

DrayTek

Vigor2762 Series ADSL2/2+ & VDSL2 Router

Your reliable networking solutions partner



User's Guide

V1.3

Vigor2762 Series ADSL2/2+ & VDSL2 Router

User's Guide

Version: 1.3

Firmware Version: V3.9.2

(For future update, please visit DrayTek web site)

Date: January 9, 2020

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, 8, 10 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

- 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>

Table of Contents

Part I Installation	1
I-1 Introduction	2
I-1-1 Indicators and Connectors	3
I-2 Hardware Installation	6
I-2-1 Installing Vigor Router	6
I-2-2 Wall-Mounted Installation	7
I-2-3 Installing USB Printer to Vigor Router	8
I-3 Accessing Web Page	15
I-4 Changing Password	17
I-5 Dashboard	18
I-5-1 Virtual Panel	19
I-5-2 Name with a Link	19
I-5-3 Quick Access for Common Used Menu	20
I-5-4 GUI Map	21
I-5-5 Web Console	22
I-5-6 Config Backup	23
I-5-7 Manual Download	24
I-5-8 Logout	24
I-5-9 Online Status	25
I-5-9-1 Physical Connection	25
I-5-9-2 Virtual WAN	27
I-6 Quick Start Wizard	28
I-6-1 For WAN1 (ADSL)	29
I-6-2 For WAN2 (Ethernet)	33
I-6-3 For WAN3 (USB)	43
I-7 Service Activation Wizard	45
I-8 Registering Vigor Router	47
Part II Connectivity	49
II-1 WAN	50
Web User Interface	52
II-1-1 General Setup	52
II-1-1-1 WAN1 (ADSL/VDSL)	53
II-1-1-2 WAN2 (Ethernet)	55
II-1-1-3 WAN3 (USB)	56
II-1-2 Internet Access	57
II-1-2-1 Details Page for PPPoE/PPPoA in WAN1 (Physical Mode: ADSL)	59
II-1-2-2 Details Page for MPoA/Static or Dynamic IP in WAN1 (Physical Mode: ADSL)	62
II-1-2-3 Details Page for PPPoE in Ethernet WAN	65
II-1-2-4 Details Page for Static or Dynamic IP in Ethernet WAN	68
II-1-2-5 Details Page for PPTP/L2TP in Ethernet WAN	71
II-1-2-6 Details Page for 3G/4G USB Modem (PPP mode) in USB WAN	73
II-1-2-7 Details Page for 3G/4G USB Modem (DHCP mode) in USB WAN	75

II-1-2-8 Details Page for IPv6 - Offline in WAN1/WAN2/WAN3	77
II-1-2-9 Details Page for IPv6 - PPP in WAN1/WAN2	78
II-1-2-10 Details Page for IPv6 - TSPC in WAN1/WAN2/WAN3	80
II-1-2-11 Details Page for IPv6 - AICCU in WAN1/WAN2/WAN3	81
II-1-2-12 Details Page for IPv6 - DHCPv6 Client in WAN1/WAN2	83
II-1-2-13 Details Page for IPv6 - Static IPv6 in in WAN1/WAN2	84
II-1-2-14 Details Page for IPv6 - 6in4 Static Tunnel in WAN1 / WAN2	86
II-1-2-15 Details Page for IPv6 - 6rd in WAN1 / WAN2	88
II-1-3 Multi-PVC/VLAN	90
II-1-4 WAN Budget	96
II-1-4-1 General Setup	96
II-1-4-2 Status	99
Application Notes	100
A-1 How to assign an IPv6 address to LAN clients?	100
A-2 How to configure IPv6 on WAN interface?	103
II-2 LAN	108
Web User Interface	110
II-2-1 General Setup	110
II-2-1-1 Details Page for LAN1 - Ethernet TCP/IP and DHCP Setup	112
II-2-1-2 Details Page for LAN2	114
II-2-1-3 Details Page for IP Routed Subnet	116
II-2-1-4 Details Page for LAN1~ LAN2 - IPv6 Setup	118
II-2-1-5 DHCP Server Option	121
II-2-2 VLAN	123
II-2-3 Bind IP to MAC	126
II-2-4 LAN Port Mirror	128
II-2-5 Wired 802.1x	129
II-3 Hardware Acceleration	130
II-3-1 Setup	130
II-4 NAT	132
Web User Interface	133
II-4-1 Port Redirection	133
II-4-2 DMZ Host	137
II-4-3 Open Ports	140
II-4-4 Port Triggering	142
II-4-5 ALG	144
II-5 Applications	145
Web User Interface	147
II-5-1 Dynamic DNS	147
II-5-2 LAN DNS / DNS Forwarding	151
II-5-3 DNS Security	154
II-5-3-1 General Setup	154
II-5-3-2 Domain Diagnose	155
II-5-4 Schedule	156
II-5-5 RADIUS	158
II-5-6 UPnP	161

II-5-7 IGMP.....	162
II-5-7-1 General Setting	162
II-5-7-2 Working Group	163
II-5-8 Wake on LAN	163
II-5-9 SMS / Mail Alert Service.....	164
II-5-9-1 SMS Alert	164
II-5-9-2 Mail Alert	165
II-5-10 Bonjour	167
II-6 Routing.....	170
Web User Interface	171
II-6-1 Static Route	171
II-6-1-1 Static Route for IPv4	171
II-6-1-2 Static Route for IPv6	174
II-6-2 Route Policy	175
II-6-2-1 General Setup	175
II-6-2-2 Diagnose	181
Application Notes	183
A-1 How to set up Address Mapping with Route Policy?	183
A-2 How to use destination domain name in a route policy?.....	185

Part III Wireless LAN.....187

III-1 Wireless LAN	188
Web User Interface	190
III-1-1 Wireless Wizard.....	190
III-1-2 General Setup	193
III-1-3 Security.....	195
III-1-4 Access Control	198
III-1-5 WPS.....	199
III-1-6 WDS	202
III-1-7 Advanced Setting	205
III-1-8 Station Control.....	208
III-1-9 Bandwidth Management.....	209
III-1-10 AP Discovery	210
III-1-11 Airtime Fairness.....	211
III-1-12 Band Steering.....	213
III-1-13 Roaming	218
III-1-14 Station List.....	219

Part IV VoIP.....221

IV-1 VoIP	222
Web User Interface	224
IV-1-1 VoIP Wizard	224
IV-1-2 General Settings	226
IV-1-3 SIP Accounts.....	228

IV-1-4 DialPlan.....	232
<i>IV-1-4-1 Phone Book</i>	232
<i>IV-1-4-2 Digit Map</i>	234
<i>IV-1-4-3 Call Barring</i>	236
<i>IV-1-4-4 Regional</i>	238
IV-1-5 Phone Settings.....	240
IV-1-6 Status.....	244
IV-1-7 Diagnostics.....	246
<i>IV-1-7-1 Caller ID</i>	246
<i>IV-1-7-2 Send Tone</i>	246

Part V VPN.....247

V-1 VPN and Remote Access.....	248
Web User Interface.....	249
V-1-1 VPN Client Wizard.....	249
V-1-2 VPN Server Wizard.....	256
V-1-3 Remote Access Control.....	260
V-1-4 PPP General Setup.....	261
V-1-5 IPsec General Setup.....	263
V-1-6 IPsec Peer Identity.....	264
V-1-7 VPN Matcher Setup.....	267
V-1-8 OpenVPN.....	269
<i>V-1-7-1 General Setup</i>	269
<i>V-1-7-2 Client Config</i>	270
V-1-8 Remote Dial-in User.....	271
V-1-9 LAN to LAN.....	275
V-1-10 Connection Management.....	284
Application Notes.....	285
<i>A-1 How to Build a LAN-to-LAN VPN Between Vigor Routers via IPsec Main Mode</i> ...	285
V-2 SSL VPN.....	290
Web User Interface.....	291
V-2-1 General Setup.....	291
V-2-2 User Account.....	292
V-2-3 SSL Portal Online User.....	296
Application Notes.....	297
<i>A-1 Vigor Router to Vigor Router - SSL VPN</i>	297
<i>VPN Client (Dial-out Site) Setup</i>	298
<i>Establishing the VPN Tunnel</i>	300
V-3 Certificate Management.....	301
Web User Interface.....	302
V-3-1 Local Certificate.....	302
V-3-2 Trusted CA Certificate.....	306
V-3-3 Certificate Backup.....	308
V-3-4 Self-Signed Certificate.....	309

Part VI Security	311
VI-1 Firewall	312
Web User Interface	314
VI-1-1 General Setup	314
VI-1-2 Filter Setup	319
VI-1-3 DoS Defense	328
<i>V-1-3-1 DoS Defense</i>	<i>328</i>
<i>V-1-3-2 Spoofing Defense</i>	<i>331</i>
VI-1-4 Diagnose	332
Application Notes	335
<i>A-1 How to Configure Certain Computers Accessing to Internet</i>	<i>335</i>
<i>A-2 How to backup and restore firewall rule and object settings?</i>	<i>339</i>
VI-2 CSM (Central Security Management).....	341
Web User Interface	342
VI-2-1 APP Enforcement Profile	342
VI-2-2 APPE Signature Upgrade	344
VI-2-3 URL Content Filter Profile	345
VI-2-4 Web Content Filter Profile	350
VI-2-5 DNS Filter Profile	354
VI-2-6 APPE Support List	356
Application Notes	357
<i>A-1 How to Create an Account for MyVigor</i>	<i>357</i>
<i>A-2 How to Block Facebook Service Accessed by the Users via Web Content Filter / URL Content Filter</i>	<i>362</i>
<i>A-3 How to use APP Enforcement to block application like Facebook, YouTube or TeamViewer?</i>	<i>367</i>
Part VII Management	371
VII-1 System Maintenance	372
Web User Interface	373
VII-1-1 System Status	373
VII-1-2 TR-069	376
VII-1-3 Administrator Password	379
VII-1-4 User Password.....	382
VII-1-5 Login Page Greeting	385
VII-1-6 Configuration Backup.....	387
VII-1-7 SysLog/Mail Alert	390
VII-1-8 Time and Date.....	393
VII-1-9 SNMP	394
VII-1-10 Management	396
VII-1-11 Panel Control	401
VII-1-12 Self-Signed Certificate	405
VII-1-13 Reboot System.....	407
VII-1-14 Firmware Upgrade	408

VII-1-15 Firmware Backup	409
VII-1-16 Modem Code Upgrade.....	409
VII-1-17 Activation.....	410
VII-1-18 Dashboard Control	412
Application Notes	413
<i>A-1 How to prevent CPE's settings from being changed by the end-users?</i>	<i>413</i>
VII-2 Bandwidth Management.....	416
Web User Interface	418
VII-2-1 Sessions Limit.....	418
VII-2-2 Bandwidth Limit.....	420
VII-2-3 Quality of Service	422
VII-2-4 APP QoS.....	428
VII-3 Hotspot Web Portal.....	430
Web User Interface	430
VII-3-1 Profile Setup.....	430
<i>VII-3-1-1 Login Method.....</i>	<i>431</i>
<i>VII-3-1-2 Steps for Configuring a Web Portal Profile</i>	<i>431</i>
VII-3-2 Quota Management	447
Application Notes	450
<i>A-1 How to allow users login to Vigor's Hotspot with their social media accounts (e.g., Facebook & Google)</i>	<i>450</i>
<i>A-2 How to allow hotspot clients to get login PIN code via SMS?.....</i>	<i>458</i>
VII-4 Central Management (AP).....	466
Web User Interface	467
VII-4-1 Status	467
VII-4-2 WLAN Profile.....	469
VII-4-3 AP Maintenance.....	474
VII-4-4 Traffic Graph	475
VII-4-5 Load Balance	476
VII-5 Central Management (External Devices)	478
Part VIII Others	479
VIII-1 Objects Settings.....	480
Web User Interface	481
VIII-1-1 IP Object	481
VIII-1-2 IP Group.....	485
VIII-1-3 IPv6 Object.....	486
VIII-1-4 IPv6 Group	488
VIII-1-5 Service Type Object.....	489
VIII-1-6 Service Type Group	491
VIII-1-7 Keyword Object.....	493
VIII-1-8 Keyword Group	495
VIII-1-9 File Extension Object	496

VIII-1-10 SMS/Mail Service Object	498
VIII-1-11 Notification Object.....	503
VIII-1-12 String Object	504
Application Notes	505
<i>A-1 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection</i>	505
VIII-2 USB Application	509
Web User Interface	510
VIII-2-1 USB General Settings.....	510
VIII-2-2 USB User Management	511
VIII-2-3 File Explorer	514
VIII-2-4 USB Device Status.....	515
VIII-2-5 Temperature Sensor	516
VIII-2-6 Modem Support List.....	518
VIII-2-7 SMB Client Support List.....	519
Application Notes	520
<i>A-1 How can I get the files from USB storage device connecting to Vigor router? ...</i>	520

Part IX Troubleshooting523

IX-1 Diagnostics	524
Web User Interface	525
IX-1-1 Dial-out Triggering.....	525
IX-1-2 Routing Table.....	526
IX-1-3 ARP Cache Table	527
IX-1-4 IPv6 Neighbour Table	528
IX-1-5 DHCP Table	529
IX-1-6 NAT Sessions Table	530
IX-1-7 DNS Cache Table	531
IX-1-8 Ping Diagnosis	532
IX-1-9 Data Flow Monitor	534
IX-1-10 Traffic Graph	536
IX-1-11 Trace Route	537
IX-1-12 Syslog Explorer.....	538
IX-1-13 IPv6 TSPC Status	539
IX-1-14 DSL Status	540
IX-1-15 DoS Flood Table	541
IX-1-16 Route Policy Diagnosis	542
IX-2 Checking If the Hardware Status Is OK or Not.....	544
IX-3 Checking If the Network Connection Settings on Your Computer Is OK or Not.....	545
IX-4 Pinging the Router from Your Computer	548
IX-5 Checking If the ISP Settings are OK or Not.....	550
IX-6 Problems for 3G/4G Network Connection	551

IX-7 Backing to Factory Default Setting If Necessary	552
IX-8 Contacting DrayTek	553
Part X DrayTek Tools	555
X-1 SmartVPN Client.....	556
X-1-1 DrayTek Android-based SmartVPN APP for the establishment of SSL VPN connection	556
X-1-2 How to Use SmartVPN Android APP to Establish SSL VPN Tunnel?.....	557
Part XI Telnet Commands.....	561
Accessing Telnet of Vigor2762	562

Part I Installation



Installation

This part will introduce Vigor router and guide to install the device in hardware and software.

I-1 Introduction

This is a generic International version of the user guide. Specification, compatibility and features vary by region. For specific user guides suitable for your region or product, please contact local distributor.

Vigor2762 series is an ADSL2/2+ 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 2 VPN tunnels.







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

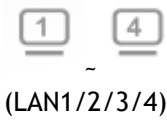
Object-based firewall is flexible and allows your network be safe. In addition, Vigor2762 Series supports USB interface for connecting USB printer to share printer, USB storage device for sharing files, or for 3G/4G WAN.

I-1-1 Indicators and Connectors

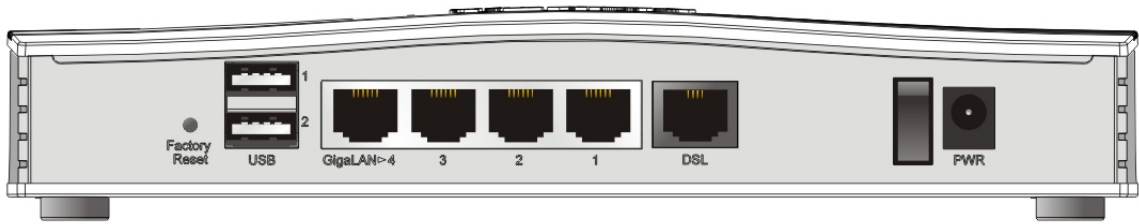
Before you use the Vigor router, please get acquainted with the LED indicators and connectors first.



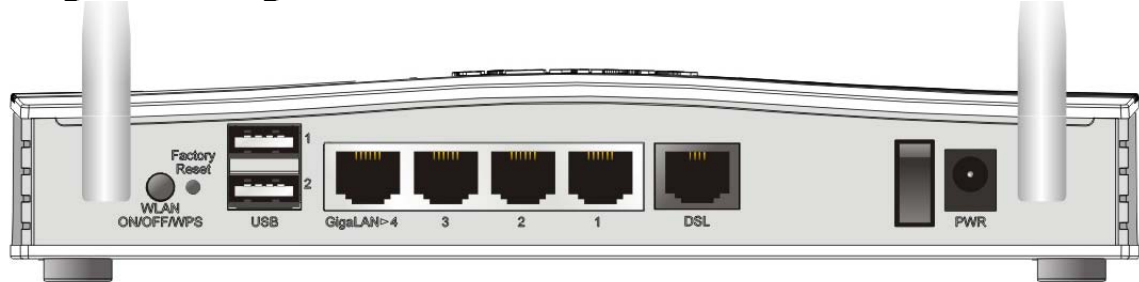
LED	Status	Explanation
 (Activity)	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
 (for "V" model)	On	The phone connected to this port is off-hook.
	Off	The phone connected to this port is on-hook.
	Blinking	A phone call comes.
 (Wireless LAN On/Off/WPS)	On (Green)	The wireless access point is ready.
	Blinking (Green)	The data is transmitting via wireless connection based on the rate of 2.4Ghz.
	Blinking (Orange)	Blinks with one second cycle for two minutes. The WPS function is active.
	Off	The wireless access point is turned off.
 (Wireless LAN On/Off/WPS)	On (Green)	The wireless access point is ready.
	Blinking (Green)	The data is transmitting via wireless connection based on the rate of 5Ghz.
	Blinking (Orange)	Blinks with one second cycle for two minutes. The WPS function is active.
 (USB)	On	A USB device is connected and active.
	Blinking	The data is transmitting.
	On	The DSL port is connected.
	Blinking	The router is ready.

	(Slowly)	
	Blinking (Quickly)	The router is trying to connect to Internet.
 (LAN1/2/3/4)	On	The LAN port is connected.
	Blinking	The data is transmitting.
	Off	The LAN port is disconnected.

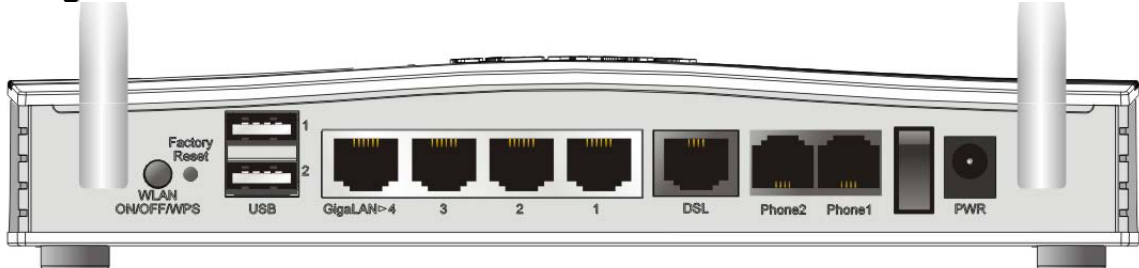
Vigor2762



Vigor2762n / Vigor2762ac



Vigor2762Vac



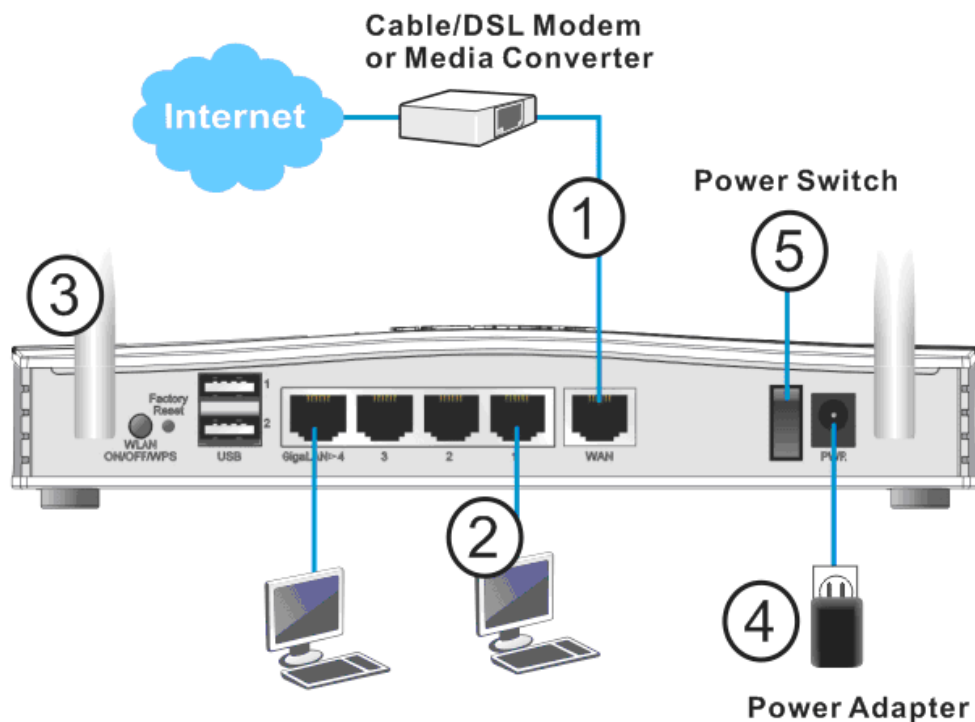
Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
WLAN ON/OFF/WPS	WLAN On - Press the button and release it within 2 seconds. When the wireless function is ready, the green LED will be on. WLAN Off - Press the button and release it within 2 seconds to turn off the WLAN function. When the wireless function is not ready, the LED will be off. WPS - When WPS function is enabled by web user interface, press this button for more than 2 seconds to wait for client's device making network connection through WPS.
USB1~USB2	Connector for a USB device (for 3G/4G USB Modem or printer).
GigaLAN1~LAN4	Connectors for local networked devices.
DSL	Connector for accessing the Internet.
Phone2/Phone1 (for "V" model)	Connector of analog phone for VoIP communication.
I / O	Power Switch.
PWR	Connector for a power adapter.

I-2 Hardware Installation

I-2-1 Installing Vigor Router

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

1. Connect the cable Modem/DSL Modem/Media Converter to any WAN port of router with Ethernet cable (RJ-45).
2. Connect the cable Modem/DSL Modem/Media Converter to any WAN port of router with Ethernet cable (RJ-45).
3. Connect detachable antennas to the router (for n/ac model only).
4. Connect one end of the power cord to the power port of this device. Connect the other end to the wall outlet of electricity.
5. Power on the router.
6. Check the ACT and DSL, LAN LEDs to assure network connection.

