note]

Broadband router: Vigor2920/Vigor3200/Vigor2925/Vigo2960/Vigor3900

Modem router: Vigor2850/Vigor2860

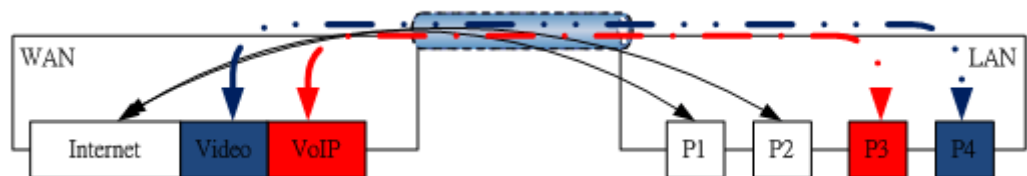
VLAN Packets on Vigor routers

Trunk mode of LAN



Trunk Port can carry the packets with VID but replace the Non-VID packet as the VID of Trunk port while forwarding the packets to another switch.

Bridge mode of WAN



P1 and P2 are doing NAT flow to access to the internet, but P3 and P4 will forward the packets between WAN and LAN ports directly.

Web User Interface

So far, there are two kinds of open system on Vigor router. One is DrayOS, which is DrayTek owned, and another is Linux-like which customized by DrayTek from OpenWRT. Here

DrayOS system is going to be introduced to you because it is the most stable and superfast booting system in DrayTek products. If the UI style of yours is different from the following. It may not DrayOS system with new web style or maybe the Linux-like model.

WAN

Internet Access >> Multi-VLAN

Multi-VLAN

Channel	Enable	WAN Type	VLAN Tag	Port-based Bridge
1	Yes	Ethernet(WAN1)	None	
2	Yes	Ethernet(WAN2)	None	
3	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
4	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
5_WAN5	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
6_WAN6	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
7_WAN7	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
8	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5

Detail settings of channel profile

Multi-VLAN Channel 5: ☐ Enable ☒ Disable
WAN Type : Ethernet(WAN1)

VLAN Settings

General Settings
VLAN Header
VLAN Tag: 0
Priority: 0
Note: 1. Tag value must be set between 1~4095 and unique for each channel.
2. Only one channel can be untagged (equal to 0) at a time.

VLAN Members

☐ Open Port-based Bridge Connection for this Channel
Physical Members
☐ P1 ☐ P2 ☐ P3 ☐ P4 ☐ P5
Note: 3. P1 is reserved for NAT use, and cannot be configured for bridge mode.

Service Binding & WAN Setup

☐ Open WAN Interface for this Channel
WAN for Router-borne Application: Management
WAN Setup: Static or Dynamic IP

ISP Access Setup
ISP Name:
Username:
Password:
PPP Authentication: PAP or CHAP
☒ Always On
Idle Timeout: -1 second(s)
IP Address From ISP
Fixed IP: ☐ Yes ☒ No (Dynamic IP)
Fixed IP Address:

WAN IP Network Settings
☐ Obtain an IP address automatically
Router Name: Vigor
Domain Name:
*: Required for some ISPs
☒ Specify an IP address
IP Address:
Subnet Mask:
Gateway IP Address:
DNS Server IP Address
Primary IP Address: 8.8.8.8
Secondary IP Address: 8.8.4.4

LAN

Enable **Port-based VLAN** by checking the option

The option of **Tag-based VLAN**

VLAN Configuration

☒ Enable

	LAN				Wireless LAN				Subnet	VLAN Tag		
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4		Enable	VID	Priority
VLAN0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LAN 1	<input checked="" type="checkbox"/>	0	0
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0