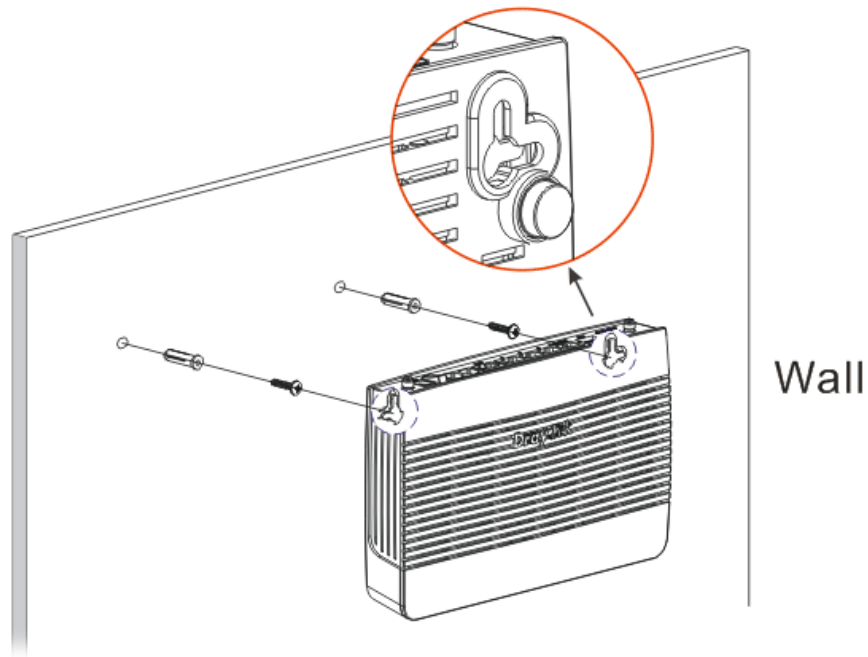


(For the detailed information of LED status, please refer to section I-1-1 Indicators and Connectors.)

I-2-2 Wall-Mounted Installation

Vigor2762 has keyhole type mounting slots on the underside.

1. A template is provided on the Vigor2762 packaging box to enable you to space the screws correctly on the wall.
2. Place the template on the wall and drill the holes according to the recommended instruction.
3. Fit screws into the wall using the appropriate type of wall plug.



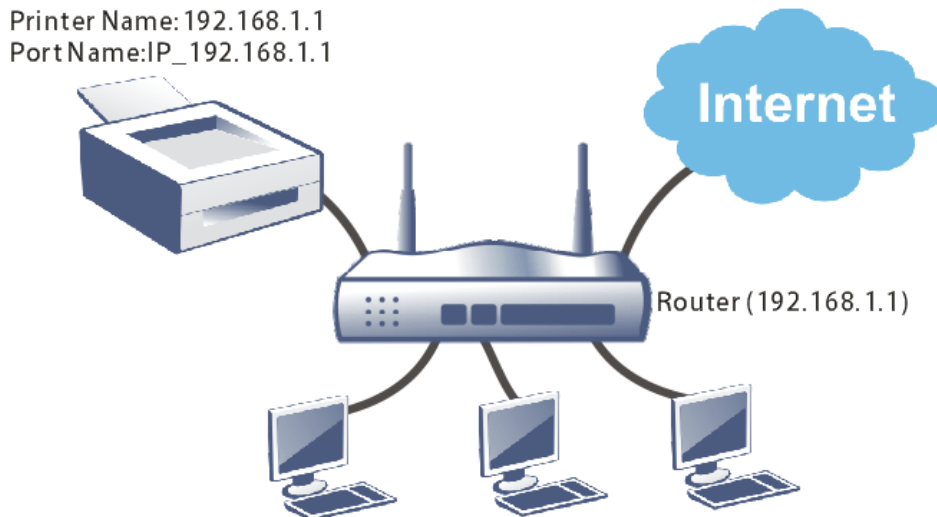
Note

The recommended drill diameter shall be 6.5mm (1/4").

4. When you finished about procedure, the router has been mounted on the wall firmly.

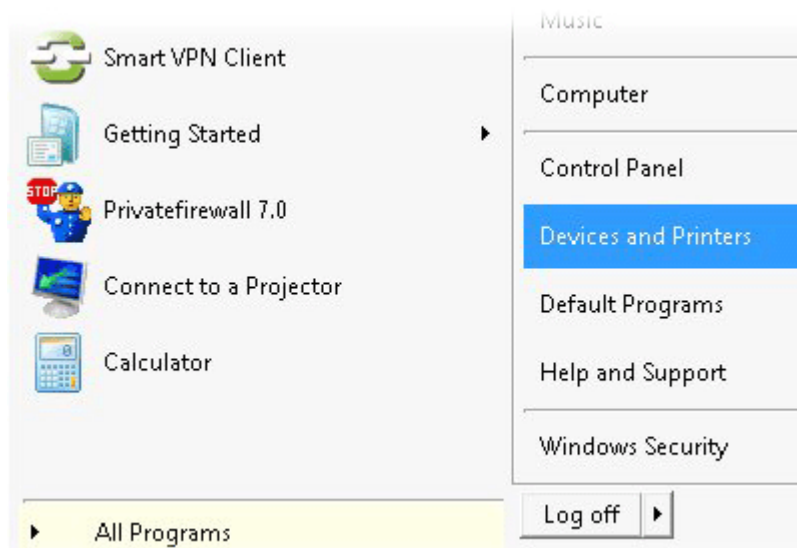
I-2-3 Installing USB Printer to Vigor Router

You can install a printer onto the router for sharing printing. All the PCs connected this router can print documents via the router. The example provided here is made based on Windows 7. For other Windows system, please visit www.DrayTek.com.

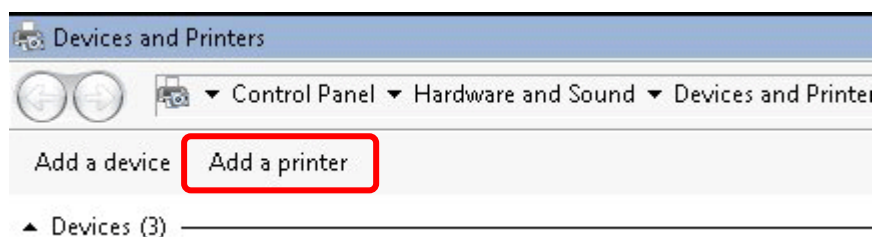


Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

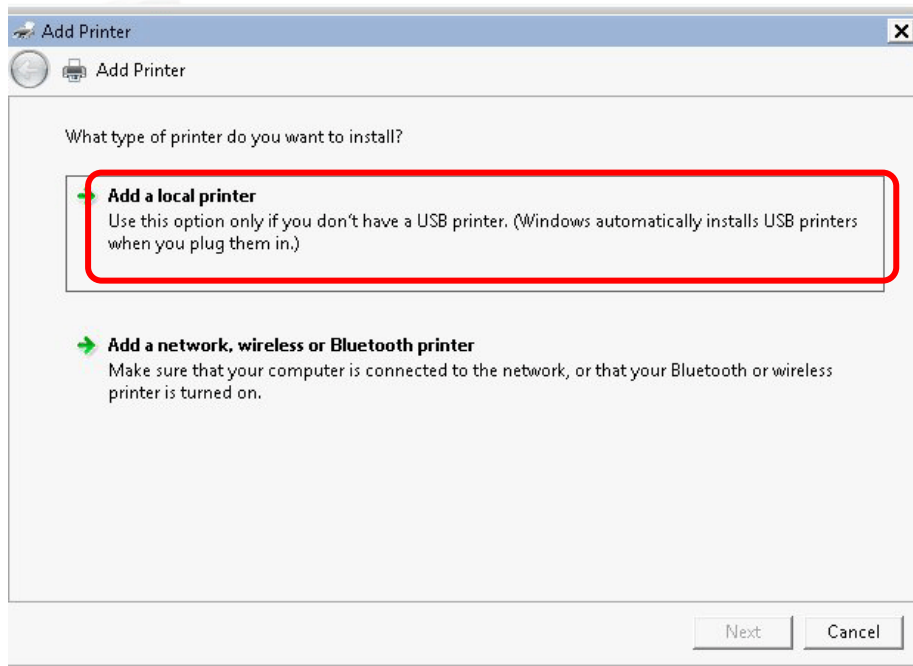
1. Connect the printer with the router through USB/parallel port.
2. Open All Programs>>Getting Started>>Devices and Printers.



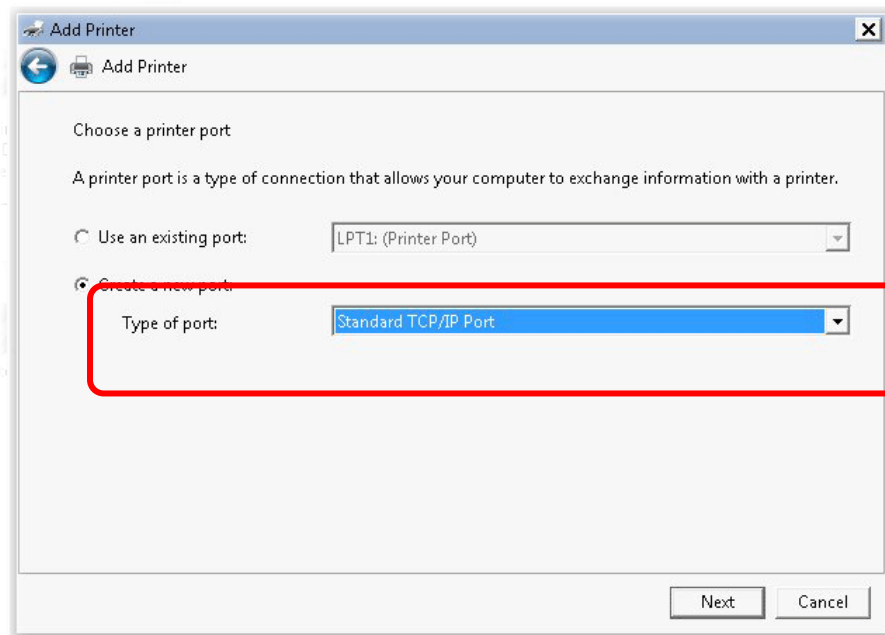
3. Click Add a printer.



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



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



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

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

- Device type: TCP/IP Device
- Hostname or IP address: 192.168.1.1
- Port name: 192.168.1.1
- Query the printer and automatically select the driver to use

Buttons: Next, Cancel

7. Click Standard and choose Generic Network Card.

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

Additional port information required

The device is not found on the network. Be sure that:

1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.

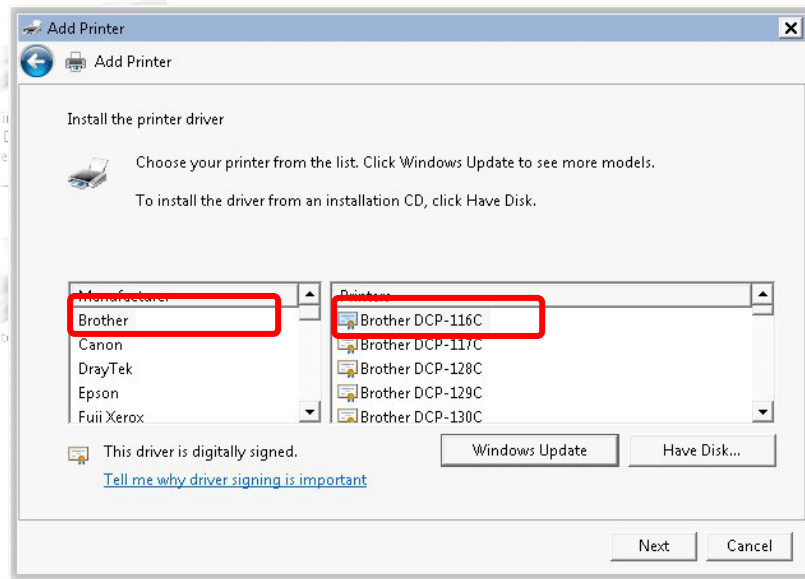
If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.

Device Type

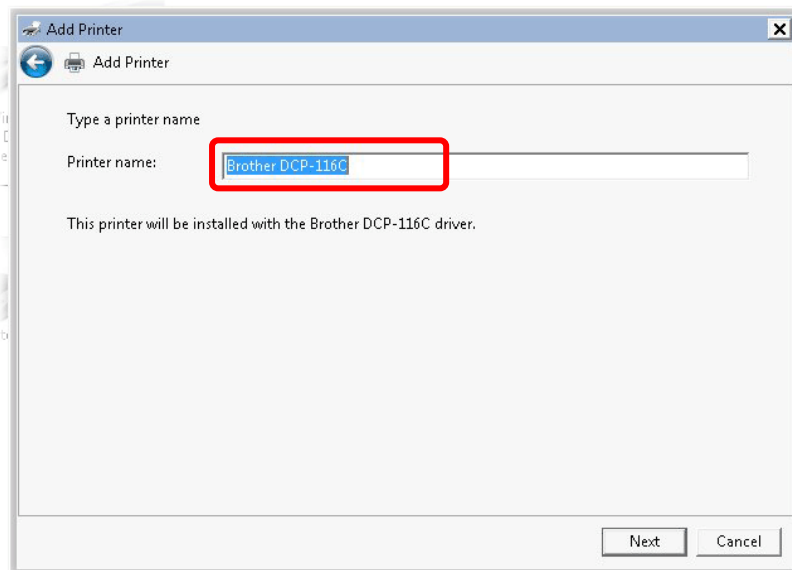
- Standard: Generic Network Card
- Custom: Settings...

Buttons: Next, Cancel

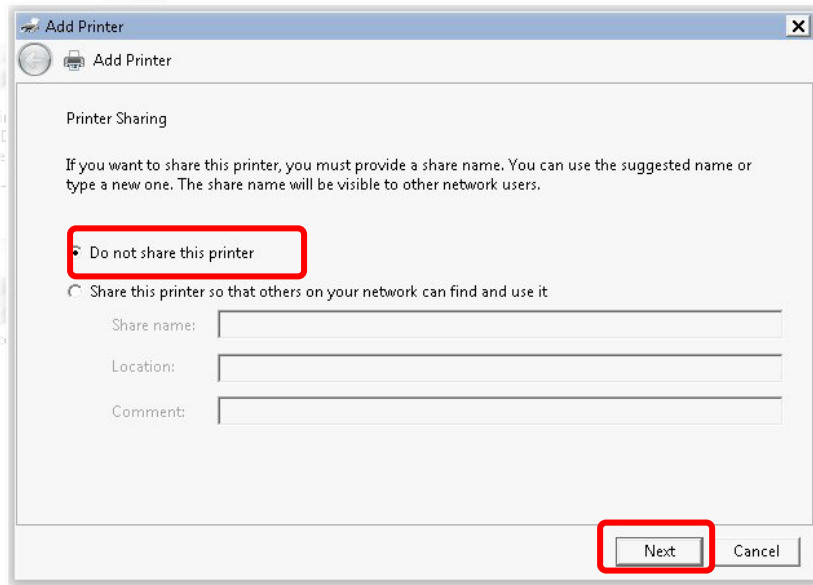
- Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click Next.



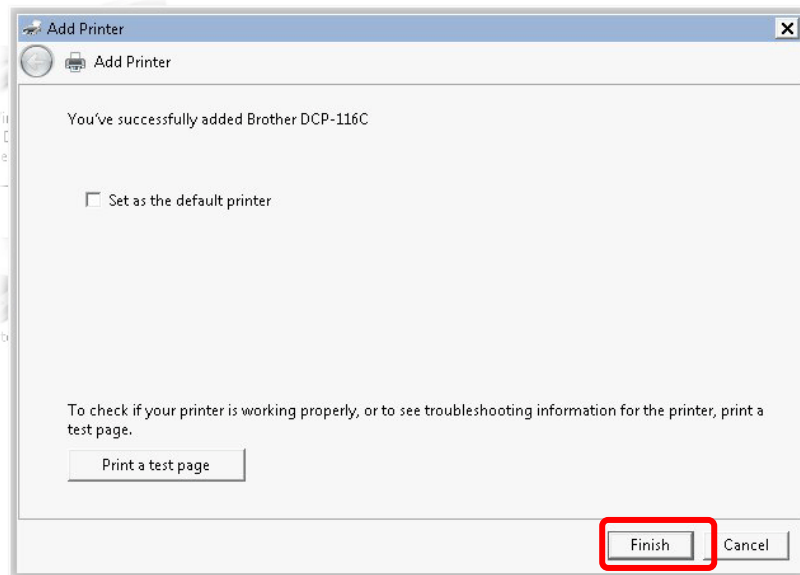
- Type a name for the chosen printer. Click Next.



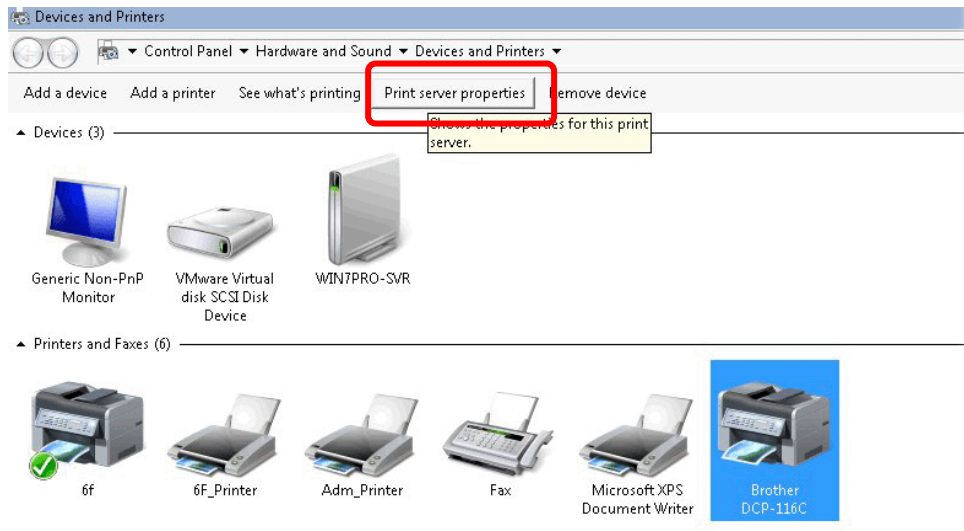
10. Choose Do not share this printer and click Next.



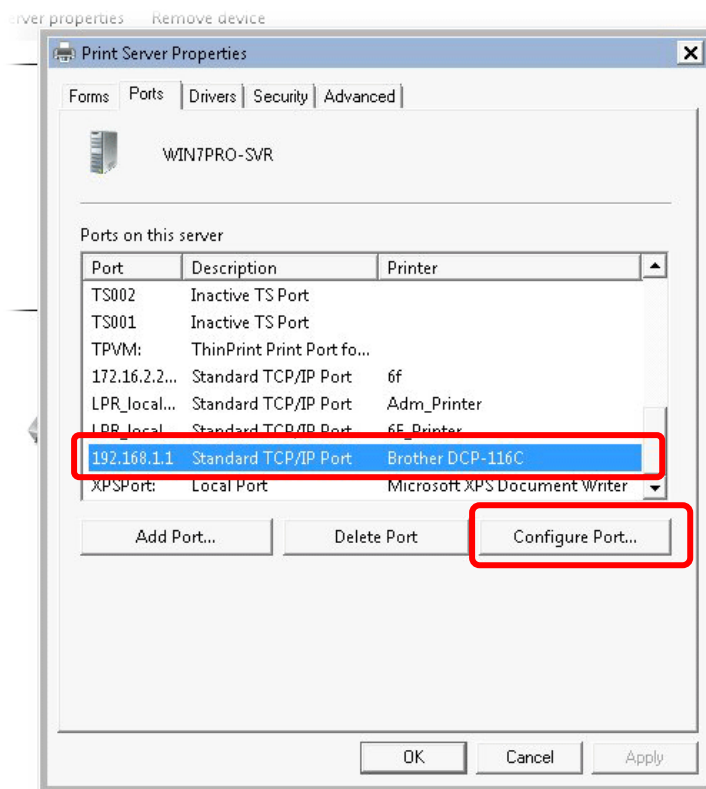
11. Then, in the following dialog, click Finish.



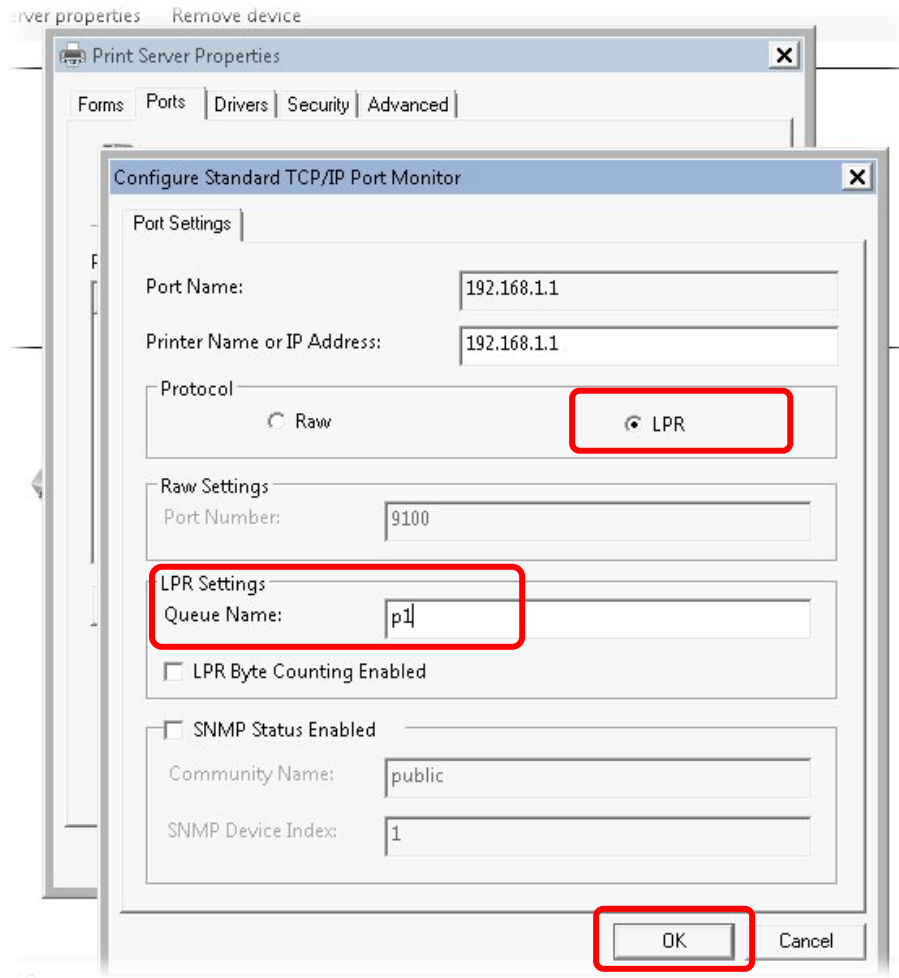
12. The new printer has been added and displayed under Printers and Faxes. Click the new printer icon and click Printer server properties.



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



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



I-3 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.



DrayTek **Vigor2762 Series**

Login

Username

Password

Login

Copyright © 2000- 2017 DrayTek Corp. All Rights Reserved.

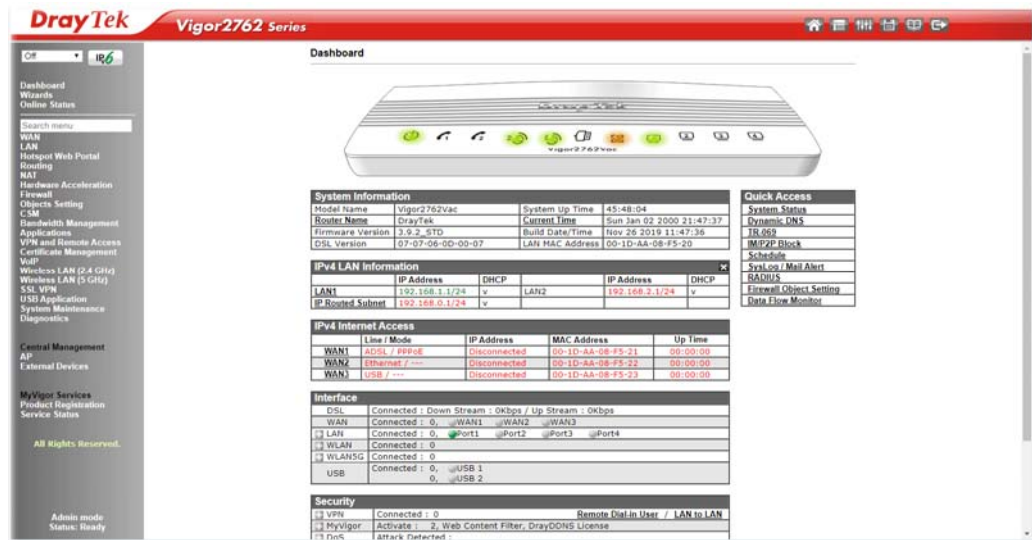
3. Please type “admin/admin” as the Username/Password and click Login.