VLAN Group

Member of **Port-based** or **Tag-based VLAN**

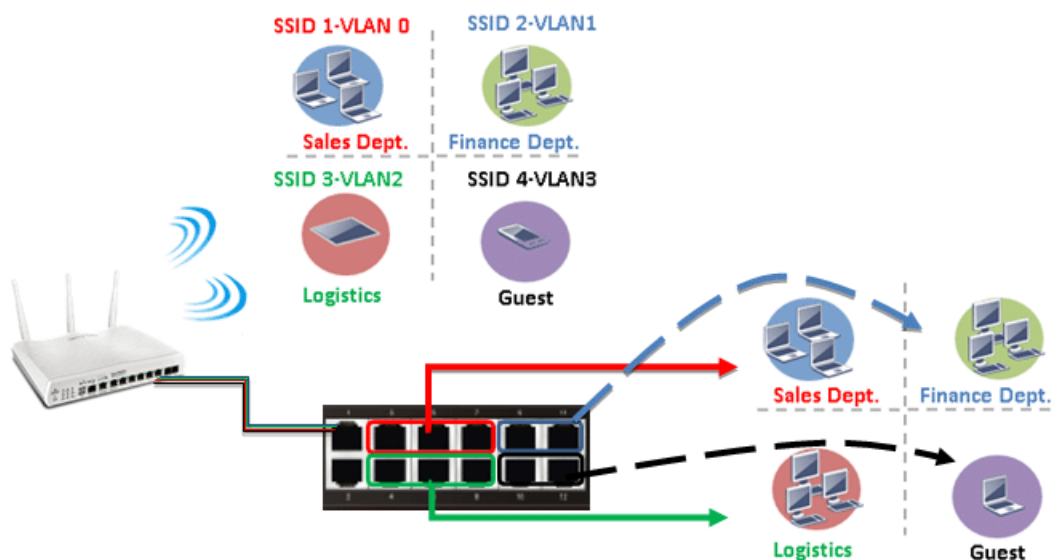
DHCP Pool will be used

VLAN ID assigned

802.1p field

VLAN applications on Vigor router

- Multi Subnet (VLAN of LAN)



Port-based mode

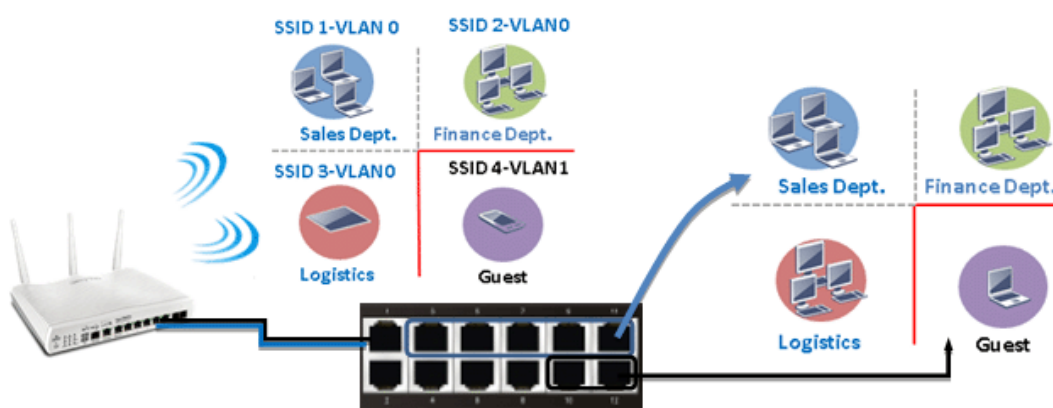
<input checked="" type="checkbox"/> Enable												
LAN				Wireless LAN				VLAN Tag				
P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 2	<input type="checkbox"/>	0	0	
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	LAN 3	<input type="checkbox"/>	0	0	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	LAN 4	<input type="checkbox"/>	0	0	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0	

Tag-based mode

<input checked="" type="checkbox"/> Enable												
LAN				Wireless LAN				VLAN Tag				
P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input checked="" type="checkbox"/>	10	0	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 2	<input checked="" type="checkbox"/>	20	0	
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	LAN 3	<input checked="" type="checkbox"/>	30	0	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	LAN 4	<input checked="" type="checkbox"/>	40	0	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0	

By above settings, there are four private networks will be created and computers attached with each of LAN ports or SSIDs which are able to obtain a private IP address from each DHCP servers (LAN1/LAN2/LAN3/LAN4). However, the traffics of the LAN port or SSID that are NOT being grouped in the same VLAN are unable to forward to each other. The benefit of Port-based is able to extend the wired ports by installing a cheaper dumb switch as many as you need, but Tag-based offers you a flexible and well-managed network. The networks are isolated, secured and reduce the broadcasting storm effectively in each of networks with VLAN.

● Guest Network



Port-based mode

VLAN Configuration												
<div><input checked="" type="checkbox"/> Enable</div>												
	LAN				Wireless LAN					VLAN Tag		
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
VLAN0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	LAN 2	<input type="checkbox"/>	0	0
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0

Tag-based mode

<input checked="" type="checkbox"/> Enable												
	LAN				Wireless LAN					VLAN Tag		
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
VLAN0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LAN 1	<input checked="" type="checkbox"/>	0	0
VLAN1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	LAN 2	<input checked="" type="checkbox"/>	10	0
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0

To deploy a guest network, which serves your guests the internet accessibility, but the traffics have to be isolated from your private network due to the security considerations, it can be done by above settings. However, a switch support VLAN function is need if VLAN Tag enabled.

● Triple Play (Multi-WAN)

NAT mode with VLAN



Following settings, the set-top box (STB) is able to attach with any LAN port. Video streaming which your ISP provided will be played on your monitor.