Info

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

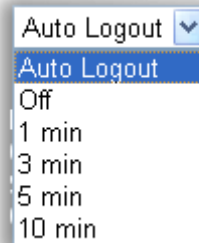
- Now, the Main Screen will appear.



Info

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.



I-4 Changing Password

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

1. Open a web browser on your PC and type `http://192.168.1.1`. A pop-up window will open to ask for username and password.
2. Please type “admin/admin” as Username/Password for accessing into the web user interface with admin mode.
3. Go to System Maintenance page and choose Administrator Password.

System Maintenance >> Administrator Password Setup

Administrator Password

Old Password	<input type="text" value="Max. 83 characters"/>
New Password	<input type="text" value="Max. 83 characters"/>
Confirm Password	<input type="text" value="Max. 83 characters"/>

Enable 'admin' account login to Web UI from the Internet
 Use only advanced authentication method for Admin "WAN" login
 Mobile one-Time Passwords(mOTP)
PIN Code Secret
 2-Step Authentication

4. Enter the login password (the default is “admin”) on the field of Old Password. Type New Password and Confirm Password. Then click OK to continue.



Info

The maximum length of the password you can set is 23 characters.

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

The image shows the login page for a DrayTek Vigor2762 Series router. The page has a red header with the DrayTek logo and "Vigor2762 Series". Below the header is a black bar with the word "Login" in white. The main content area is white and contains two input fields: "Username" with the value "admin" and "Password" with five dots. A "Login" button is positioned below the password field. At the bottom of the page, there is a copyright notice: "Copyright © 2000-2017 DrayTek Corp. All Rights Reserved."



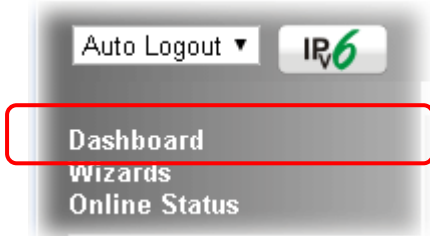
Info

Even the password is changed, the Username for logging onto the web user interface is still “admin”.

I-5 Dashboard

Dashboard shows the connection status including System Information, IPv4 Internet Access, IPv6 Internet Access, Interface (physical connection), Security and Quick Access.

Click Dashboard from the main menu on the left side of the main page.



A web page with default selections will be displayed on the screen. Refer to the following figure:

Dashboard

The router shown is a white, rectangular device with the DrayTek logo and 'Vigor2762Vac' printed on the front. It features several status LEDs: a power LED (green), two LAN LEDs (1 and 2, green), two WAN LEDs (5 and 6, green), a DSL LED (orange), a WLAN LED (green), and four numbered LAN port LEDs (2, 3, 4, and 5).

System Information			
Model Name	Vigor2762Vac	System Up Time	45:48:04
Router Name	DrayTek	Current Time	Sun Jan 02 2000 21:47:37
Firmware Version	3.9.2_STD	Build Date/Time	Nov 26 2019 11:47:36
DSL Version	07-07-06-0D-00-07	LAN MAC Address	00-1D-AA-08-F5-20

IPv4 LAN Information			
	IP Address	DHCP	IP Address
LAN1	192.168.1.1/24	v	LAN2
IP Routed Subnet	192.168.0.1/24	v	192.168.2.1/24

IPv4 Internet Access				
	Line / Mode	IP Address	MAC Address	Up Time
WAN1	ADSL / PPPoE	Disconnected	00-1D-AA-08-F5-21	00:00:00
WAN2	Ethernet / ---	Disconnected	00-1D-AA-08-F5-22	00:00:00
WAN3	USB / ---	Disconnected	00-1D-AA-08-F5-23	00:00:00

Interface	
DSL	Connected : Down Stream : 0Kbps / Up Stream : 0Kbps
WAN	Connected : 0, <input type="radio"/> WAN1 <input type="radio"/> WAN2 <input type="radio"/> WAN3
LAN	Connected : 0, <input checked="" type="radio"/> Port1 <input type="radio"/> Port2 <input type="radio"/> Port3 <input type="radio"/> Port4
WLAN	Connected : 0
WLAN5G	Connected : 0
USB	Connected : 0, <input type="radio"/> USB 1 <input type="radio"/> USB 2

Quick Access	
System Status	
Dynamic DNS	
TR-069	
IM/P2P Block	
Schedule	
SysLog / Mail Alert	
RADIUS	
Firewall Object Setting	
Data Flow Monitor	

I-5-1 Virtual Panel

On the top of the Dashboard, a virtual panel (simulating the physical panel of the router) displays the physical interface connection. It will be refreshed every five seconds. When you move and click the mouse cursor on LEDs (except ACT), USB ports, LAN, or WAN, related web setting page will be open for you to configure if required.

Dashboard



For detailed information about the LED display, refer to I-1-1 LED Indicators and Connectors.

I-5-2 Name with a Link

A name with a link (e.g., [Router Name](#), [Current Time](#), [WANx](#) and etc.) below means you can click it to open the configuration page for modification.

System Information			
Model Name	Vigor2762Vac	System Up Time	45:48:04
Router Name	DrayTek	Current Time	Sun Jan 02 2000 21:47:37
Firmware Version	3.9.2_STD	Build Date/Time	Nov 26 2019 11:47:36
DSL Version	07-07-06-0D-00-07	LAN MAC Address	00-1D-AA-08-F5-20

IPv4 LAN Information					
	IP Address	DHCP		IP Address	DHCP
LAN1	192.168.1.1/24	v	LAN2	192.168.2.1/24	v
IP Routed Subnet	192.168.0.1/24	v			

IPv4 Internet Access				
	Line / Mode	IP Address	MAC Address	Up Time
WAN1	ADSL / PPPoE	Disconnected	00-1D-AA-08-F5-21	00:00:00
WAN2	Ethernet / ---	Disconnected	00-1D-AA-08-F5-22	00:00:00
WAN3	USB / ---	Disconnected	00-1D-AA-08-F5-23	00:00:00

Interface	
DSL	Connected : Down Stream : 0Kbps / Up Stream : 0Kbps
WAN	Connected : 0, <input type="radio"/> WAN1 <input type="radio"/> WAN2 <input type="radio"/> WAN3
LAN	Connected : 0, <input checked="" type="radio"/> Port1 <input type="radio"/> Port2 <input type="radio"/> Port3 <input type="radio"/> Port4
WLAN	Connected : 0
WLAN5G	Connected : 0
USB	Connected : 0, <input type="radio"/> USB 1 0, <input type="radio"/> USB 2

I-5-3 Quick Access for Common Used Menu

All the menu items can be accessed and arranged orderly on the left side of the main page for your request. However, some important and common used menu items which can be accessed in a quick way just for convenience.

Look at the right side of the Dashboard. You will find a group of common used functions grouped under Quick Access.

Quick Access
System Status
Dynamic DNS
TR-069
IM/P2P Block
Schedule
SysLog / Mail Alert
RADIUS
Firewall Object Setting
Data Flow Monitor

The function links of System Status, Dynamic DDNS, TR-069, User Management, IM/P2P Block, Schedule, Syslog/Mail Alert, RADIUS, Firewall Object Setting and Data Flow Monitor are displayed here. Move your mouse cursor on any one of the links and click on it. The corresponding setting page will be open immediately.

In addition, quick access for VPN security settings such as Remote Dial-in User and LAN to LAN are located on the bottom of this page. Scroll down the page to find them and use them if required.

Interface	
DSL	Connected : Down Stream : 0Kbps / Up Stream : 0Kbps
WAN	Connected : 0, <input type="radio"/> WAN1 <input type="radio"/> WAN2 <input type="radio"/> WAN3
<input type="checkbox"/> LAN	Connected : 0, <input checked="" type="radio"/> Port1 <input type="radio"/> Port2 <input type="radio"/> Port3 <input type="radio"/> Port4
<input type="checkbox"/> WLAN	Connected : 0
<input type="checkbox"/> WLAN5G	Connected : 0
USB	Connected : 0, <input type="radio"/> USB 1 0, <input type="radio"/> USB 2

Security	
<input type="checkbox"/> VPN	Connected : 0 Remote Dial-in User / LAN to LAN
<input type="checkbox"/> MyVigor	Activate : 2, Web Content Filter, DrayDDNS License
<input type="checkbox"/> DoS	Attack Detected :

Note that there is a plus () icon located on the left side of VPN/LAN. Click it to review the VPN connection(s) used presently.

Security				
VPN	Connected : 1	Remote Dial-in User / LAN to LAN		
	Current Page: 1	Page No.	1	<input type="button" value="Go To"/>
Name / User	Type / Security	Host IP	Up Time	
V2920	IPsec/3DES	172.16.2.145	0:0:20	

User Mode is OFF now.

WAN	Connected : 2, <input checked="" type="radio"/> WAN1 <input checked="" type="radio"/> WAN2 <input type="radio"/> WAN3		
LAN	Connected : 3, <input checked="" type="radio"/> LAN1 <input checked="" type="radio"/> LAN2 <input type="radio"/> LAN3 <input type="radio"/> LAN4 <input type="radio"/> LAN5 <input type="radio"/> LAN6		
	Host ID	IP Address	MAC
	ALPHA-NB	10.28.60.13	1C-4B-D6-D2-D7-DB
		10.28.60.14	00-15-AF-09-7E-FA
		10.28.60.11	00-50-7F-C9-76-45

Host connected physically to the router via LAN port(s) will be displayed with green circles in the field of Connected.

All of the hosts (including wireless clients) displayed with Host ID, IP Address and MAC address indicates that the traffic would be transmitted through LAN port(s) and then the WAN port. The purpose is to perform the traffic monitor of the host(s).

I-5-4 GUI Map



All the functions the router supports are listed with table clearly in this page. Users can click the function link to access into the setting page of the function for detailed configuration. Click the icon on the top of the main screen to display all the functions.

GUI Map

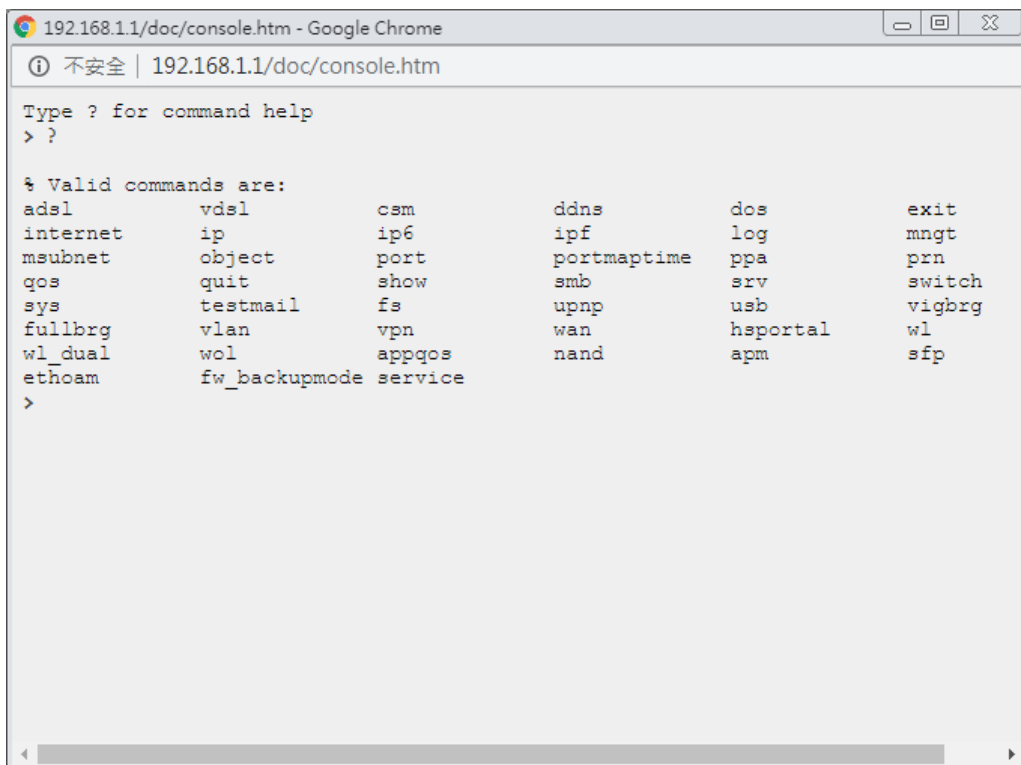
Dashboard		Certificate Management	Local Certificate Trusted CA Certificate Certificate Backup
Wizards	Quick Start Wizard Service Activation Wizard VPN Client Wizard VPN Server Wizard Wireless Wizard VoIP Wizard	VoIP	General Settings
Online Status	Physical Connection Virtual WAN	Wireless LAN (2.4 GHz)	General Setup Security Access Control WPS WDS Advanced Setting Station Control Bandwidth Management AP Discovery Airtime Fairness Band Steering Roaming Station List
WAN	General Setup Internet Access Multi-PVC WAN Budget	Wireless LAN (5 GHz)	General Setup Security Access Control WPS
LAN	General Setup VLAN Bind IP to MAC LAN Port Mirror Wired 802.1X		
Hotspot Web Portal	Profile Setup Quota Management		

I-5-5 Web Console



It is not necessary to use the telnet command via DOS prompt. The changes made by using web console have the same effects as modified through web user interface. The functions/settings modified under Web Console also can be reviewed on the web user interface.

Click the Web Console icon on the top of the main screen to open the following screen.



I-5-6 Config Backup



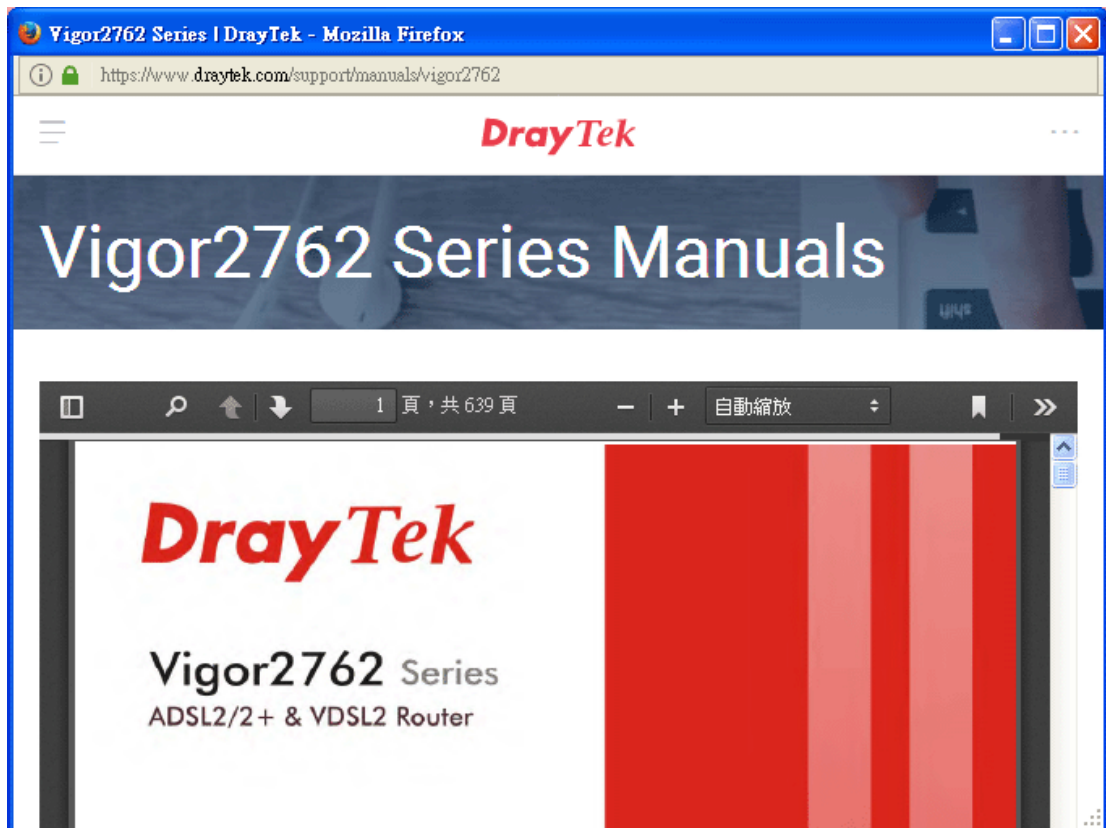
There is one way to store current used settings quickly by clicking the Config Backup icon. It allows you to backup current settings as a file. Such configuration file can be restored by using System Maintenance>>Configuration Backup.

Simply click the icon on the top of the main screen to store the setting.

I-5-7 Manual Download



Click this icon to open online user's guide of Vigor router. This document offers detailed information for the settings on web user interface.



I-5-8 Logout



Click this icon to exit the web user interface.

I-5-9 Online Status

[Wizards](#)
[Online Status](#)
[Physical Connection](#)
[Virtual WAN](#)

I-5-9-1 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		System Uptime: 1day 5:29:14			
IPv4		IPv6			
LAN Status					
IP Address		TX Packets	RX Packets	Router Primary DNS:	Router Secondary DNS:
192.168.1.1		5,620	15,414	8.8.8.8	8.8.4.4
WAN 1 Status >> Dial PPPoE					
Enable	Line	Name	Mode	Up Time	
Yes	VDSL2		PPPoE	00:00:00	
IP	GW IP	TX Bytes	TX Rate(bps)	RX Bytes	RX Rate(bps)
---	---	0 (B)	0	0 (B)	0
WAN 2 Status					
Enable	Line	Name	Mode	Up Time	
No	Ethernet		---	00:00:00	
IP	GW IP	TX Bytes	TX Rate(bps)	RX Bytes	RX Rate(bps)
---	---	0 (B)	0	0 (B)	0
WAN 3 Status					
Enable	Line	Name	Mode	Up Time	Signal
Yes	USB		---	00:00:00	-
IP	GW IP	TX Bytes	TX Rate(bps)	RX Bytes	RX Rate(bps)
---	---	0 (B)	0	0 (B)	0
Line 1 Information (VDSL2 Firmware Version: 779517_A/B/C)					
Profile	State	UP Speed	Down Speed	SNR Upstream	SNR Downstream
	TRAINING	0 (Kbps)	0 (Kbps)	0 (dB)	0 (dB)

Physical Connection for IPv6 Protocol

Online Status

Physical Connection		System Uptime: 2days 20:16:48	
IPv4		IPv6	
LAN Status			
IP Address FE80::21D:A AFF:FE00:0/64 (Link)			
TX Packets 1,065	RX Packets 0	TX Bytes 83,078	RX Bytes 0
WAN1 IPv6 Status			
Enable No	Mode Offline	Up Time ---	
IP ---			Gateway IP ---
WAN2 IPv6 Status			
Enable No	Mode Offline	Up Time ---	
IP ---			Gateway IP ---
WAN3 IPv6 Status			
Enable No	Mode Offline	Up Time ---	
IP ---			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 /WAN4 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</p>

Item	Description
	interface.

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> <p>Up Time - Displays the total uptime of the interface.</p> <p>IP - Displays the IP address of the WAN interface.</p> <p>Gateway IP - Displays the IP address of the default gateway.</p>



Info

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.

I-5-9-2 Virtual WAN

Such page displays the virtual WAN connection information.

Virtual WAN are used by TR-069 management, VoIP service and so on.

The field of Application will list i-9the purpose of such WAN connection.

I-6 Quick Start Wizard

Quick Start Wizard can help you to deploy and use the router easily and quickly. Click Wizards>>Quick Start Wizard. 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**.

Old Password	<input type="text"/>
New Password	<input type="text" value="Max 23 characters"/>
Confirm Password	<input type="text"/>

Hint: If you want to keep the password unchanged, leave the password blank and press "Next" button to skip this process.

On the next page as shown below, please select the WAN interface (WAN 1 to WAN3) that you use. If DSL interface is used, please choose WAN1; if Ethernet interface is used, please choose WAN2; if 3G/4G USB modem is used, please choose WAN3. For WAN2, choose Auto negotiation as the physical type for your router.

Quick Start Wizard

WAN Interface

WAN Interface:	<input type="text" value="WAN1"/>
Display Name:	<input type="text"/>
Physical Mode:	ADSL / VDSL2
Physical Type:	<input type="text" value="Auto negotiation"/>
VLAN Tag insertion (ADSL):	<input type="text" value="Disable"/>
VLAN Tag insertion (VDSL2):	<input type="text" value="Enable"/>
Tag value	<input type="text" value="0"/> (0~4095)
Priority	<input type="text" value="0"/> (0~7)

WAN1- WAN3 will bring up different configuration page. Refer to the following sections for detailed information.

I-6-1 For WAN1 (ADSL)

WAN1 is specified for ADSL or VDSL2 connection.

Quick Start Wizard

WAN Interface

WAN Interface:	<input type="text" value="WAN1"/>
Display Name:	<input type="text"/>
Physical Mode:	ADSL / VDSL2
Physical Type:	Auto negotiation
VLAN Tag insertion (ADSL):	Disable
VLAN Tag insertion (VDSL2):	Enable
Tag value	<input type="text" value="0"/> (0~4095)
Priority	<input type="text" value="0"/> (0~7)

Available settings are explained as follows:

Item	Description
Display Name	Type a name to identify such WAN.
VLAN Tag insertion (VDSL2)/(ADSL)	The settings configured in this field are available for WAN1 and WAN2. 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 Enter the tag value and specify the priority for the packets sending by WAN1. Disable - Disable the function of VLAN with tag. Tag value - Enter the value as the VLAN ID number. The range is from 0 to 4095. Priority - Enter the packet priority number for such VLAN. The range is from 0 to 7.

Please select the appropriate Internet access type according to the information from your ISP. Click Next.

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

For ADSL Only:

Encapsulation

VPI

VCI

Fixed IP Yes No(Dynamic IP)

IP Address

Subnet Mask

Default Gateway

Primary DNS

Second DNS

Available settings are explained as follows:

Item	Description
Protocol / Encapsulation	Choose PPPoE/PPPoA 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	Enter the IP address if Fixed IP is enabled.
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)	84005755@hinet.net
Username	84005755
Password	*****
Confirm Password	*****

Available settings are explained as follows:

Item	Description
Service Name (Optional)	Enter the description of the specific network service.
User Name	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	ReEnter 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 / VDSL2
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!

- Now, you can enjoy surfing on the Internet.

MPoA

- Choose WAN1 as WAN Interface and click the Next button; you will get the following page.

Quick Start Wizard

Connect to Internet

WAN 1

Protocol MPoA / Static or Dynamic IP ▾

For ADSL Only:

Encapsulation 1483 Bridged IP LLC ▾

VPI Auto detect

VCI

Fixed IP Yes No(Dynamic IP)

IP Address

Subnet Mask

Default Gateway

Primary DNS

Second DNS

Available settings are explained as follows:

Item	Description
Protocol	There are two modes offered for you to choose for WAN1 interface. Choose MPoA as the protocol.
For ADSL Only	Such field is provided for ADSL only. You have to choose encapsulation and Enter the values for VPI and VCI. Or, click Auto detect to find out the best values. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <div style="border: 1px solid gray; padding: 2px;">1483 Bridged IP LLC ▾</div> <div style="border: 1px solid gray; padding: 2px; background-color: #e0e0e0;">1483 Bridged IP LLC</div> <div style="border: 1px solid gray; padding: 2px;">1483 Routed IP LLC</div> <div style="border: 1px solid gray; padding: 2px;">1483 Bridged IP VC-Mux</div> <div style="border: 1px solid gray; padding: 2px;">1483 Routed IP VC-Mux (IPoA)</div> <div style="border: 1px solid gray; padding: 2px;">1483 Bridged IP (IPoE)</div> <p style="margin-top: 5px;"><input type="radio"/> Yes <input checked="" type="radio"/> No(Dynamic IP)</p> </div>
Fixed IP	Click Yes to enable Fixed IP feature.
IP Address	Enter the IP address if Fixed IP is enabled.
Subnet Mask	Enter the subnet mask.
Default Gateway	Enter 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.

- 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 / VDSL2
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

- 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.

I-6-2 For WAN2 (Ethernet)

WAN2 is dedicated to physical mode in Ethernet. 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.

Quick Start Wizard

WAN Interface

WAN Interface:	WAN2 ▾
Display Name:	<input type="text"/>
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.
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 Enter the tag value and specify the priority for the packets sending by WAN2.</p> <p>Disable - Disable the function of VLAN with tag. Tag value - Enter the value as the VLAN ID number. The range is form 0 to 4095. Priority - Enter the packet priority number for such VLAN. The range is from 0 to 7.</p>

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)

Username

Password

Confirm Password

Available settings are explained as follows:

Item	Description
Service Name (Optional)	Enter the description of the specific network service.
Username	Assign a specific valid user name provided by the ISP. Note: The maximum length of the user name you can set is 63 characters.
Password	Assign a valid password provided by the ISP. Note: The maximum length of the password you can set is 62 characters.
Confirm Password	ReEnter 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

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.

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

PPTP Client Mode

WAN 2
Enter the username, password, WAN IP configuration and PPTP server IP provided by your ISP.

Username
Password
Confirm Password

WAN IP Configuration
 Obtain an IP address automatically
 Specify an IP address

IP Address
Subnet Mask
Gateway
Primary DNS
Second DNS
PPTP Server

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
Username	Assign a specific valid user name provided by the ISP. The maximum length of the user name you can set is 63 characters.
Password	Assign a valid password provided by the ISP. The maximum length of the password you can set is 62 characters.
Confirm Password	ReEnter 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> <ul style="list-style-type: none"> ● IP Address - Enter the IP address. ● Subnet Mask -Enter the subnet mask. ● Gateway - Enter the IP address of the gateway. ● Primary DNS -Type in the primary IP address for the router. ● Second DNS -Type in secondary IP address for necessity in the future.
PPTP Server / L2TP Server	Enter 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:	PPTP

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

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

Quick Start Wizard Setup OK!

- Now, you can enjoy surfing on the Internet.

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 192.168.3.102
Subnet Mask 255.255.255.0
Gateway 192.168.3.1
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	Enter the IP address.
Subnet Mask	Enter the subnet mask.
Gateway	Enter 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
<p>Click Back to modify changes if necessary. Otherwise, click Finish to save the current settings and restart the Vigor router.</p>	

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 00 - 1D - AA - 00 - 00 - 02 (optional)

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
Host Name	Enter the name of the host. Note: The maximum length of the host name you can set is 39 characters.
MAC	Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to enter the MAC address.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

3. After 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.

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.

I-6-3 For WAN3 (USB)

WAN3/WAN4 is dedicated to physical mode in USB.

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 getting the following page.

Quick Start Wizard

Connect to Internet

WAN 3	
Internet Access :	3G/4G USB Modem(PPP mode) ▾ 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)	<p>SIM Pin code -Type PIN code of the SIM card that will be used to access Internet. The maximum length of the pin code you can set is 15 characters.</p> <p>Modem Initial String - Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP. The maximum length of the string you can set is 47 characters.</p>

	APN Name - APN means Access Point Name which is provided and required by some ISPs. Enter the name and click Apply .
--	---

3. 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.

< Back

Next >

Finish

Cancel

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.

I-7 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 of WCF directly without accessing into the server (**MyVigor**) located on <http://myvigor.draytek.com>. For using Web Content Filter Profile, please refer to later section Web Content Filter Profile for detailed information.

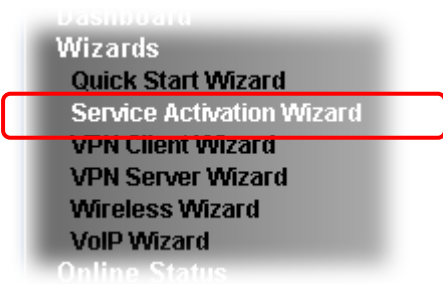
Now, follow the steps listed below to activate WCF feature for your router.



Info

Such function is available only for Admin Mode.

1. Open Wizards>>Service Activation Wizard.



2. In the following page, you can activate the web content filter services, APP Enforcement service and Dynamic DNS Service at the same time or individually. When you finish the selection, check the box of "I have read..." and click Next.

Service Activation Wizard

Select the service type that you want to activate

Activation Date : 2019-02-01

Web Content Filter(WCF) Service :

BPjM [License Agreement](#)
This is a web content filter that is provided by the German government. It is a free service without any guarantee and will expire one year after activation. You may re-activate the service after expiry.

Cyren 30-Days Free Trial [License Agreement](#)
This is a worldwide web content filter service. The free trail license can only be used once. At the end of the free trail period you may purchase the official one-year Cyren Web Content Filter from an authorized DrayTek reseller.

APP Enforcement(APPE) Service :

DT-APPE [License Agreement](#)
Upgrade APPE Signature automatically.

Dynamic DNS(DDNS) Service :

DT-DDNS [License Agreement](#)
This Dynamic Domain Name service is provided by DrayTek Corporation. To activate the DrayDDNS (Global) service, please select this option to activate the license. This is a 1-year free license key. For re-activation after expiry, you have to obtain a new license from MyVigor website (<https://myvigor.draytek.com>).

I agree to let the MyVigor server record the WAN or Internet IP address of this router in order to activate the DrayDDNS service.
You can stop this service and clear your IP address at any time.

Domain Name : 2019020111592701 .draydns.com

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

Next >

Cancel



Info

BPjM is web content filter (WCF) for German Speaking users. It is ideal for your family to provide more Internet security for youngsters.

DT-APPE, developed by DrayTek, offers a mechanism to upgrade APPE signature automatically.

DT-DDNS, developed by DrayTek, offers one year free charge service of dynamic DNS service for internal use.

3. Setting confirmation page will be displayed as follows, please click Activate.

Service Activation Wizard

Please confirm your settings

Service Type :	Trial version
Service Activated :	Web Content Filter (BPjM)
	APP Enforcement (DT-APPE)
	Dynamic DNS (2019020111592701.drayddns.com)
Please click Back to re-select service type you to activate.	

< Back Activate Cancel



Info

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

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

DrayTek Service Activation

Service Name	Start Date	Expire Date	Status
Web Content filter	2019-02-01	2019-03-03	Cyren
APP Enforcement	---	---	Not Activated
DDNS	2019-02-01	2020-02-01	DT-DDNS

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.

I-8 Registering Vigor Router

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

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

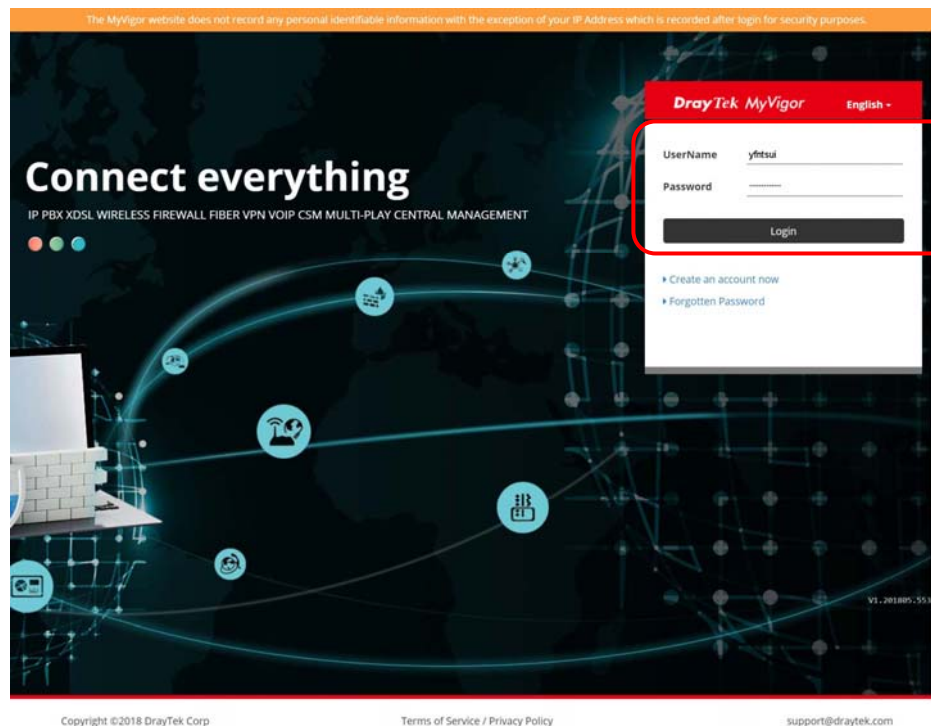


- 2 Click Support Area>>Production Registration from the home page.



Support Area
Product Registration

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



The MyVigor website does not record any personal identifiable information with the exception of your IP Address which is recorded after login for security purposes.

DrayTek MyVigor English -

UserName yhtsui

Password

Login

► Create an account now

► Forgotten Password

Copyright ©2018 DrayTek Corp. Terms of Service / Privacy Policy support@draytek.com



Info

If you haven't an accessing account, please refer to section Creating an Account for MyVigor to create your own one. Please read the articles on the Agreement regarding user rights carefully while creating a user account.

- The following page will be displayed after you logging in MyVigor. Type a nickname for the router, then click Add.

DrayTek MyVigor

Login User : carrieni (Logout)

My Information - My Products

Registration Device :

*Nickname :

Registration Date : 01-17-2017

Serial number : 2017011710270702

Last login time : 2016-09-12 13:53:29
Last login from : 111.251.222.175

Rows : 10 Page : 1

Serial Number / Host ID	Device Name	Model	Note
111900325027	2130	Vigor2130	
2013030811172502	vigor2760	Vigor2760	
2015022415571701	Vigor2132ac	Vigor2132	

Copyrights © DrayTek Corp.

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

Your device has been successfully added to the database.



- After clicking OK, you will see the following page. Your router has been registered to myvigor website successfully.

DrayTek MyVigor

Login User : carrieni (Logout)

My Information - My Products

Last login time : 2016-09-12 13:53:29
Last login from : 111.251.222.175

Rows : 10 Page : 1

Serial Number / Host ID	Device Name	Model	Note
111900325027	2130	Vigor2130	
2013030811172502	vigor2760	Vigor2760	
2015022415571701	Vigor2132ac	Vigor2132	
2015030413341201	Vigor2762	Vigor2762	

Copyrights © DrayTek Corp.

Part II Connectivity



WAN

It means wide area network. Public IP will be used in WAN.



LAN

It means local area network. Private IP will be used in 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.



NAT

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.



Applications

DNS, LAN DNS, UPnP, IGMP, WOL, RADIUS, ...



Routing

Static Route, Route Policy

II-1 WAN

It allows users to access Internet.

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.

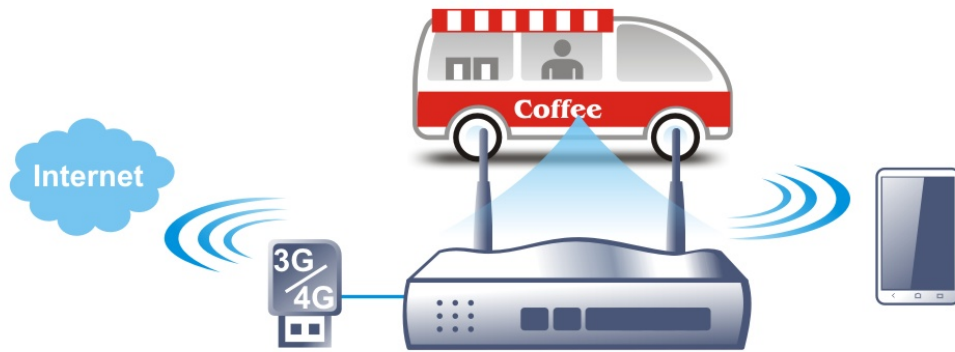
Get Your Public IP Address from ISP

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, Vigor2762 adds the function of 3G/4G network connection for such purpose. By connecting 3G/4G USB Modem to the USB port of Vigor2762, it can support LTE/HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G/4G standard (HSUPA, etc). Vigor2762n with 3G/4G USB Modem allows you to receive 3G/4G 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 LAN ports on the router to access Internet. Also, they can access Internet via 802.11(a/b/g/n/ac) wireless standard, and enjoy the powerful firewall, bandwidth management, and VPN features of Vigor2762n series.



After connecting into the router, 3G/4G USB Modem will be regarded as the WAN3/WAN4 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/WAN4 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.

Web User Interface



II-1-1 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, WAN3 and WAN4 settings.

This webpage allows you to set general setup for WAN1, WAN2, and WAN3 respectively. In default, WAN2 is disabled. If you want to enable it, simply click the WAN2 link and select Yes in the field of Enable.

WAN >> General Setup

Load Balance Mode:

Index	Enable	Physical Mode/Type	Active Mode	Load Balance
WAN1	<input checked="" type="checkbox"/>	ADSL/-	Always On	V
WAN2	<input type="checkbox"/>	LAN Port 4	Failover	V
WAN3	<input checked="" type="checkbox"/>	USB/-	Failover	V

Note:

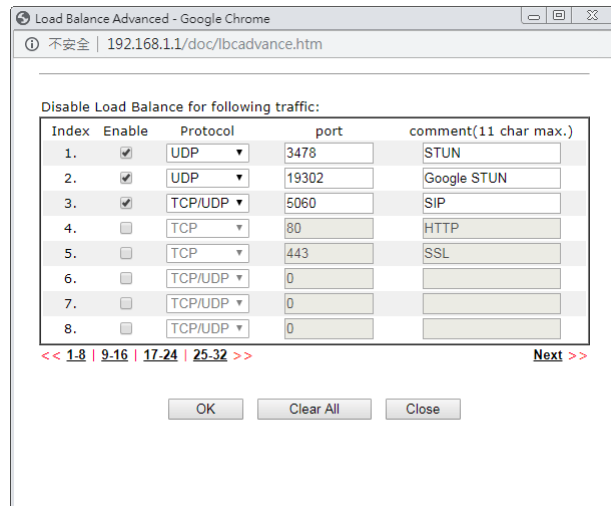
When WAN2 is enabled, LAN P4 port will be used as WAN2.

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> <ul style="list-style-type: none">● IP Based - The same source / destination IP pair will select the same WAN interface as policy. It is the default setting.● Sesseion Based- All of the WAN interfaces will be used (as out-going WAN) for passing through new sessions to get better transmission speed. Though good speed test result for throughput might be reached; however, some

web site may not open smoothly, especially the site need authentication, e.g., FTP.

- Advance - Load Balance for the traffic of STUN, google STUN, and SIP are disabled in default to prevent from conflict. The following dialog allows you to define protocol, port and name for the traffic not to be applied with load balance. That is, when an item is enabled (checked), it might not be affected by load balance.



If you have no strong demand about speed test result, keep default settings as IP based.

Index	Click the WAN interface link under Index to access into the WAN configuration page.
Enable	Check the box to enable this WAN interface. Uncheck the box to disable this WAN interface.
Physical Mode / Type	Display the physical mode and physical type of such WAN interface.
Active Mode	Display whether such WAN interface is Active device or backup device.
Load Balance	V means the function of load balance for this WAN interface is enabled.

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

II-1-1-1 WAN1 (ADSL/VDSL)

Vigor router will detect the physical line is connected by ADSL automatically. Therefore, this page allows you to configure settings for ADSL at one time. That is, it is not necessary for you to configure different profile settings for ADSL respectively.

WAN >> General Setup

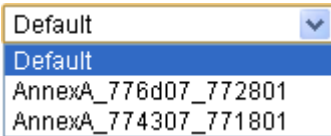
WAN 1

Enable:	Yes ▾	
Display Name:	<input type="text"/>	
Physical Mode:	ADSL	
DSL Mode:	Auto ▾	
DSL Modem Code:	Default ▾	
Line Speed(Kbps):		
DownLink	<input type="text" value="0"/>	
UpLink	<input type="text" value="0"/>	
Active Mode:	Always On ▾	
VLAN Tag insertion	Customer (TPID 0x8100)	Service (TPID 0x8100)
ADSL	Disable ▾ Tag value Priority <input type="text" value="0"/> <input type="text" value="0"/> (0~4095) (0~7)	
VDSL2	Disable ▾ Tag value Priority <input type="text" value="0"/> <input type="text" value="0"/> (0~4095) (0~7)	Disable ▾ Tag value Priority <input type="text" value="0"/> <input type="text" value="0"/> (0~4095) (0~7)

Note:
 Customer and service tag are used for different network environments. Customer tag is required for most ISPs while Service tag is required when ISP needs QinQ packets.

OK Cancel

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	Enter the description for such interface.
Physical Mode	Display the physical mode of such interface.
DSL Mode	Specify the physical mode (VDSL or ADSL) for such router manually.
DSL Modem Code	Choose the correct DSL modem code for ensuring the network connection.  If you have no idea about the selection, simply choose Default or contact the dealer for assistance.
VLAN Tag insertion (ADSL/VDSL)	Such feature is offered to the user with the environment supporting IEEE_802.1ad. In which, service is used for outer tag; customer is used for inner tag. 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 Enter the tag value and specify the priority for the packets sending by WAN1. Tag value - Enter the value as the VLAN ID number. The range is form 0 to 4095. Priority - Enter the packet priority number for such VLAN. The range is from 0 to 7.

Disable - Disable the function of VLAN with tag.

II-1-1-2 WAN2 (Ethernet)

Ethernet is the Physical Mode for WAN2.

WAN >> General Setup

WAN 2

Enable:	Yes ▾
Display Name:	<input type="text"/>
Physical Mode:	Ethernet
Physical Type:	Auto negotiation ▾
Line Speed(Kbps):	
DownLink	<input type="text" value="0"/>
UpLink	<input type="text" value="0"/>
Active Mode:	Failover ▾
	<input checked="" type="radio"/> WAN Failure
VLAN Tag insertion	Enable ▾
	Tag value Priority
	<input type="text" value="0"/> <input type="text" value="0"/>
	(0~4095) (0~7)

Note:

Customer and service tag are used for different network environments. Customer tag is required for most ISPs while Service tag is required when ISP needs QinQ packets.

OK Cancel

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	Enter 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 WAN1/WAN2/WAN3 or choose Auto negotiation for determined by the system.
Active Mode	<p>Always On - Choose it to make the WAN connection being activated always.</p> <p>Failover - Choose it to make the WAN connection as a backup connection.</p> <ul style="list-style-type: none"> ● WAN Failure - When the active WAN failed, such WAN will be activated as the main network connection.
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 Enter the tag value and specify the priority for the packets sending by WAN1.</p> <p>Tag value - Enter the value as the VLAN ID number. The range is form 0 to 4095.</p> <p>Priority - Enter the packet priority number for such VLAN. The range is from 0 to 7.</p> <p>Disable - Disable the function of VLAN with tag.</p>

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

II-1-1-3 WAN3 (USB)

To use 3G/4G network connection through 3G/4G USB Modem, please configure WAN3 or WAN4 interface.

WAN >> General Setup

WAN 3

Enable:	Yes ▾
Display Name:	<input type="text"/>
Physical Mode:	USB
Line Speed(Kbps):	
DownLink	<input type="text" value="0"/>
UpLink	<input type="text" value="0"/>
Active Mode:	Failover ▾
	<input checked="" type="radio"/> WAN Failure

OK Cancel

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	Enter the description for such WAN interface.
Physical Mode	Display the physical mode of such WAN interface.
Active Mode	Always On - Choose it to make the WAN connection being activated always. Failover - Choose it to make the WAN connection as a backup connection. ● WAN Failure - When the active WAN failed, such WAN will be activated as the main network connection.

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

II-1-2 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 / VDSL2	PPPoE / PPPoA	Details Page	IPv6
WAN2		Ethernet	None	Details Page	IPv6
WAN3		USB	MPoA / Static or Dynamic IP	Details Page	IPv6

DHCP Client Option

And,

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode		
WAN1		ADSL / VDSL2	PPPoE / PPPoA	Details Page	IPv6
WAN2		Ethernet	None	Details Page	IPv6
WAN3		USB	None	Details Page	IPv6

DHCP Client Option

And,

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode		
WAN1		ADSL / VDSL2	PPPoE / PPPoA	Details Page	IPv6
WAN2		Ethernet	None	Details Page	IPv6
WAN3		USB	None	Details Page	IPv6

DHCP Client Option

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 WAN1-2 (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 (based on IPv4) according to the access mode that you choose in WAN interface.

	<p>Note that Details Page will be changed slightly based on physical mode.</p>										
IPv6	<p>This button will open different web page (based on Physical Mode) to setup IPv6 Internet Access Mode for WAN interface. If IPv6 service is active on this WAN interface, the color of “IPv6” will become green.</p>										
DHCP Client Option	<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> <div data-bbox="703 622 1422 994" style="border: 1px solid black; padding: 5px;"> <p>Options List</p> <table border="1"> <thead> <tr> <th>Enable</th> <th>Interface</th> <th>Option</th> <th>Type</th> <th>Data</th> </tr> </thead> <tbody> <tr> <td colspan="5" style="height: 100px;"> </td> </tr> </tbody> </table> <p>Enable: <input checked="" type="checkbox"/></p> <p>Interface: <input type="checkbox"/> All <input checked="" type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3 <input type="checkbox"/> WAN4 <input type="checkbox"/> WAN5 <input type="checkbox"/> WAN6</p> <p>Option Number: <input type="text"/></p> <p>DataType: <input checked="" type="radio"/> ASCII Character (EX: Option:10, Data:/path) <input type="radio"/> Hexadecimal Digit (EX: Option:10, Data:2F70617468) <input type="radio"/> Address List (EX: Option:44, Data:172.16.2.10,172.16.2.20...)</p> <p>Data: <input type="text"/></p> <p style="text-align: center;"> <input type="button" value="Add"/> <input type="button" value="Update"/> <input type="button" value="Delete"/> <input type="button" value="Reset"/> </p> </div> <p>Note:</p> <ol style="list-style-type: none"> Option 12 is reserved. You cannot configure it here, but you can configure it in "Router Name" field of "WAN >> Internet Access >> Details Page". Option 55 is reserved and configured with value 1, 3, 6, 15 and 212, also 33 and 121 for some models. Configuring option 61 here will override the setting in "WAN >> Internet Access" page's DHCP Client Identifier field. <p style="text-align: center;"><input type="button" value="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>Interface - Specify the WAN interface(s) that will be overwritten by such function. WAN5 - WAN7 can be located under WAN>>Multi-PVC/VLAN.</p> <p>Option Number - Type a number for such function.</p> <p>DataType - Choose the type (ASCII or Hex) for the data to be stored.</p> <p>Data - Enter the content of the data to be processed by the function of DHCP option.</p>	Enable	Interface	Option	Type	Data					
Enable	Interface	Option	Type	Data							



Info

If you choose to configure option 61 here, the detailed settings in WAN>>Internet Access will be overwritten.