WAN 1

Enable: ☒ Yes

Display Name:

Physical Mode: Ethernet

Physical Type: Auto negotiation

Line Speed(Kbps):

DownLink:

UpLink:

VLAN Tag insertion: ☒ Enable (Please configure Internet Access setting first)

Tag value: 10 (0~4095)

Priority: 0 (0~7)

Active Mode: Always On Load Balance: ☒

1. Setup the VLAN ID on WAN1 profiles if WAN is the primary interface of IPTV service.

2. Open the profile of WAN5 by clicking the ID.

General					
Channel	Enable	WAN Type	VLAN Tag	Port-based Bridge	
1	Yes	Ethernet(WAN1)	None		
2	Yes	Ethernet(WAN2)	None		
3	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
4	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
5, WAN5	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
6, WAN6	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
7, WAN7	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
8	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4

Multi-VLAN Channel 5: ☒ Enable ☐ Disable

WAN Type: Ethernet(WAN1)

General Settings

VLAN Header

VLAN: 20

Tag: 3

Priority: 3

Note: 1. Tag value must be set between 1~4095 and unique for each channel.
2. Only one channel can be untagged (equal to 0).

☐ Open Port-based Bridge Connection for this Channel

Physical Members

☐ P1 ☐ P2 ☐ P3 ☐ P4 ☐ P5

Note: 3. P1 is reserved for NAT use, and cannot be configured for bridge mode.

3. Setup connection of WAN 5 and bind the service onto it.

NO need to enable Port-based Bridge.

4. Go to Application >> IGMP to bind it on PVC WAN.

IGMP

☒ Enable IGMP Proxy PVC

IGMP Proxy is to act as a multicast proxy for will access any multicast group. But this function take up extra 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.

ISP Access Setup

ISP Name:

Username:

Password:

PPP Authentication: PAP or CHAP

☒ Always On

Idle Timeout: 1 second(s)

IP Address From ISP

Fixed IP: ☐ Yes ☒ No

(Dynamic IP)

Fixed IP Address:

WAN IP Network Settings

☒ Obtain an IP address automatically

Router: Vigor

Name:

Domain:

Name:

*: Required for some ISPs

☐ Specify an IP address

IP Address:

Subnet:

Mask:

Gateway:

IP Address:

DNS Server IP Address

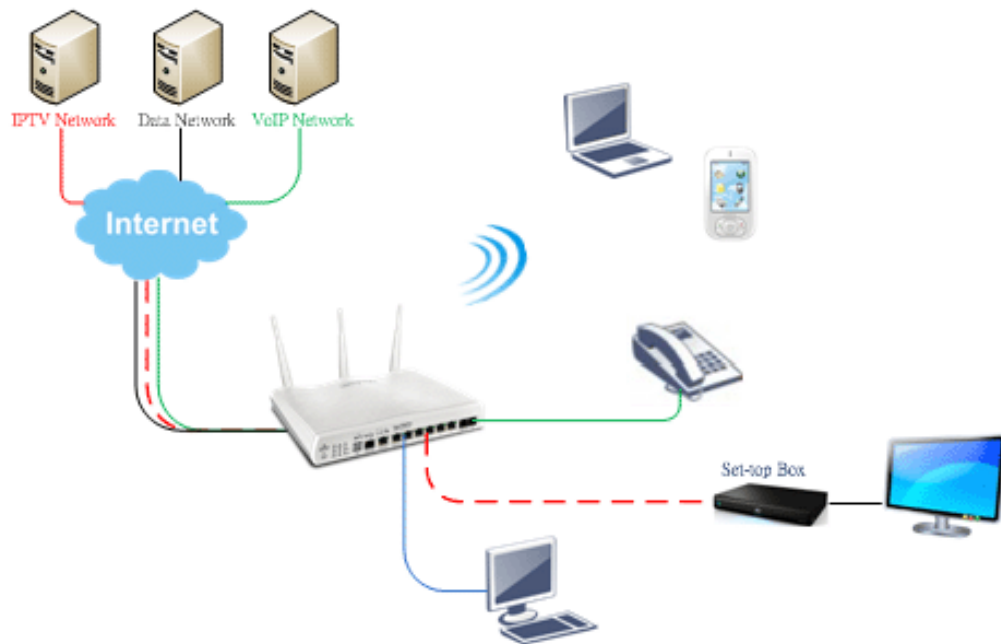
Primary IP: 8.8.8.8

Address:

Secondary: 8.8.4.4

IP Address:

Bridge mode with VLAN



Multi-VLAN

General				
Channel	Enable	WAN Type	VLAN Tag	Port-based Bridge
1	Yes	Ethernet(WAN1)	None	
2	Yes	Ethernet(WAN2)	None	
3	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
4	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
5	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
6	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
7	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
8	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5

Multi-VLAN Channel 3: ☒ Enable ☐ Disable

WAN Type :

General Settings

VLAN Header

VLAN Tag:

Priority:

Note: 1. Tag value must be set between 1~4095 and unique for each channel.
2. Only one channel can be untagged (equal to 0) at a time.

Bridge mode

☒ Enable

Physical Members

☐ P1 ☐ P2 ☐ P3 ☒ P4 ☒ P5

Note: 3. P1 is reserved for NAT use, and cannot be configured for bridge mode.

Set-top box (STB) or the other kinds of media devices are able to attach with Port4 or Port5 of LAN. Those devices that attached with Port4 or Port5 are able to access the services network directly which your ISP provided.