II-1-2-1 Details Page for PPPoE/PPPoA in WAN1 (Physical Mode: ADSL)

WAN >> Internet Access

WAN 1

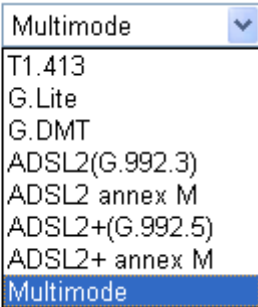
PPPoE / PPPoA	MPoA / Static or Dynamic IP	IPv6
<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
ADSL Modem Settings Multi-PVC channel: Channel 1 VPI: 0 VCI: 33 Encapsulating Type: LLC/SNAP Protocol: PPPoE Modulation: Multimode		
ISP Access Setup Username: Max: 63 characters Password: Max: 62 characters More Options +		
WAN Connection Detection Mode: PPP Detect		
MTU 1492 (Max:1500) Path MTU Discovery		
PPP/MP Setup PPP Authentication: PAP or CHAP IP Assignment (IPCP): <input type="radio"/> Static <input checked="" type="radio"/> Dynamic Fixed IP Address: <input type="text"/> <input type="button" value="WAN IP Alias"/>		
Dial-Out Schedule Index(1-15) in <u>Schedule</u> Setup: None => None => None => None		
PPPoE Pass-through <input type="checkbox"/> For Wired LAN ² <input type="checkbox"/> For Wireless LAN		
MAC Address <input checked="" type="radio"/> Default MAC Address <input type="radio"/> Use the following MAC Address 00 : 1D : AA : 08 : F5 : 21		

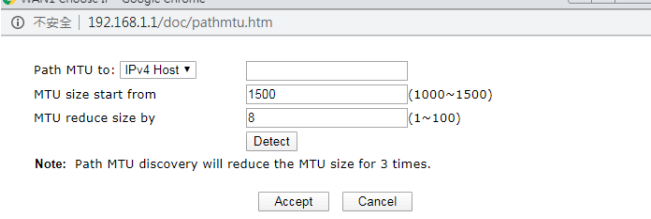
Note:

1. If PPPoE Pass-through for Wired LAN is checked while protocol is PPPoA, the router will behave like a modem which only serves the PPPoE client on the LAN.
2. VPN feature may be affected when the value of MTU is changed, please also check your value of VPN mss by using "VPN mss set" command.
We recommend to put the same decreased value on VPN mss. For example, reducing the MTU from 1500 -> 1400, then it will need to reduce 100 from mss value.

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.
ADSL Modem Settings	Set up the DSL parameters required by your ISP. These settings configured here are specified for ADSL only. Multi-PVC channel - The selections displayed here are determined by the page of WAN >> Multi-PVC/VLAN. Select M-PVCs Channel means no selection will be chosen. VPI - Type in the value provided by ISP. VCI - Type in the value provided by ISP. Encapsulating Type - Drop down the list to choose the type provided by ISP. Protocol - Drop down the list to choose the one (PPPoE or PPPoA) provided by ISP. 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. Modulation -Default setting is Multimode. Choose the one

	<p>that fits the requirement of your router.</p> <p>Modulation</p> 
<p>ISP Access Setup</p>	<p>Enter your allocated username, password and authentication parameters according to the information provided by your ISP.</p> <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>More Options - It shows optional settings for configuration.</p> <ul style="list-style-type: none"> ● Service Name - Enter the description of the specific network service. ● Separate Account for ADSL - In default, WAN1 supports VDSL2/ADSL and uses the same PPPoE account and password for connection. If required, you can configure another account and password for ADSL connection by checking this box. If it is checked, the system will ask you to type another group of account and password additionally.
<p>WAN Connection Detection</p>	<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 - Enter the interval for the system to execute the PING operation. ● Ping Retry - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
<p>MTU</p>	<p>It means Max Transmit Unit for packet.</p> <p>Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path.</p> <p>Click Detect to open the following dialog.</p>

	 <ul style="list-style-type: none"> ● Path MTU to - Enter the IP address as the specific transmit path. ● MTU size start from - Determine the starting point value of the packet. Default setting is 1500. ● MTU reduce size by - It determines the decreasing size of MTU value. For example, the number specified in this field is “8”. The maximum MTU size is “1500”. After clicking the “detect” button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically. ● Detect - Click it to detect a suitable MTU value ● Accept - After clicking it, the detected value will be displayed in the field of MTU.
<p>PPP/MP Setup</p>	<p>PPP Authentication - Select PAP only or PAP or CHAP for PPP.</p> <p>IP Assignment (IPCP)- Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function.</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>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>Dial-Out Schedule</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>
<p>PPPoE Pass-through</p>	<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 - It is available for n model. 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>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>

MAC 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>Use the following MAC Address - Type in the MAC address for the router manually.</p>
-------------	---

II-1-2-2 Details Page for MPoA/Static or Dynamic IP in WAN1 (Physical Mode: ADSL)

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 / Static or Dynamic IP as the accessing protocol of the Internet, select MPoA / Static or Dynamic IP from the WAN>>Internet Access >>WAN1 page. The following web page will appear.

WAN >> Internet Access

WAN 1

PPPoE / PPPoA
 MPoA / Static or Dynamic IP
 IPv6

Enable Disable

ADSL Modem Settings

Multi-PVC channel:

Encapsulation:

VPI:

VCI:

Modulation:

IP Network Settings

Obtain an IP address automatically
More Options

Specify an IP address

IP Address:

Subnet Mask:

Gateway IP Address:

DNS Server IP Address

Primary Server:

Secondary Server:

WAN Connection Detection

Mode:

MTU

(Max: 1500)

RIP Routing

Enable RIP

Bridge Mode

Enable Bridge Mode

Enable Full Bridge Mode

Bridge Subnet:

MAC Address

Default MAC Address

Use the following MAC Address

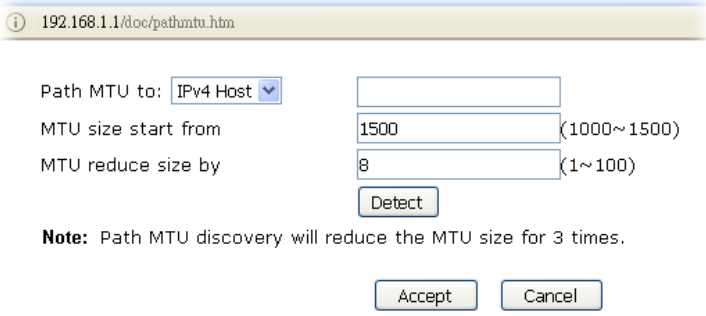
Note:

1. VPN feature may be affected when the value of MTU is changed, please also check your value of VPN mss by using "VPN mss set" command.
We recommend to put the same decreased value on VPN mss. For example, reducing the MTU from 1500 -> 1400, then it will need to reduce 100 from mss value.
2. Full Bridge Mode supports forwarding packets with VLAN tags.
3. Full Bridge Mode doesn't support wireless LAN.

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.
ADSL Modem Settings	<p>Set up the DSL parameters required by your ISP. These settings configured here are specified for ADSL only.</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>Encapsulation - Drop down the list to choose the type provided by ISP.</p> <p>VPI - Type in the value provided by ISP.</p> <p>VCI - Type in the value provided by ISP.</p> <p>Modulation -Default setting is Multimode. Choose the one that fits the requirement of your router.</p>
IP Network Settings	<p>This group allows you to obtain an IP address automatically and allows you type in IP address manually.</p> <p>Obtain an IP address automatically - Click this button to obtain the IP address automatically.</p> <p>More Options - It shows optional settings for configuration.</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. ● DHCP Client Identifier for some ISP - 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. ● Gateway IP Address - Type in gateway IP address. <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. Enter the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.</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.
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, Ping Detect, Always On or Strict ARP 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

	<p>gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off.</p> <ul style="list-style-type: none"> ● TTL (Time to Live) - Set TTL value of PING operation. ● Ping Interval - Enter the interval for the system to execute the PING operation. ● Ping Retry - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
MTU	<p>It means Max Transmit Unit for packet.</p> <p>Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path.</p> <p>Click Detect to open the following dialog.</p>  <p>Note: Path MTU discovery will reduce the MTU size for 3 times.</p> <ul style="list-style-type: none"> ● Path MTU to - Enter the IP address as the specific transmit path. ● MTU size start from - Determine the starting point value of the packet. Default setting is 1500. ● MTU reduce size by - It determines the decreasing size of MTU value. For example, the number specified in this field is “8”. The maximum MTU size is “1500”. After clicking the “detect” button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically. ● Detect - Click it to detect a suitable MTU value ● Accept - After clicking it, the detected value will be displayed in the field of MTU.
RIP Routing	<p>Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.</p>
Bridge Mode	<p>Enable Bridge Mode - If the function is enabled, the router will work as a bridge modem.</p> <p>Enable Full Bridge Mode - If the function is enabled, the router will work as a bridge modem which is able to forward incoming packets with VLAN tags.</p> <ul style="list-style-type: none"> ● Bridge Subnet - Make a bridge between the selected LAN subnet and such WAN interface.
MAC 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>Use the following MAC Address - Type in the MAC address for the router manually.</p>

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

II-1-2-3 Details Page for PPPoE in Ethernet WAN

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

WAN >> Internet Access

WAN 2

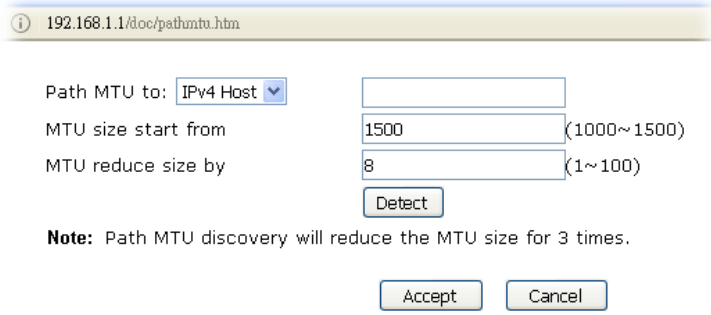
PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
ISP Access Setup Username <input type="text" value="Max: 63 characters"/> Password <input type="text" value="Max: 62 characters"/> More Options <input type="button" value="+"/>		PPP/MP Setup PPP Authentication <input type="text" value="PAP or CHAP"/> Idle Timeout <input type="text" value="180"/> second(s) IP Assignment (IPCP) <input type="radio"/> Static <input checked="" type="radio"/> Dynamic Fixed IP Address <input type="text"/> <input type="button" value="WAN IP Alias"/>	
WAN Connection Detection Mode <input type="text" value="PPP Detect"/>		Dial-Out Schedule Index(1-15) in <u>Schedule</u> Setup: <input type="text" value="None"/> => <input type="text" value="None"/> => <input type="text" value="None"/> => <input type="text" value="None"/>	
MTU <input type="text" value="1492"/> (Max:1500) <input type="button" value="Path MTU Discovery"/>		TTL <input checked="" type="checkbox"/> Change the TTL value <input checked="" type="radio"/> Default MAC Address <input type="radio"/> Use the following MAC Address <input type="text" value="00 :1D :AA :08 :F5 :22"/>	

Note:

VPN feature may be affected when the value of MTU is changed, please also check your value of VPN mss by using "VPN mss set" command.
 We recommend to put the same decreased value on VPN mss. For example, reducing the MTU from 1500 -> 1400, then it will need to reduce 100 from mss value.

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. Username - Type in the username provided by ISP in this field. The maximum length of the user name you can set is 63 characters. Password - Type in the password provided by ISP in this field. The maximum length of the password you can set is 62 characters. More Options - It shows optional settings for configuration. <ul style="list-style-type: none"> ● Service Name - Enter the description of the specific network service.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.

	<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 - Enter the interval for the system to execute the PING operation. ● Ping Retry - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
MTU	<p>It means Max Transmit Unit for packet.</p> <p>Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path.</p> <p>Click Detect to open the following dialog.</p>  <ul style="list-style-type: none"> ● Path MTU to - Enter the IP address as the specific transmit path. ● MTU size start from - Determine the starting point value of the packet. Default setting is 1500. ● MTU reduce size by - It determines the decreasing size of MTU value. For example, the number specified in this field is “8”. The maximum MTU size is “1500”. After clicking the “detect” button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically. ● Detect - Click it to detect a suitable MTU value ● Accept - After clicking it, the detected value will be displayed in the field of MTU.
PPP/MP 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> <p>IP Assignment (IPCP) - Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your</p>

	<p>ISP before you want to use this function.</p> <p>Fixed IP Address - Click Yes to use this function and type in a fixed IP address in the box of Fixed IP Address.</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. Enter the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.</p>
Dial-Out Schedule	<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>
TTL	<p>Change the TTL value - Enable or disable the TTL (Time to Live) for a packet transmitted through Vigor router.</p> <ul style="list-style-type: none"> ● Enable - TTL value will be reduced (-1) when it passes through Vigor router. It will cause the client, accessing Internet through Vigor router, to be blocked by certain ISP when TTL value becomes "0". ● Disable - TTL value will not be reduced. Then, when a packet passes through Vigor router, it will not be cancelled. That is, the client who sends out the packet will not be blocked by ISP. <p>Default MAC Address - You can use Default MAC Address or specify another MAC address by typing on the boxes of MAC Address for the router.</p> <p>Specify a MAC Address - Enter the MAC address for the router manually.</p>

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

II-1-2-4 Details Page for Static or Dynamic IP in Ethernet WAN

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 >> Internet Access

WAN 2

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
<input type="radio"/> Enable <input checked="" type="radio"/> Disable		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)	
IP Network Settings <input type="radio"/> Obtain an IP address automatically More Options <input type="button" value="+"/> <input checked="" type="radio"/> Specify an IP address IP Address <input type="text"/> Subnet Mask <input type="text"/> Gateway IP Address <input type="text"/> <input type="button" value="WAN IP Alias"/>		TTL <input checked="" type="checkbox"/> Change the TTL value	
DNS Server IP Address Primary Server <input type="text" value="8.8.8.8"/> Secondary Server <input type="text" value="8.8.4.4"/>		RIP Routing <input type="checkbox"/> Enable RIP	
WAN Connection Detection Mode <input type="text" value="ARP Detect"/>		MAC Address <input checked="" type="radio"/> Default MAC Address <input type="radio"/> Use the following MAC Address <input type="text" value="00:1D:AA:08:F5:22"/>	
MTU <input type="text" value="1500"/> <input type="button" value="Path MTU Discovery"/>			

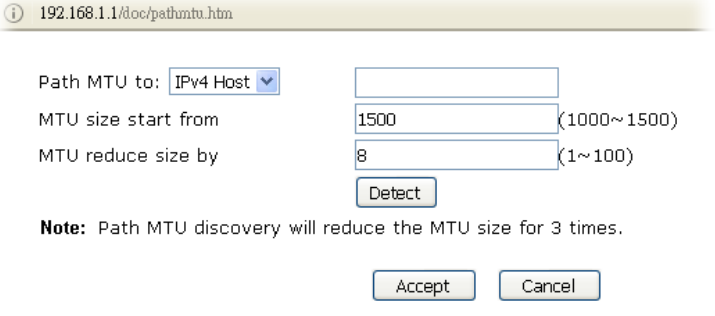
Note:

VPN feature may be affected when the value of MTU is changed, please also check your value of VPN mss by using "VPN mss set" command.
 We recommend to put the same decreased value on VPN mss. For example, reducing the MTU from 1500 -> 1400, then it will need to reduce 100 from mss value.

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.
IP Network Settings	This group allows you to obtain an IP address automatically and allows you type in IP address manually. Obtain an IP address automatically - Click this button to obtain the IP address automatically if you want to use Dynamic IP mode. More Options - It shows optional settings for configuration. <ul style="list-style-type: none"> ● Router Name: Type in the router name provided by ISP.

	<ul style="list-style-type: none"> ● Domain Name: Type in the domain name that you have assigned. ● DHCP Client Identifier for some ISP: 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: Enter the IP address. ● Subnet Mask: Enter the subnet mask. ● Gateway IP Address: Enter the gateway IP address. <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>
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.
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 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 - Enter the interval for the system to execute the PING operation. ● Ping Retry - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
MTU	<p>It means Max Transmit Unit for packet.</p> <p>Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path.</p> <p>Click Detect to open the following dialog.</p>

	 <ul style="list-style-type: none"> ● Path MTU to - Enter the IP address as the specific transmit path. ● MTU size start from - Determine the starting point value of the packet. Default setting is 1500. ● MTU reduce size by - It determines the decreasing size of MTU value. For example, the number specified in this field is “8”. The maximum MTU size is “1500”. After clicking the “detect” button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically. ● Detect - Click it to detect a suitable MTU value ● Accept - After clicking it, the detected value will be displayed in the field of MTU.
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>
TTL	<p>Change the TTL value - Enable or disable the TTL (Time to Live) for a packet transmitted through Vigor router.</p> <ul style="list-style-type: none"> ● Enable - TTL value will be reduced (-1) when it passes through Vigor router. It will cause the client, accessing Internet through Vigor router, to be blocked by certain ISP when TTL value becomes “0”. ● Disable - TTL value will not be reduced. Then, when a packet passes through Vigor router, it will not be cancelled. That is, the client who sends out the packet will not be blocked by ISP.
RIP Routing	<p>Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.</p>
MAC 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>

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

II-1-2-5 Details Page for PPTP/L2TP in Ethernet WAN

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 Server Address <input style="width: 150px;" type="text" value="Max: 63 characters"/> Specify Gateway IP Address <input style="width: 150px;" type="text" value="Max: 63 characters"/>		PPP Setup PPP Authentication <input style="width: 80px;" type="text" value="PAP or CHAP"/> Idle Timeout <input style="width: 40px;" type="text" value="180"/> second(s) IP Address Assignment Method (IPCP) <input style="width: 80px;" type="text" value="WAN IP Alias"/> Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address <input style="width: 100px;" type="text"/>	
ISP Access Setup Username <input style="width: 150px;" type="text" value="Max: 63 characters"/> Password <input style="width: 150px;" type="text"/> Schedule Profile: <input type="text" value="None"/> => <input type="text" value="None"/> => <input type="text" value="None"/> => <input type="text" value="None"/>		WAN IP Network Settings <input type="radio"/> Obtain an IP address automatically <input checked="" type="radio"/> Specify an IP address IP Address <input style="width: 100px;" type="text"/> Subnet Mask <input style="width: 100px;" type="text"/>	
MTU <input style="width: 40px;" type="text" value="1460"/> (Max:1460) Path MTU Discovery <input type="button" value="Detect"/>			

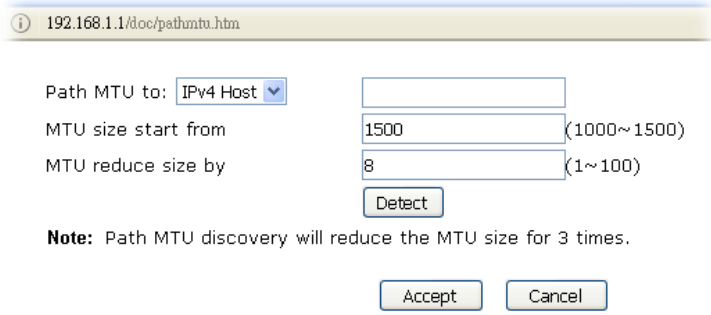
Note:

VPN feature may be affected when the value of MTU is changed, please also check your value of VPN mss by using "VPN mss set" command.

We recommend to put the same decreased value on VPN mss. For example, reducing the MTU from 1500 -> 1400, then it will need to reduce 100 from mss value.

Available settings are explained as follows:

Item	Description
PPTP/L2TP	Enable PPTP- Click this radio button to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface. Enable L2TP - Click this radio button to enable a L2TP client to establish a tunnel to a DSL modem on the WAN interface. Disable - Click this radio button to close the connection through PPTP or L2TP. Server Address - Specify the IP address of the PPTP/L2TP server if you enable PPTP/L2TP client mode. Specify Gateway IP Address - Specify the gateway IP address for DHCP server.
ISP Access Setup	Username -Type in the username provided by ISP in this field. The maximum length of the user name you can set is 63 characters. Password -Type in the password provided by ISP in this field. The maximum length of the password you can set is 62 characters. Schedule Profile- You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page.
MTU	It means Max Transmit Unit for packet. Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit

	<p>path. Click Detect to open the following dialog.</p>  <ul style="list-style-type: none"> ● Path MTU to - Enter the IP address as the specific transmit path. ● MTU size start from - Determine the starting point value of the packet. Default setting is 1500. ● MTU reduce size by - It determines the decreasing size of MTU value. For example, the number specified in this field is “8”. The maximum MTU size is “1500”. After clicking the “detect” button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically. ● Detect - Click it to detect a suitable MTU value ● Accept - After clicking it, the detected value will be displayed in the field of MTU.
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> <ul style="list-style-type: none"> ● IP Address - Enter the IP address. ● Subnet Mask - Enter the subnet mask.

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

II-1-2-6 Details Page for 3G/4G USB Modem (PPP mode) in USB WAN

To use 3G/4G USB Modem (PPP mode) as the accessing protocol of the internet, please choose Internet Access from WAN menu. Then, select 3G/4G USB Modem (PPP mode) for WAN5. 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) Enable Disable

SIM PIN code

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

APN Name

Modem Initial String2

Modem Dial String
(Default:ATDT*99#, CDMA:ATDT#777, TD-SCDMA:ATDT*98*1#)

Service Name (Optional)

PPP Username (Optional)

PPP Password (Optional)

PPP Authentication

Schedule Profile:

=> => =>

WAN Connection Detection

Mode

Available settings are explained as follows:

Item	Description
Modem Support List	<p>It lists all of the modems supported by such router.</p> <p>WAN >> Internet Access ?</p> <hr/> <p>WAN 3</p> <p>3G/4G USB Modem(PPP mode) 3G/4G USB Modem(DHCP mode) IPv6 Modem Support List</p> <div style="border: 1px solid black; padding: 5px;"> <p>3G/4G USB Modem(PPP mode) <input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> <p>SIM PIN code <input type="text"/></p> <p>Modem Initial String <input type="text" value="AT&FE0V1X1&D2&C1S0=0"/> (Default:AT&FE0V1X1&D2&C1S0=0)</p> <p>APN Name <input type="text"/> <input type="button" value="Apply"/></p> <p>Modem Initial String2 <input type="text" value="AT"/></p> <p>Modem Dial String <input type="text" value="ATDT*99#"/> (Default:ATDT*99#, CDMA:ATDT#777, TD-SCDMA:ATDT*98*1#)</p> <p>Service Name <input type="text"/> (Optional)</p> <p>PPP Username <input type="text"/> (Optional)</p> <p>PPP Password <input type="text"/> (Optional)</p> <p>PPP Authentication <input type="text" value="PAP or CHAP"/></p> <p>Schedule Profile:</p> <p><input type="text" value="None"/> => <input type="text" value="None"/> => <input type="text" value="None"/> => <input type="text" value="None"/></p> <hr/> <p>WAN Connection Detection</p> <p>Mode <input type="text" value="PPP Detect"/></p> </div> <p style="text-align: center;"> <input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Default"/> </p>
3G /4G USB Modem (PPP mode)	<p>Click Enable for activating this function. If you click Disable, this function will be closed and all the settings that you</p>

	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 15 characters.
Modem Initial String	Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP. The maximum length of the string you can set is 47 characters.
APN Name	APN means Access Point Name which is provided and required by some ISPs. Enter the name and click Apply. The maximum length of the name you can set is 43 characters.
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. The maximum length of the string you can set is 47 characters.
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. The maximum length of the string you can set is 31 characters.
Service Name	Enter the description of the specific network service.
PPP Username	Enter the PPP username (optional). The maximum length of the name you can set is 63 characters.
PPP Password	Enter the PPP password (optional). The maximum length of the password you can set is 62 characters.
PPP Authentication	Select PAP only or PAP or CHAP for PPP.
Schedule Profile	You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode - Choose PPP 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. <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. ● TTL (Time to Live) - Set TTL value of PING operation. ● Ping Interval - Enter the interval for the system to execute the PING operation. ● Ping Retry - Enter 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 activate them.

II-1-2-7 Details Page for 3G/4G USB Modem (DHCP mode) in USB WAN

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 >> Internet Access ?

WAN 3

3G/4G USB Modem(PPP mode) 3G/4G USB Modem(DHCP mode) IPv6

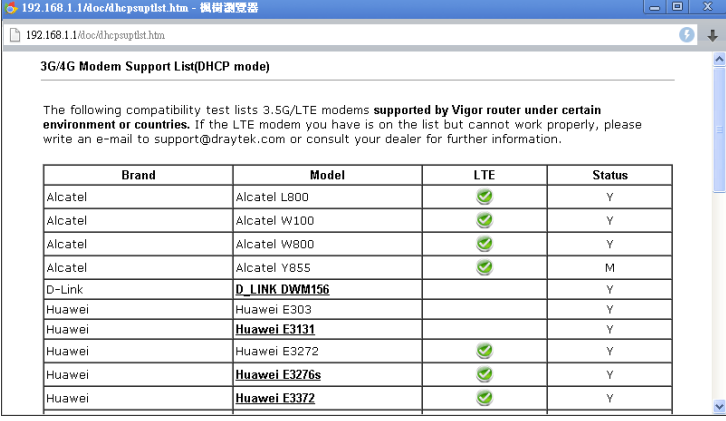
[Modem Support List](#)

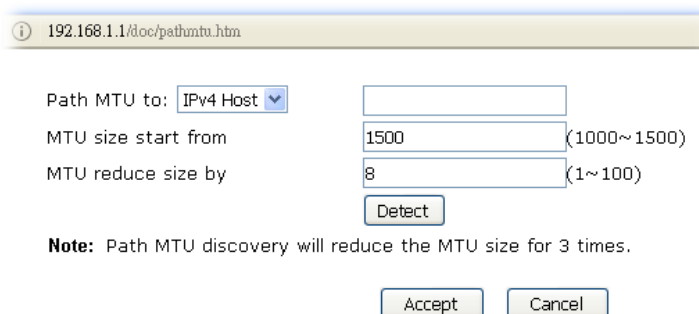
<input type="radio"/> Enable <input checked="" type="radio"/> Disable SIM PIN code <input type="text"/> Network Mode <input type="text" value="4G/3G/2G"/> (Default:4G/3G/2G) APN Name <input type="text"/> LTE hardware version --- WAN Connection Detection Mode <input type="text" value="ARP Detect"/> Schedule Profile: <input type="text" value="None"/> => <input type="text" value="None"/> => <input type="text" value="None"/> => <input type="text" value="None"/> MTU <input type="text" value="1500"/> (Default:1500) Path MTU Discovery <input type="button" value="Choose IP"/>	Authentication <input type="text" value="PAP or CHAP"/> Username <input type="text"/> (Optional) Password <input type="text"/> (Optional)
---	---

Note:

- Please note that in some case USB port connection will be terminated temporarily to activate the new configuration.
- VPN feature may be affected when the value of MTU is changed, please also check your value of VPN mss by using "VPN mss set" command.
We recommend to put the same decreased value on VPN mss. For example, reducing the MTU from 1500 - > 1400, then it will need to reduce 100 from mss value.

Available settings are explained as follows:

Item	Description																																												
Modem Support List	It lists all of the modems supported by such router.  <table border="1" data-bbox="742 1590 1372 1836"> <thead> <tr> <th>Brand</th> <th>Model</th> <th>LTE</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>Alcatel</td> <td>Alcatel L800</td> <td>✓</td> <td>Y</td> </tr> <tr> <td>Alcatel</td> <td>Alcatel W100</td> <td>✓</td> <td>Y</td> </tr> <tr> <td>Alcatel</td> <td>Alcatel W800</td> <td>✓</td> <td>Y</td> </tr> <tr> <td>Alcatel</td> <td>Alcatel Y855</td> <td>✓</td> <td>M</td> </tr> <tr> <td>D-Link</td> <td>D_LINK DWM156</td> <td></td> <td>Y</td> </tr> <tr> <td>Huawei</td> <td>Huawei E303</td> <td></td> <td>Y</td> </tr> <tr> <td>Huawei</td> <td>Huawei E3131</td> <td></td> <td>Y</td> </tr> <tr> <td>Huawei</td> <td>Huawei E3272</td> <td>✓</td> <td>Y</td> </tr> <tr> <td>Huawei</td> <td>Huawei E3276s</td> <td>✓</td> <td>Y</td> </tr> <tr> <td>Huawei</td> <td>Huawei E3372</td> <td>✓</td> <td>Y</td> </tr> </tbody> </table>	Brand	Model	LTE	Status	Alcatel	Alcatel L800	✓	Y	Alcatel	Alcatel W100	✓	Y	Alcatel	Alcatel W800	✓	Y	Alcatel	Alcatel Y855	✓	M	D-Link	D_LINK DWM156		Y	Huawei	Huawei E303		Y	Huawei	Huawei E3131		Y	Huawei	Huawei E3272	✓	Y	Huawei	Huawei E3276s	✓	Y	Huawei	Huawei E3372	✓	Y
Brand	Model	LTE	Status																																										
Alcatel	Alcatel L800	✓	Y																																										
Alcatel	Alcatel W100	✓	Y																																										
Alcatel	Alcatel W800	✓	Y																																										
Alcatel	Alcatel Y855	✓	M																																										
D-Link	D_LINK DWM156		Y																																										
Huawei	Huawei E303		Y																																										
Huawei	Huawei E3131		Y																																										
Huawei	Huawei E3272	✓	Y																																										
Huawei	Huawei E3276s	✓	Y																																										
Huawei	Huawei E3372	✓	Y																																										
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. Enter the name and click Apply. The maximum length of the name you can set is 47 characters.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode - Choose ARP Detect, Ping Detect or Strict ARP 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. <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 - Enter the interval for the system to execute the PING operation. ● Ping Retry - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
Schedule Profile	You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page
MTU	It means Max Transmit Unit for packet. Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path. Click Detect to open the following dialog.  <ul style="list-style-type: none"> ● Path MTU to - Enter the IP address as the specific transmit path. ● MTU size start from - Determine the starting point value of the packet. Default setting is 1500. ● MTU reduce size by - It determines the decreasing size

	<p>of MTU value. For example, the number specified in this field is “8”. The maximum MTU size is “1500”. After clicking the “detect” button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically.</p> <ul style="list-style-type: none"> ● Detect - Click it to detect a suitable MTU value ● Accept - After clicking it, the detected value will be displayed in the field of MTU.
<p>Authentication</p>	<p>Select PAP only or PAP or CHAP for PPP authentication. Username - Enter the username for authentication (optional). Password - Enter the password for authentication (optional).</p>

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

II-1-2-8 Details Page for IPv6 – Offline in WAN1/WAN2/WAN3

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

II-1-2-9 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 / Static or Dynamic IP	IPv6
Internet Access Mode Connection Type: <input type="text" value="PPP"/>		
WAN Connection Detection Mode: <input type="text" value="Ping Detect"/> Ping IP/Hostname: <input type="text"/> TTL(1-255,0:Auto): <input type="text" value="0"/>		
RIPng Protocol <input type="checkbox"/> Enable		

Note:

IPv4 WAN setting should be PPPoE / PPPoA client.

OK

Cancel

Available settings are explained as follows:

Item	Description
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.
RIPng Protocol	RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.

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

Online Status

Physical Connection		System Uptime: 0:2:32	
IPv4	IPv6		
LAN Status			
IP Address			
2001:B010:7300:201:21D:AFF:FEA6:2568/64 (Global)			
FE80::21D:AFF:FEA6:2568/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
7	4	690	328
WAN2 IPv6 Status >> Drop PPP			
Enable	Mode	Up Time	
Yes	PPP	0:02:08	
IP		Gateway IP	
2001:B010:7300:201:21D:AFF:FEA6:256A/128 (Global)		FE80::90:1A00:242:AD52	
FE80::1D:AFF:FEA6:256A/128 (Link)			
DNS IP			
2001:8000:168::1			
2001:8000:168::2			
TX Packets	RX Packets	TX Bytes	RX Bytes
7	9	544	1126



Info

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.

II-1-2-10 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 >> Internet Access ?

WAN 1

PPPoE / PPPoA	MPoA / Static or Dynamic IP	IPv6
<p>Internet Access Mode</p> <p>Connection Type: TSPC</p> <p>TSPC Configuration</p> <p>Username: <input style="width: 100%;" type="text" value="Max: 63 characters"/></p> <p>Password: <input style="width: 100%;" type="text" value="Max: 63 characters"/></p> <p>Tunnel Broker: <input style="width: 100%;" type="text"/></p> <p>WAN Connection Detection</p> <p>Mode: Ping Detect</p> <p>Ping IP/Hostname: <input style="width: 100%;" type="text"/></p> <p>TTL(1-255,0:Auto): <input style="width: 50px;" type="text" value="0"/></p>		
<p>OK Cancel</p>		

Available settings are explained as follows:

Item	Description
Username	Enter 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 . The maximum length of the name you can set is 63 characters.
Password	Enter the password assigned with the user name. The maximum length of the name you can set is 19 characters.
Tunnel Broker	Enter the address for the tunnel broker IP, FQDN or an optional port number.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. 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. <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.

II-1-2-11 Details Page for IPv6 – AICCU in WAN1/WAN2/WAN3

WAN >> Internet Access



WAN 1

PPPoE / PPPoA	MPoA / Static or Dynamic IP	IPv6
Internet Access Mode		
Connection Type		AICCU ▼
AICCU Configuration		
<input type="checkbox"/> Always On		
Username		Max: 63 characters
Password		Max: 63 characters
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	Enter 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. The maximum length of the name you can set is 19 characters.
Password	Enter the password assigned with the user name. The maximum length of the password you can set is 19 characters.
Tunnel Broker	It means a server of AICCU. The server can provide IPv6 tunnels to sites or end users over IPv4. Enter the address for the tunnel broker IP, FQDN or an optional port number.
Tunnel ID	One user account may have several tunnels. And, each tunnel shall have one specified tunnel ID (e.g., T115394). Enter the ID offered by Tunnel Broker.

Subnet Prefix	Enter the subnet prefix address obtained from service provider. The maximum length of the prefix you can set is 128 characters.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. Mode - Choose Always On or Ping Detect for the system to execute for WAN detection. <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.

II-1-2-12 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): 44178403
 DUID (DHCP Unique ID): 00030001001daa08f521
 Authentication Protocol: None

WAN Connection Detection
 Mode: Ping Detect
 Ping IP/Hostname:
 TTL(1-255,0:Auto): 0

RIPng Protocol
 Enable

Bridge Mode
 Enable Bridge Mode
 Enable Firewall
 Bridge Subnet: LAN 1

OK Cancel

Available settings are explained as follows:

Item	Description
IAID	Type a number as IAID.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through NS Detect or Ping Detect. 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. <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.
RIPng Protocol	RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.
Bridge Mode	Enable Bridge Mode - If the function is enabled, the router will work as a bridge modem. Enable Firewall - It is available when Bridge Mode is enabled. When both Bridge Mode and Firewall check boxes are enabled, the settings configured (user profiles) under User Management will be ignored. And all of the filter rules defined and enabled in Firewall menu will be activated.

Bridge Subnet - Make a bridge between the selected LAN subnet and such WAN interface.

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

II-1-2-13 Details Page for IPv6 – Static IPv6 in 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="text"/> / <input type="text"/> Add Update 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> <tr> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>			Index	IPv6 Address/Prefix Length	Scope			
Index	IPv6 Address/Prefix Length	Scope						
Static IPv6 Gateway configuration IPv6 Gateway Address: <input type="text"/>								
WAN Connection Detection Mode: NS Detect								
RIPng Protocol <input type="checkbox"/> Enable								
Bridge Mode <input checked="" type="checkbox"/> Enable Bridge Mode <input type="checkbox"/> Enable Firewall Bridge Subnet: LAN 1								

OK Cancel

Available settings are explained as follows:

Item	Description
Static IPv6 Address Configuration	IPv6 Address - Enter the IPv6 Static IP Address. Prefix Length - Enter the fixed value for prefix length. Add - Click it to add a new entry. Update - Click it to modify an existed 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.
RIPng Protocol	<p>RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.</p>
Bridge Mode	<p>Enable Bridge Mode - If the function is enabled, the router will work as a bridge modem.</p> <p>Enable Firewall - It is available when Bridge Mode is enabled. When both Bridge Mode and Firewall check boxes are enabled, the settings configured (user profiles) under User Management will be ignored. And all of the filter rules defined and enabled in Firewall menu will be activated.</p> <p>Bridge Subnet - Make a bridge between the selected LAN subnet and such WAN interface.</p>

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

II-1-2-14 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 anycast 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: / (default:64)

LAN Routed Prefix: / (default:64)

Tunnel TTL: (default:255)

WAN Connection Detection

Mode: Ping Detect ▼

Ping IP/Hostname:

TTL(1-255,0:Auto):

OK Cancel

Available settings are explained as follows:

Item	Description
Remote Endpoint IPv4 Address	Enter the static IPv4 address for the remote server.
6in4 IPv6 Address	Enter the static IPv6 address for IPv4 tunnel with the value for prefix length.
LAN Routed Prefix	Enter the static IPv6 address for LAN routing with the value for prefix length.
Tunnel TTL	Enter the number for the data lifetime in tunnel.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. 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. <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 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

II-1-2-15 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: Auto 6rd Static 6rd

Static 6rd Settings
 IPv4 Border Relay:
 IPv4 Mask Length:
 6rd Prefix:
 6rd Prefix Length:

WAN Connection Detection
 Mode: Ping Detect
 Ping IP/Hostname:
 TTL(1-255,0:Auto):

OK Cancel

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	Enter 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	Enter the 6rd IPv6 address.
6rd Prefix Length	Enter the IPv6 prefix length for the 6rd IPv6 prefix in number of bits.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. 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. <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

II-1-3 Multi-PVC/VLAN

Multi-PVC/VLAN lets you configure multiple permanent virtual circuits (PVCs) and ATM QoS for channels using ADSL.

Channel 1 to 4 have the following fixed assignments and cannot be altered.

- Channel 1: ADSL on WAN1.
- Channel 2: Ethernet on WAN2.
- Channel 3: USB1 (WAN3).

Channels 4 through 10 can be bridged to one or more of the 3 LAN ports P2 through P4. In addition, Channels 4 through 6 can be configured as virtual WANs (WAN4 through WAN6).

General

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	
4. WAN4	No	ADSL	1/44	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
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.	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
9.	No	ADSL	1/49	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
10.	No	ADSL	1/50	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4

Note:

Channel 3 are reserved for USB WAN.

Available settings are explained as follows:

Item	Description
Channel	Display the number of each channel. Channels 4 - 10 are configurable.
Enable	Display whether the settings in this channel are enabled (Yes) or not (No).

To configure a PVC channel, click its channel number.

WAN links for Channel 4, 5 and 6 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 4, 5 or 6 to configure your router.

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

Enable Channel 5:

WAN Type :

General Settings	ATM QoS
VPI <input type="text" value="1"/>	QoS Type <input type="text" value="UBR"/>
VCI <input type="text" value="45"/>	PCR <input type="text" value="0"/>
Protocol <input type="text" value="PPPoA"/>	SCR <input type="text" value="0"/>
Encapsulation <input type="text" value="VC MUX"/>	MBS <input type="text" value="0"/>
<input type="checkbox"/> Add VLAN Header	
VLAN Tag <input type="text" value="0"/>	
Priority <input type="text" value="0"/>	

Open Port-based Bridge Connection for this Channel

Physical Members

P1 P2 P3 P4

Open WAN Interface for this Channel

WAN Application: Management VoIP IPTV

WAN Connection Detection

Mode

PPPoE/PPPoA Client	MPoA (RFC1483/2684)	
ISP Access Setup		
ISP Name <input type="text"/>	<input type="radio"/> Obtain an IP address automatically	
Username <input type="text"/>	Router Name <input type="text" value="Vigor"/> *	
Password <input type="text"/>	Domain Name <input type="text"/> *	
PPP Authentication <input type="text" value="PAP or CHAP"/>	*: Required for some ISPs	
<input checked="" type="checkbox"/> Always On	<input checked="" type="radio"/> Specify an IP address	
Idle Timeout <input type="text" value="-1"/> second(s)	IP Address <input type="text"/>	
IP Address From ISP	Subnet Mask <input type="text"/>	
Fixed IP <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP)	Gateway IP Address <input type="text"/>	
Fixed 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"/>	

Available settings are explained as follows:

Item	Description
Multi-VLAN Channel 4/5/6	Enable - Click it to enable the configuration of this channel. Disable -Click it to disable the configuration of this channel.
WAN Type	The connections and interfaces created in every channel may select a specific WAN type to be built upon. In the Multi-PVC application, only the Ethernet WAN type is available. The user will be able to select the physical WAN interface the channel shall use here.
General Settings	VPI - Type in the value provided by your ISP. VCI - Type in the value provided by your ISP. Protocol - Select a proper protocol for this channel.

	<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 - Enter 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>Such function is available only when ADSL is selected as WAN Type.</p> <p>QoS Type - Select a proper QoS type for the channel. Enter 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> <ul style="list-style-type: none"> ● 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. ● IPTV - The IPTV configuration will allow the WAN interface to send IGMP packets to IPTV servers. ● VoIP- The VoIP configuration will allow the WAN interface created here to send SIP registration packets and other VoIP management packets.
WAN Connection Detection	<p>Such function is available only when ADSL is selected as WAN Type.</p> <p>It 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 - Enter the interval for the system to execute the PING operation. ● Ping Retry - Enter the number of times that the system is

	<p>allowed to execute the PING operation before WAN disconnection is judged.</p>
<p>PPPoE/PPPoA Client ISP Access Setup</p>	<p>Enter your allocated username, password and authentication parameters according to the information provided by your ISP.</p> <p>ISP Name - PPP Service Name. Enter if your ISP requires this setting; otherwise leave blank.</p> <p>Username - Name provided by the ISP for PPPoE/PPPoA authentication. Maximum length is 62 characters.</p> <p>Password - Password provided by the ISP for PPPoE/PPPoA authentication. Maximum length is 62 characters.</p> <p>PPP Authentication - The protocol used for PPP authentication.</p> <ul style="list-style-type: none"> ● PAP only- Only PAP (Password Authentication Protocol) is used. ● PAP or CHAP- Both PAP and CHAP (Challenge-Handshake Authentication Protocol) can be used for PPP authentication. Router negotiates with the PPTP or L2TP server to determine which protocol to use. <p>Always On - If selected, the router will maintain the PPPoE/PPPoA connection.</p> <p>Idle Timeout - Maximum length of time, in seconds, of idling allowed (no traffic) before the connection is dropped.</p> <p>ISP Address from ISP - Specifies how the WAN IP address of the channel configured.</p> <ul style="list-style-type: none"> ● Fixed IP <ul style="list-style-type: none"> Yes - IP address entered in the Fixed IP Address field will be used as the IP address of the virtual WAN. No - Virtual WAN IP address will be assigned by the ISP's PPPoE/PPPoA server.
<p>MPoA</p>	<p>Obtain an IP address automatically - Select this option if the router is to receive IP configuration information from a DHCP server.</p> <ul style="list-style-type: none"> ● Router Name - Sets the value of DHCP Option 12, which is used by some ISPs. ● Domain Name - Sets the value of DHCP Option 15, which is used by some ISPs. <p>Specify an IP address - Select this option to manually enter the IP address.</p> <ul style="list-style-type: none"> ● IP Address - Type in the 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 necessary, type in secondary IP address for necessity in the future.</p>

After finished the above settings, click OK to save the settings and return to previous page.

Click any index (7-10) to get the following web page:

WAN >> Multi-PVC/VLAN >> Channel 7

Enable Channel 7:

WAN Type : ADSL ▼

General Settings	ATM QoS
VPI 1	QoS Type UBR ▼
VCI 47	PCR 0
Protocol PPPoA ▼	SCR 0
Encapsulation VC MUX ▼	MBS 0
<input type="checkbox"/> Add VLAN Header	
VLAN Tag 0	
Priority 0	

Bridge mode

Enable

Physical Members

P1 P2 P3 P4

OK
Cancel

Available settings are explained as follows:

Item	Description
Enable Channel 7~10	Enable - Click it to enable the configuration of this channel. Disable - Click it to disable the configuration of this channel.
WAN Type	The connections and interfaces created in every channel may select a specific WAN type to be built upon. In the Multi-VLAN application, only the Ethernet WAN type is available. The user will be able to select the physical WAN interface the channel shall use here.
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 - Enter 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>
Bridge mode	<p>Enable - Click it to enable Bridge mode for such channel.</p> <p>Physical Members - Group the physical ports by checking the corresponding check box(es) for applying the bridge connection.</p>

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 ▼
4.	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 ▼
9.	UBR ▼	0	0	0	Disable ▼
10.	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.
3. Channel 3 are reserved for USB WAN.

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.
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 enabled 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.

II-1-4 WAN Budget

This function is used to determine the data *traffic volume* for each WAN interface respectively to prevent from overcharges for data transmission by the ISP. Please note that the Quota Limit and Billing cycle day of month settings will need to be configured correctly first in order for some period calculations to be performed correctly.

II-1-4-1 General Setup

WAN >> WAN Budget



General Setup		Status			
Index	Enable	Quota	When quota exceeded	Time cycle	Duration
WAN1	<input type="checkbox"/>	OMB/OMB			0/00/00 00:00~0/00/00 00:00
WAN2	<input type="checkbox"/>	OMB/OMB			0/00/00 00:00~0/00/00 00:00
WAN3	<input type="checkbox"/>	OMB/OMB			0/00/00 00:00~0/00/00 00:00

Note:

1. The budget traffic information provided here is for reference only, please consult your ISP for the actual traffic usage and charges.
2. When hardware acceleration function is used, the monitored WAN traffic of Ethernet WAN interfaces may be slightly inaccurate.

OK

Cancel

Click WAN1/WAN2/WAN3 link to open the following web page.

WAN >> WAN Budget

WAN 1

Enable

Criterion and Action

Quota Limit: MB

When quota exceeded :

Shutdown WAN interface

Using **Notification Object**

Set **Mail Alert** or **SMS message**.

Select the day of a month when your (cellular) data resets.

Data quota resets on day at

Note:

1. Please make sure the **Time and Date** of the router is configured.
2. SMS message and mail will be sent when the usage reaches 95% and 100% of quota.

OK

Cancel

Available settings are explained as follows:

Item	Description
Enable	Check the box to enable such function.
Quota Limit	Enter the data traffic quota allowed for such WAN interface. There are two unit (MB and GB) offered for you to specify.
When quota exceeded	Check the box(es) as the condition(s) for the system to perform when the traffic has exceeded the budget limit. Shutdown WAN interface - All the outgoing traffic through such WAN interface will be terminated. <ul style="list-style-type: none"> ● Using Notification Object - The system will send out a notification based on the content of the notification

	<p>object.</p> <ul style="list-style-type: none"> ● Set Mail Alert - The system will send out a warning message to the administrator when the quota is running out. However, the connection charges will be calculated continuously. ● Set SMS message - The system will send out SMS message to the administrator when the quota is running out.
Monthly	<p>Some ISP might apply for the network limitation based on the traffic limit per month. This setting is to offer a mechanism of resetting the traffic record every month.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p style="text-align: center;"> <input checked="" type="radio"/> Monthly <input type="radio"/> Custom </p> </div> <p>Select the day of a month when your (cellular) data resets. Data quota resets on day <input type="text" value="1"/> at <input type="text" value="00:00"/></p> <p>Data quota resets on day ... - You can determine the starting day in one month.</p>
Custom	<p>This setting allows the user to define the billing cycle according to his request. The WAN budget will be reset with an interval of billing cycle.</p> <p>Monthly is default setting. If long period or a short period is required, use Custom. The period of cycle duration is between 1 day and 60 days. You can determine the cycle duration by specifying the days and the hours. In addition, you can specify which day of today is in a cycle.</p> <p>Use Cycle in hours -</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p style="text-align: center;"> <input type="radio"/> Monthly <input checked="" type="radio"/> Custom </p> </div> <p> <input checked="" type="radio"/> Use Cycle in hours <input type="radio"/> Use Cycle in days </p> <p>Usage counter resets at the beginning of each cycle. Cycle duration : <input type="text" value="1"/> days and <input type="text" value="0"/> hours Today is day <input type="text" value="1"/> in the cycle.</p> <ul style="list-style-type: none"> ● Cycle duration: Specify the days and hours to reset the traffic record. For example, 7 means the whole cycle is 7 days; 20 means the whole cycle is 20 days. When the time is up, the router will reset the traffic record automatically. ● Today is day - Specify the day in the cycle as the starting point which Vigor router will reset the traffic record. For example, "3" means the third day of the cycle duration. <p>Use Cycle in days -</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p style="text-align: center;"> <input type="radio"/> Monthly <input checked="" type="radio"/> Custom </p> </div> <p> <input type="radio"/> Use Cycle in hours <input checked="" type="radio"/> Use Cycle in days </p> <p>Usage counter resets at the beginning of each cycle. Cycle duration : <input type="text" value="1"/> days. Today is day <input type="text" value="1"/> in the cycle and data quota resets at <input type="text" value="00:00"/></p> <ul style="list-style-type: none"> ● Cycle duration: Specify the days to reset the traffic record. For example, 7 means the whole cycle is 7 days; 20 means the whole cycle is 20 days. When the time is up, the router will reset the traffic record automatically. ● Today is day - Specify the day and time for data quota

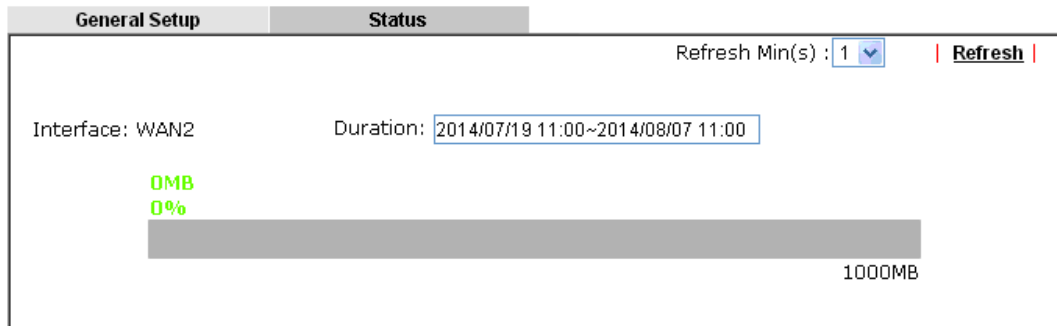
	rest in the cycle as the starting point which Vigor router will reset the traffic record. For example, “3” means the third day of the cycle duration.
--	---

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

II-1-4-2 Status

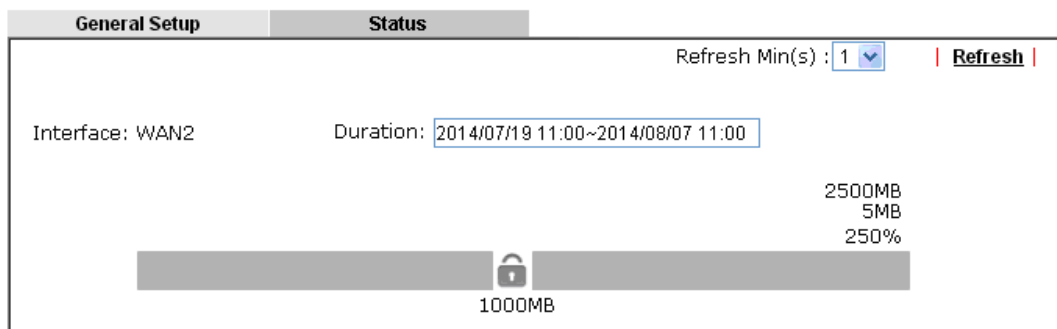
The status page displays the status WAN budget, including the duration and the usage.

WAN >> WAN Budget



If the WAN budget is exhausted, a lock will be displayed on the page if Shutdown WAN interface is selected. Which means no data transmission will be carried out. Moreover, the system will send out a warning message to the administrator if Send Mail Alert to Administrator is selected. Or, the system will send out SMS message to the administrator if Send SMS messages to Administrator is selected.

WAN >> WAN Budget



Application Notes

A-1 How to assign an IPv6 address to LAN clients?

This document introduces how to set up Vigor Router for the LAN clients to obtain an IPv6 address from it.

1. Make sure there is a WAN interface that has IPv6 access available. (See How to configure IPv6 on WAN interface?)

IPv4 Internet Access				
	Line / Mode	IP Address	MAC Address	Up Time
WAN1	Fiber / ---	Disconnected	00-1D-AA-B3-85-B9	00:00:00
WAN2	Ethernet / PPPoE	118.200.100.121	00-1D-AA-B3-85-BA	2:56:04
WAN3	USB / ---	Disconnected	00-1D-AA-B3-85-BB	00:00:00

IPv6 Internet Access				
	Mode	Address	Scope	Up Time
WAN2	AICCU	2401::E800:100:70::2/128 FE80::E800:100:70:2/128	Global Link	2:56:01

2. Go to LAN >> General Setup, and click on "IPv6" for the LAN subnet to enter IPv6 setting page.

LAN >> General Setup

General Setup

Index	Enable	DHCP	IP Address		
LAN 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.1.1	Details Page	IPv6 <input type="checkbox"/>
LAN 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.2.1	Details Page	IPv6 <input type="checkbox"/>
IP Routed Subnet	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.0.1	Details Page	

DHCP Server Option

Note:

Please enable LAN 2 on [LAN >> VLAN](#) page before configure them.

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

Inter-LAN Routing

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

OK

- In IPv6 Setup page, set WAN Primary Interface to the WAN interface that has IPv6 service available, enable DHCPv6 Server, and click OK to apply.

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

/

Unique Local Address(ULA) configuration

Off ▼ / 64

Current IPv6 Address Table

Index	IPv6 Address/Prefix Length	Scope
1	FE80::21D:AAFF:FE08:F520/64	Link

DNS Server IPv6 Address Deploy when WAN is up ▼

Primary DNS Server:

Secondary DNS Server:

Management SLAAC(stateless) ▼

Other Option(0-bit)

DHCPv6 Server

Enable Server Disable Server

IPv6 Address Random Allocation

Auto IPv6 range

Start IPv6 Address:

End IPv6 Address:

Advance setting

Advance setting

- With the above configuration, LAN clients will be able to obtain an IPv6 address and an IPv6 Gateway from Vigor Router. For Windows PC, we may check this by command "ipconfig".

```
C:\Documents and Settings\User>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.11
    Subnet Mask . . . . . : 255.255.255.0
    IP Address. . . . . : 2401:e000:100:0070:0025:100b:ce5d:e0
9b
    IP Address. . . . . : 2401:e000:100:0070:10da:e9ff:feb1:ee
d8
    IP Address. . . . . : fe80::16da:e9ff:feb1:cad8%5
    Default Gateway . . . . . : 192.168.1.1
    IP Address. . . . . : fe80::21d:aaff:feb3:85b8%5
```

PC will be able to ping and get response from an IPv6 host, e.g. "ipv6.google.com".

```
C:\WINDOWS>ping ipv6.google.com

Pinging ipv6.1.google.com [2404:6800:4008:c01::71] with 32 bytes of data:

Reply from 2404:6800:4008:c01::71: time=326ms
Reply from 2404:6800:4008:c01::71: time=172ms
Reply from 2404:6800:4008:c01::71: time=243ms
Reply from 2404:6800:4008:c01::71: time=246ms

Ping statistics for 2404:6800:4008:c01::71:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 172ms, Maximum = 326ms, Average = 246ms
```

A-2 How to configure IPv6 on WAN interface?

This document is going to demonstrate how to implement an IPv6 address on Vigor Router's WAN.

1. Before configuring IPv6 on WAN, please make sure the router is connected to the IPv4 Internet.

Online Status

Physical Connection System Uptime: 0day 0:3:29

IPv4		IPv6			
LAN Status	Primary DNS: 168.95.1.1	Secondary DNS: 168.95.192.1			
IP Address	TX Packets	RX Packets			
192.168.86.1	643	793			
WAN 1 Status >> Dial PPPoA					
Enable	Line	Name	Mode	Up Time	
Yes	ADSL		PPPoA	00:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
---	---	0	0	0	0
WAN 2 Status >> Drop PPPoE					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:03:20	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
118.106.103.153	168.95.192.1	79	3	81	9

2. Go to WAN >> Internet Access, click on IPv6 of the WAN interface that you would like to configure an IPv6 address.

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode	Details Page	IPv6
WAN1		ADSL / VDSL2	PPPoE / PPPoA	Details Page	IPv6
WAN2		Ethernet	PPPoE	Details Page	IPv6
WAN3		USB	None	Details Page	IPv6

3. Select a Connection Type from the drop-down list, enter the required parameters. Then click OK and reboot the router to apply the settings.

WAN >> Internet Access ?

WAN 2

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
Internet Access Mode			
Connection Type			
<div style="border: 1px solid gray; padding: 5px; display: inline-block;"> Offline Offline PPP TSPC AICCU DHCPv6 Client Static IPv6 6in4 Static Tunnel 6rd </div>			
<input type="button" value="OK"/>			

- After accomplishing the configurations, Network Administrator may check the status from the IPv6 tab on Online Status >> Physical Connection page.

Online Status

Physical Connection System Uptime: 0day 0:57:49

IPv4
 IPv6

LAN Status			
IP Address			
2406:FA70:F1::C64/123 (Global)			
FE80::21D:5A7F:FE0A:47A0/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
1277	3060	182180	450067

WAN1 IPv6 Status			
Enable	Mode	Up Time	
No	Offline	---	
IP	Gateway IP		
---	---		

WAN2 IPv6 Status			
Enable	Mode	Up Time	
Yes	Static IPv6	0:57:43	
IP	Gateway IP		
2406:FA70:F1::C64/123 (Global)	2406:FA70:F1::C64		
2406:FA70:F1::C64/123 (Global)			
FE80::21D:5A7F:FE0A:47A0/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
5180	2612	445044	224316

- Furthermore, Network Administrator may test the connectivity of IPv6 from the router by going to Diagnostics >> Ping Diagnosis and selecting "IPv6".

Diagnostics >> Ping Diagnosis

Ping Diagnosis

IPV4
 IPV6

Note: If you want to ping a LAN PC or you don't want to specify which WAN to ping through, please select "Unspecified".

Ping through:

Ping IPv6 Address:

Result |

```

Pinging ipv6.google.com with 64 bytes of Data:
Receive reply from 2404:6800:4008:C04::66, time==400ms
Receive reply from 2404:6800:4008:C04::66, time==400ms
Receive reply from 2404:6800:4008:C04::66, time==400ms
Receive reply from 2404:6800:4008:C04::66, time==400ms
Receive reply from 2404:6800:4008:C04::66, time==400ms
Packets: Sent = 5, Received = 5, Lost = 0 (0% loss)
  
```

Below we will provide some examples of configuring IPv6 with different connection types.

PPP (Point-to-Point Protocol)

This applies if the IPv4 access mode is PPPoE, and the IPv4 ISP also provides an IPv6 address. To use IPv6 PPP, you just need to choose the Connection Type to "PPP", no other setting is required.

WAN >> Internet Access



WAN 2

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
Internet Access Mode			
Connection Type		PPP	
WAN Connection Detection			
Mode		Always On	
RIPng Protocol			
<input type="checkbox"/> Enable			

Note:

IPv4 WAN setting should be PPPoE / PPPoA client.

OK

Cancel

TSPC (Tunnel Setup Protocol Client)

In this mode, the IPv6 connectivity is provided by a tunnel broker on the IPv4 Internet through a tunnel set up by Tunnel Setup Protocol (TSP). To use TSPC, you'll need to sign up for a tunnel broker service and get a username and password first, then, configure the router as follows:

1. Set Connection Type to TSPC.
2. Enter the Username and Password registered at the TSP server.
3. Enter the IP or Domain Name of the TSPC server for Tunnel Broker.

WAN >> Internet Access



WAN 2

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
Internet Access Mode			
Connection Type		TSPC	
TSPC Configuration			
Username		mamepv6	
Password		*****	
Tunnel Broker		broker.aarnet.net.au	
WAN Connection Detection			
Mode		Always On	

OK

Cancel

Static IPv6

If your ISP provides a static IPv6 address for you, you may configure that IPv6 address for WAN by doing the following steps:

1. Set Connection Type to Static IPv6.
2. Enter the IPv6 address and Prefix Length which provided by the ISP, and click Add.

WAN >> Internet Access ?

WAN 2

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
Internet Access Mode			
Connection Type: Static IPv6			
Static IPv6 Address Configuration			
IPv6 Address: 2406:1000:1:3ea3 / Prefix Length: 123			
<input type="button" value="Add"/> <input type="button" value="Delete"/>			
Current IPv6 Address Table			
Index	IPv6 Address/Prefix Length	Scope	
1	FE80::6FFB:C69D/128	Link	

3. You should see the IPv6 address in Current IPv6 Address Table. Then, specify the IP address of IPv6 Gateway.

WAN >> Internet Access ?

WAN 2

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
Internet Access Mode			
Connection Type: Static IPv6			
Static IPv6 Address Configuration			
IPv6 Address: / Prefix Length: /			
<input type="button" value="Add"/> <input type="button" value="Delete"/>			
Current IPv6 Address Table			
Index	IPv6 Address/Prefix Length	Scope	
1	2406:1000:1:3ea3/123	Global	
2	FE80::21D:AAFF:FECE:2DD2/64	Link	

Static IPv6 Gateway configuration

IPv6 Gateway Address: 2406:1000:1:3ea3

WAN Connection Detection

Mode: Always On

Bridge Mode

Enable Bridge Mode

Bridge Subnet: LAN 1

6in4 Static Tunnel

In this mode, the IPv6 connectivity is provided by a tunnel broker on the IPv4 Internet through a tunnel configured manually. To use 6in4 Static Tunnel, you need sign up for a tunnel broker service and get an IPv6 address and routed IPv6 prefixes first. Then, configure the router as follows:

1. Set Connection Type to 6in4 Static Tunnel.
2. Enter the tunnel server's IPv4 address in Remote Endpoint IPv4 Address.
3. Enter the router's IPv6 address in 6in4 IPv6 Address.
4. Enter the routed IPv6 prefix in LAN Routed Prefix.

WAN >> Internet Access



WAN 2

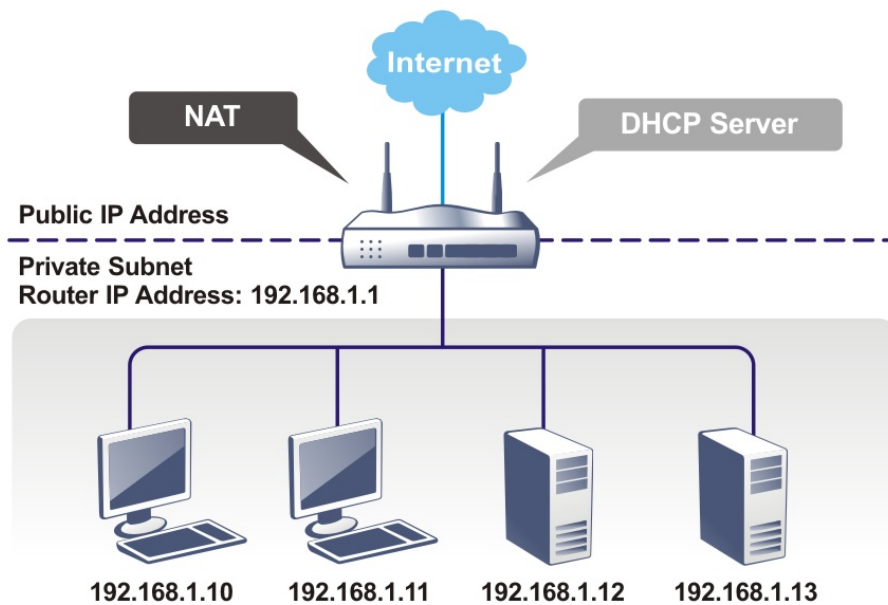
PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
Internet Access Mode			
Connection Type		6in4 Static Tunnel	
6in4 Static Tunnel			
Remote Endpoint IPv4 Address		216.211.221.16	
6in4 IPv6 Address		2001:47c:15:836::2 / 64 (default:64)	
LAN Routed Prefix		2001:47c:15:836:: / 64 (default:64)	
Tunnel TTL		255 (default:255)	
WAN Connection Detection			
Mode		Always On	

OK Cancel

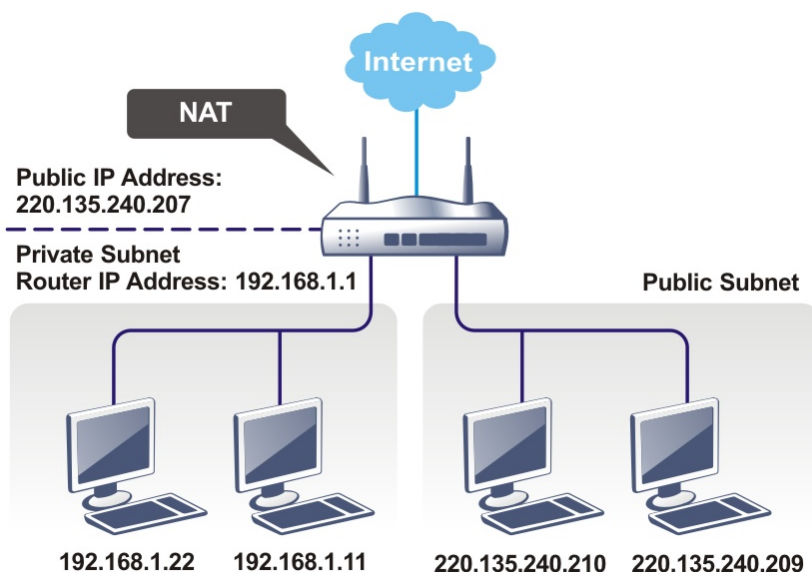
II-2 LAN

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.

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)

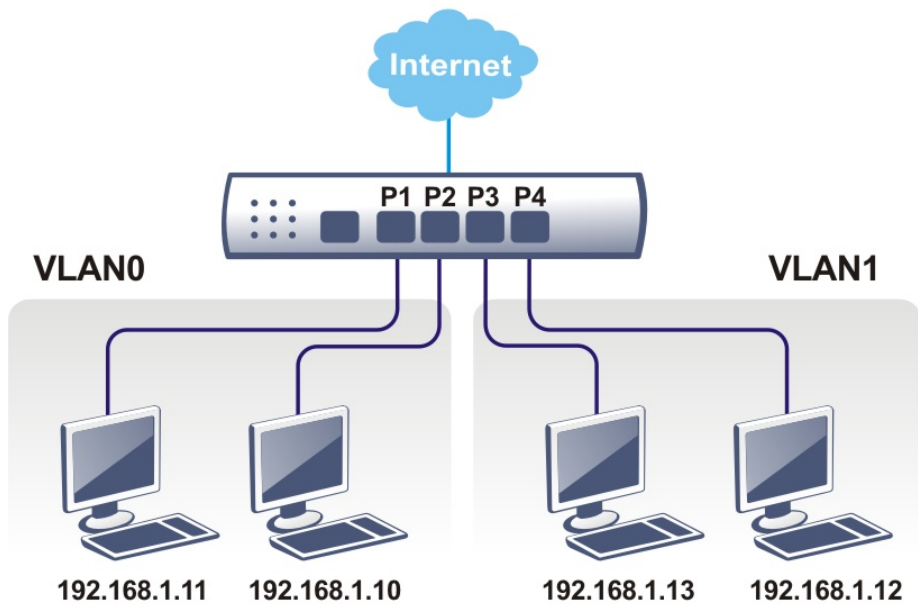
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

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 8 virtual LANs. To manage the communication between different groups, please set up rules in Virtual LAN (VLAN) function and the rate of each.



Web User Interface



II-2-1 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 several subnets provided by the router which allow users to divide groups into different subnets (LAN1 - LAN2). 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 can be operated under NAT or Route mode. IP Routed Subnet can be operated under Route mode.

LAN >> General Setup

General Setup

Index	Enable	DHCP	IP Address		
LAN 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.1.1	Details Page	IPv6
LAN 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.2.1	Details Page	IPv6
IP Routed Subnet	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.0.1	Details Page	

DHCP Server Option

Note:

Please enable LAN 2 on [LAN >> VLAN](#) page before configure them.

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

Inter-LAN Routing

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

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>Enable- Basically, LAN1 status is enabled in default. LAN2 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</p>

	<p>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>
DHCP Server Option	DHCP packets can be processed by adding option number and data information when such function is enabled. Refer to II-2-1-5 DHCP Server Option.
Force router to use DNS server IP address	Force Vigor router to use DNS servers configured in LAN1/LAN2 instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).
Inter-LAN Routing	Check the box to link two or more different subnets (LAN and LAN).

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

II-2-1-1 Details Page for LAN1 – Ethernet TCP/IP and DHCP 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.

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 / 24"/> ▾ RIP Protocol Control: <input type="text" value="Disable"/> ▾	DHCP Server Configuration <input type="radio"/> Disable <input checked="" type="radio"/> Enable Server <input type="radio"/> Enable Relay Agent Start IP Address: <input type="text" value="192.168.1.10"/> IP Pool Counts: <input type="text" value="200"/> (max. 253) 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"/>

Available settings are explained as follows:

Item	Description
Network Configuration	For NAT Usage, IP Address - Type in private IP address for connecting to a local private network (Default: 192.168.1.1). Subnet Mask - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24) RIP Protocol Control, Disable - deactivate the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default) Enable - activate the RIP protocol.
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically 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. 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. Disable Server - Let you manually assign IP address to every host in the LAN. Enable Server - Let the router assign IP address to every host in the LAN. <ul style="list-style-type: none"> ● Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.

- IP Pool Counts - Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.
- Gateway IP Address - Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway.
- Lease Time - Enter the time to determine how long the IP address assigned by DHCP server can be used.
- Clear DHCP lease for inactive clients periodically - Whenever a DHCP client requests an IP address from the LAN DHCP server, the server will give out an IP to this client for a certain amount of time (e.g., 1 day). However, even if this client only uses the IP for say 5 minutes, the server still "reserves" 1 day for that client. Because a DHCP server only has a limited number of IPs to lease to its DHCP clients, soon enough all the IPs will be used out and then no one will be able to get any IPs from this server anymore. Therefore, this feature is used to get the IP back from inactive clients (i.e. doesn't use the IP but the server still reserves the IP for him).

Enable Relay Agent -Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.

- DHCP Server IP Address - It is available when Enable Relay Agent is checked. Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.

DNS Server IP Address

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

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

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

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

Physical Connection		System Uptime: 22:22:45	
IPV4	IPV6		
LAN Status	Primary DNS: 8.8.8.8	Secondary DNS: 8.8.4.4	
IP Address	TX Packets	RX Packets	
192.168.1.1	0	41533	

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

If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately.

Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable) connection.

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

II-2-1-2 Details Page for LAN2

LAN >> General Setup

LAN 2 Ethernet TCP / IP and DHCP Setup	LAN 2 IPv6 Setup
<p>Network Configuration</p> <p> <input type="radio"/> Enable <input checked="" type="radio"/> Disable <input checked="" type="radio"/> For NAT Usage <input type="radio"/> For Routing Usage </p> <p>IP Address: <input type="text" value="192.168.2.1"/></p> <p>Subnet Mask: <input type="text" value="255.255.255.0 / 24"/></p>	<p>DHCP Server Configuration</p> <p> <input type="radio"/> Disable <input checked="" type="radio"/> Enable Server <input type="radio"/> Enable Relay Agent </p> <p>Start IP Address: <input type="text" value="192.168.2.10"/></p> <p>IP Pool Counts: <input type="text" value="100"/> (max. 253)</p> <p>Gateway IP Address: <input type="text" value="192.168.2.1"/></p> <p>Lease Time: <input type="text" value="259200"/> (s)</p> <p><input checked="" type="checkbox"/> Clear DHCP lease for inactive clients periodically.</p> <hr/> <p>DNS Server IP Address</p> <p>Primary IP Address: <input type="text"/></p> <p>Secondary IP Address: <input type="text"/></p>

OK

Available settings are explained as follows:

Item	Description
Network Configuration	<p>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>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 - 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>DHCP Server IP Address - It is available when Enable Relay</p>

	<p>Agent is checked. Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.</p> <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 IP Address	<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 data-bbox="699 1680 1396 1848" data-label="Table"> <p>Online Status</p> <hr/> <p>Physical Connection System Uptime: 22:22:45</p> <table border="1"> <thead> <tr> <th colspan="2">IPv4</th> <th colspan="2">IPv6</th> </tr> </thead> <tbody> <tr> <td>LAN Status</td> <td>Primary DNS: 8.8.8.8</td> <td colspan="2">Secondary DNS: 8.8.4.4</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>0</td> <td colspan="2">41533</td> </tr> </tbody> </table> </div> <p>If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.</p> <p>If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable)</p>	IPv4		IPv6		LAN Status	Primary DNS: 8.8.8.8	Secondary DNS: 8.8.4.4		IP Address	TX Packets	RX Packets		192.168.1.1	0	41533	
IPv4		IPv6															
LAN Status	Primary DNS: 8.8.8.8	Secondary DNS: 8.8.4.4															
IP Address	TX Packets	RX Packets															
192.168.1.1	0	41533															

connection.

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

II-2-1-3 Details Page for IP Routed Subnet

LAN >> General Setup

TCP/IP and DHCP Setup for IP Routed Subnet

Network Configuration <input type="radio"/> Enable <input checked="" type="radio"/> Disable For Routing Usage IP Address: <input type="text" value="192.168.0.1"/> Subnet Mask: <input type="text" value="255.255.255.0 / 24"/> RIP Protocol Control: <input type="text" value="Disable"/>	DHCP Server Configuration Start IP Address: <input type="text"/> IP Pool Counts: <input type="text" value="0"/> (max. 32) Lease Time: <input type="text" value="259200"/> (s) <input type="checkbox"/> Use LAN Port <input checked="" type="checkbox"/> P1 <input checked="" type="checkbox"/> P2 <input checked="" type="checkbox"/> Use MAC Address <table border="1"><thead><tr><th>Index</th><th>Matched MAC Address</th><th>given IP Address</th></tr></thead><tbody></tbody></table> MAC Address : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> <input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/>	Index	Matched MAC Address	given IP Address
Index	Matched MAC Address	given IP Address		

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 Routing Usage,</p> <p>IP Address - Type in private IP address for connecting to a local private network (Default: 192.168.1.1).</p> <p>Subnet Mask - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)</p> <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 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>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>Lease Time - Enter the time to determine how long the IP address assigned by DHCP server can be used.</p> <p>Use LAN Port - Specify an IP for IP Route Subnet. If it is enabled, DHCP server will assign IP address automatically for the clients coming from P1. Please check the box of P1.</p> <p>Use MAC Address - Check such box to specify MAC address.</p> <p>MAC Address - Enter the MAC Address of the host one by one and click Add to create a list of hosts which can be assigned, deleted or edited from above pool. Set a list of MAC Address for 2nd DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2nd subnet won't get an IP address belonging to 1st subnet.</p> <p>Add - Enter the MAC address in the boxes and click this button to add.</p> <p>Delete - Click it to delete the selected MAC address.</p> <p>Edit - Click it to edit the selected MAC address.</p> <p>Cancel - Click it to cancel the job of adding, deleting and editing.</p>

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

II-2-1-4 Details Page for LAN1~ LAN2 – IPv6 Setup

There are two configuration pages for each LAN port, 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

/

Unique Local Address(ULA) configuration

Off / 64

Current IPv6 Address Table

Index	IPv6 Address/Prefix Length	Scope
1	FE80::21D:AAFF:FE08:F520/64	Link

DNS Server IPv6 Address Deploy when WAN is up

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

IPv6 Address Random Allocation

Auto IPv6 range

Start IPv6 Address ::

End IPv6 Address ::

Advance setting

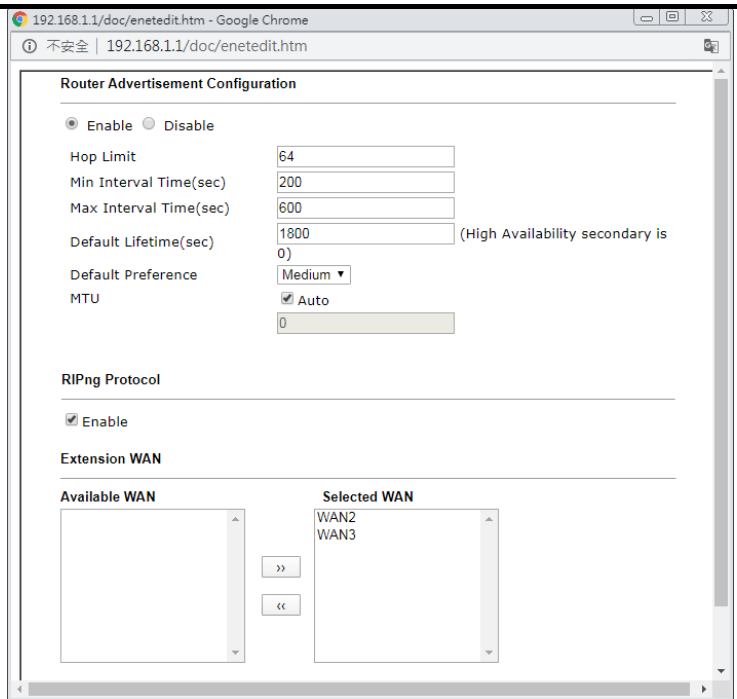
Advance setting

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	IPv6 Address -Type static IPv6 address for LAN. Prefix Length - Enter the fixed value for prefix length.

	<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>Unique Local Addresses (ULAs) are private IPv6 addresses assigned to LAN clients.</p> <p>Off - ULA is disabled.</p> <p>Manually ULA Prefix - LAN clients will be assigned ULAs generated based on the prefix manually entered.</p> <p>Auto ULA Prefix - LAN clients will be assigned ULAs using an automatically-determined prefix.</p>
Current IPv6 Address Table	Display current used IPv6 addresses.
DNS Server IPv6 Address	<p>Deploy when WAN is up - The RA (router advertisement) packets will be sent to LAN PC with DNS server information only when network connection by any one of WAN interfaces is up.</p> <p>Enable - The RA (router advertisement) packets will be sent to LAN PC with DNS server information no matter WAN connection is up or not.</p> <ul style="list-style-type: none"> ● Primary DNS Sever - Enter the IPv6 address for Primary DNS server. ● Secondary DNS Server -Type another IPv6 address for DNS server if required. <p>Disable - DNS server will not be used.</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"> ● Off - No IP address is assigned. ● 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. <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 Configuration	<p>Disable Server -Click it to disable DHCPv6 server.</p> <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>IPv6 Address Random Allocation - Check it to assign the DHCPv6 IP address randomly to prevent the attacks from the IPv6 reconnaissance techniques.</p> <p>Auto IPv6 range - IPv6 address(es) will be assigned by DHCPv6 server automatically.</p> <p>Start IPv6 Address / End IPv6 Address -Enter the start and end address for IPv6 server.</p> <p>Advance setting - Click the Edit button to configure advanced IPv6 settings for DHCPv6 server.</p>
Advance setting	More options are offered under the Advance setting. Click Edit to open the pop-up window.



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.

Disable - Click it to disable router advertisement server.

Hop Limit - The value is required for the device behind the router when IPv6 is in use.

Min/Max Interval Time (sec) - It defines the interval (between minimum time and maximum time) for sending RA (Router Advertisement) packets.

Default Lifetime (sec) - Within such period of time, Vigor2762 can be treated as the default gateway.

Default Preference - It determines the priority of the host behind the router when RA (Router Advertisement) packets are transmitted.

MTU - It means Max Transmit Unit for packet. If **Auto** is selected, the router will determine the MTU value for LAN.

RIPng Protocol - RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.

Extension WAN - In addition to the default WAN used for IPv6 traffic specified in the WAN Primary Interface in the LAN IPv6 Setup page, additional WANs can be selected to carry IPv6 traffic by enabling them in the Extension WAN section.

Available WAN - Additional WANs available but not currently selected to carry IPv6 traffic.

Selected WAN - Additional WANs selected to carry IPv6 traffic.

After making changes on the Advance setting page, click the OK button to retain the changes and return to the LAN IPv6 Setup page. Be sure to click OK on the LAN IPv6 Setup page or else changes made on the Advance setting page will not be saved.

II-2-1-5 DHCP Server Option

DHCP Server Option can be configured by clicking the DHCP Server Option button on the LAN >>General Setup screen.

LAN >> General Setup

DHCP Server Customized Status

Customized List

Enable	Interface	Option	Type	Data

Enable:

Interface: All LAN1 LAN2 IP Routed Subnet

Next Server IP Address/SIAddr :

Option Number:

Data Type: ASCII Character (EX :Option:18, Data:/path)

Hexadecimal Digit (EX: Option:18, Data:2f70617468)

Address List (EX :Option:44, Data:172.16.2.10,172.16.2.20...)

Data: Max: 127 characters

Note:

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" Detail Page's "Domain Name" field.

Available settings are explained as follows:

Item	Description
Customized List	Shows all the DHCP options that have been configured in the system.
Enable	If selected, DHCP option entry is enabled. If unselected, DHCP option entry is disabled.
Interface	LAN interface(s) to which this entry is applicable.
Next Server IP Address/SIAddr	Overrides the DHCP Next Server IP address (DHCP Option 66) supplied by the DHCP server.
Option Number	DHCP option number (e.g., 100).
Data Type	Type of data in the Data field: ASCII Character - A text string. Example: /path. Hexadecimal Digit - A hexadecimal string. Valid characters are from 0 to 9 and from <i>a</i> to <i>f</i> . Example: 2f70617468. Address List - One or more IPv4 addresses, delimited by commas.
Data	Data of this DHCP option.

To add a DHCP option entry from scratch, clear the data entry fields (Enable, Interface, Option Number, DataType and Data) by clicking Reset. After filling in the values, click Add to create the new entry.

To add a DHCP option entry modeled after an existing entry, click the model entry in Customized List. The data entry fields will be populated with values from the model entry. After making all necessary changes for the new entry, click Add to create it.

To modify an existing DHCP option entry, click on it in Customized List. The data entry fields will be populated with the current values from the entry. After making all necessary changes, click Update to save the changes.

To delete a DHCP option entry, click on it in Customized List, and then click Delete.

II-2-2 VLAN

Vigor router provides extremely high-speed connectivity for the highest speed local data transfer of any server or local PCs. On the Wireless-equipped models (e.g., Vigor2762n), each of the wireless SSIDs can also be grouped within one of the VLANs.

Tagged VLAN

The tagged VLANs (802.1q) can 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 is just passed to the LAN. You can set the priorities for LAN-side QoS. You can assign each of VLANs to each of the different IP subnets that the router may also be operating, to provide even more isolation. The said 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 (P1 ~ P3) to separate the clients into different VLAN group.

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

Below is an example page in Vigor2762Vac:

LAN >> VLAN Configuration ?

VLAN Configuration

Enable

VLAN	LAN			Wireless LAN				Wireless LAN 5G				Subnet	VLAN Tag			
	P1	P2	P3	SSID1	SSID2	SSID3	SSID4	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 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 checked="" 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 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"/>	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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1 ▼	<input type="checkbox"/>	0	0 ▼



Info

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

Available settings are explained as follows:

Item	Description
Enable	Click it to enable VLAN configuration.
LAN	P1 - P3 - Check the LAN port(s) to group them under the selected VLAN.

Wireless LAN	SSID1 - SSID4 - Check the SSID boxes to group them under the selected VLAN.
Wireless LAN 5G	SSID1 - SSID4 - Check the SSID boxes to group them under the selected VLAN. It is available for "ac" model only.
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	Enable - Check the box to enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the LAN while sending them out. Please Enter the tag value and specify the priority for the packets sending by LAN. VID - Enter the value as the VLAN ID number. The range is form 0 to 4095. Priority - Enter the packet priority number for such VLAN. The range is from 0 to 7.



Info

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

Inter-LAN Routing

The Vigor router supports up to 15 VLANs. Each VLAN can be set up to use one or more of the Ethernet ports and wireless LAN Service Set Identifiers (SSIDs). Within the grid of VLANs (horizontal rows) and LAN interfaces (vertical columns),

- all hosts within the same VLAN (horizontal row) are visible to one another
- all hosts connected to the same LAN or WLAN interface (vertical column) are visible to one another if
 - they belong to the same VLAN, or
 - they belong to different VLANs, and inter-LAN routing (LAN>>General Setup) between them is enabled (see below).

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

Inter-LAN Routing

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

Inter-LAN Routing allows different LAN subnets to be interconnected or isolated. It is only available when the VLAN functionality is enabled. In the Inter-LAN Routing matrix, a selected checkbox means that the 2 intersecting LANs can communicate with each other.

Vigor2762 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				Wireless LAN 5G				VLAN Tag			
	P1	P2	P3	SSID1	SSID2	SSID3	SSID4	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 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 checked="" 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 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"/>	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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1 ▼	<input type="checkbox"/>	0	0 ▼

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.

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

Inter-LAN Routing

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

Note:

LAN2 is available when VLAN is enabled.

Vigor router supports up to two 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.

II-2-3 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
 Apply Strict Bind to Subnet:

ARP Table | [Select All](#) | [Sort](#) | [Refresh](#) | [Add/Update to IP Bind List](#)

IP Address	Mac Address	HOST ID	
192.168.1.5	00-1D-AA-00-00-00		
192.168.1.10	60-A4-4C-E6-5A-4F	A1000381	

IP Address: <input style="width: 90%;" type="text"/>	Mac Address: <input style="width: 90%;" type="text"/>
Comment: <input style="width: 90%;" type="text"/> <small>Max: 12 characters</small>	
<input type="button" value="Add"/>	<input type="button" value="Update"/> <input type="button" value="Delete"/>

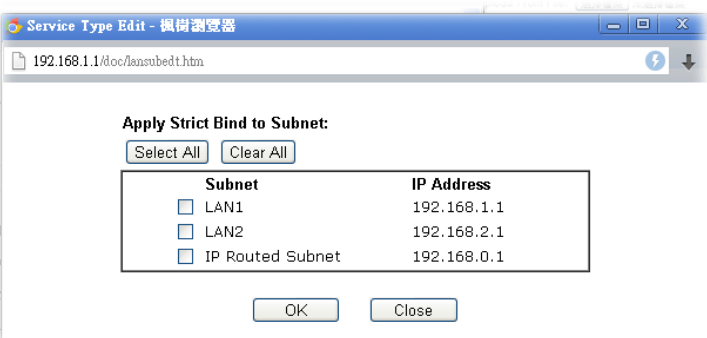
IP Bind List (Limit: 300 entries) | [Select All](#) | [Sort](#) |

Index	IP Address	Mac Address	Host ID	Comment

Backup IP Bind List : <input type="button" value="Backup"/>	Upload From File: <input type="button" value="選擇檔案"/> 未選擇任何檔案	<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	<p>Click this radio button to block the connection of the IP/MAC which is not listed in IP Bind List.</p> <p>Apply Strict Bind to Subnet – Choose the subnet(s) for applying the rules of Bind IP to MAC.</p> 
ARP Table	<p>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.</p>
Select All	<p>Click this link to select all the items in the ARP table.</p>
Sort	<p>Reorder the table based on the IP address.</p>
Refresh	<p>Refresh the ARP table listed below to obtain the newest ARP table information.</p>
Add or Update	<p>IP Address – Enter the IP address that will be used for the specified MAC address.</p> <p>Mac Address – Enter the MAC address that is used to bind with the assigned IP address.</p> <p>Comment – Type a brief description for the entry.</p>
Add	<p>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.</p>
Update	<p>It allows you to edit and modify the selected IP address and MAC address that you create before.</p>
Delete	<p>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.</p>
IP Bind List	<p>It displays a list for the IP bind to MAC information.</p>
Backup	<p>Store the configuration for Bind IP to MAC as a file.</p>
Restore	<p>Restore the previously stored configuration file and apply to such page.</p>



Info

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.

When you finish the configuration, click OK to save the settings.

II-2-4 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 connecting to the mirroring port. Last, it is more convenient and easy to configure in user's interface.

LAN >> LAN Port Mirror

LAN Port Mirror

Port Mirror:
 Enable Disable

	Port1	Port2	Port3	WAN2	WAN1
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"/>
Mirrored Rx Port	<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.

II-2-5 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 type="checkbox"/> Enable		
802.1X ports:		
<input type="checkbox"/> P1	<input type="checkbox"/> P2	<input type="checkbox"/> P3

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.

II-3 Hardware Acceleration

Hardware Acceleration is also called PPA in DrayTek for it is based on Protocol Processing Engine (PPE) of Infineon. It can only support 128 sessions for network traffic (IN & OUT) with implementing three kinds of modes - Disable, Auto and Manual.



Info

Such feature is only supported by certain firmware version.

II-3-1 Setup

When the data traffic is heavy and data transmission is getting slowly and slowly, you can configure this page to accelerate the data streaming by hardware itself. Open Hardware Acceleration to access into the following page:

Hardware Acceleration >> Setup

Mode:
 Protocol: TCP UDP
 Option: Accelerate heaviest traffic sessions
 Specific Hosts:

Index	Enable	Dest Port Start	Dest Port End	Private IP	
1.	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="button" value="Choose PC"/>
2.	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="button" value="Choose PC"/>
3.	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="button" value="Choose PC"/>
4.	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="button" value="Choose PC"/>
5.	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="button" value="Choose PC"/>

WAN Information:

	Status	TX	RX
WAN1-ADSL	Enable	--	--
WAN2-Ethernet	Enable	V	--

	Status	TX	RX
WAN1-ADSL	Disable	--	--
WAN2-Ethernet	Enable	V	V

Note:

1. If Hardware Acceleration is enabled, the accelerated sessions will bypass Traffic Graph.
2. Hardware Acceleration and WAN1&WAN2 Budget can't be enabled simultaneously.

Available settings are explained as follows:

Item	Description
Mode	<p>Disable - The default setting.</p> <p>Auto - When the hardware acceleration is configured with the Auto mode, the sessions with the heaviest loading and the lower latency traffic will be added into PPA. However, the Auto mode does not support UDP protocol by designed.</p> <p>Manual - The Manual mode implements three sub-items--</p>

	<i>Accelerate most heavy traffic sessions, Apply the Class Rule in Quality of Service, and Specific Hosts.</i> Each of these sub-items can support TCP and UDP protocol.
Protocol	There are two types supported by this function, TCP and UDP.
Option	<p>Accelerate heaviest traffic sessions - Such option is available in Auto Mode, too. But the UDP protocol is only supported in this sub-item.</p> <p>Specific Hosts - This sub-item provides 5 hosts for adding NAT sessions into the PPA. For the PPA only supports 128 sessions, these hosts will share these sessions. Therefore, the performance will be lower than only one host.</p> <p>Choose this option to specify certain PCs on LAN to apply the hardware acceleration.</p> <ul style="list-style-type: none"> ● Enable - Check the box to make PC(s) specified in the selected index entry to be applied. ● Dest Port Start - Enter the starting port for the PC(s) in LAN. ● Dest Port End - Enter the ending port for the PC(s) in LAN. ● Private IP/Choose PC - Enter the IP address as the selected host. Or click the Choose PC button to specify one IP address from the pop-up window.

Checking the PPA status

For checking whether the rule of PPA is working or not, a user can login to Vigor2862 series by using telnet. User can view how many sessions are transferring in each direction of PPA table after entering “`ppa -v`”.

```

> ppa -v
% PPA mode is Auto
% PPA mode is Manual <traffic>
% PPA time is 10
% PPA range is 255
*****
WAN Acceleration session
Session - Src_ip:Src_port ----- Dest_ip:Dest_port --- Nat_ip:Nat_port
*****
⏱
*****
LAN Acceleration session
Session - Src_ip:Src_port ----- Dest_ip:Dest_port --- Nat_ip:Nat_port
*****
0 - 192.168. 1. 10: 2938 - 119.236.154.122: 5590 - 192.168. 3. 10:52524
Src_mac:00:22:15:8f:85:59 ---- Dest_mac:00:50:7f:37:c8:4c
1 - 192.168. 1. 10: 2952 - 193. 88. 6. 13:33033 - 192.168. 3. 10:52538
Src_mac:00:22:15:8f:85:59 ---- Dest_mac:00:50:7f:37:c8:4c

```

II-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:

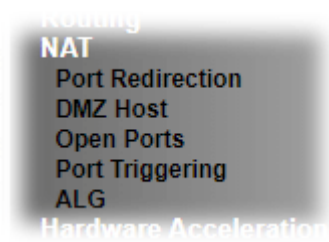
- Save cost on applying public IP address and apply efficient usage of IP address. NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.
- Enhance security of the internal network 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.



Info

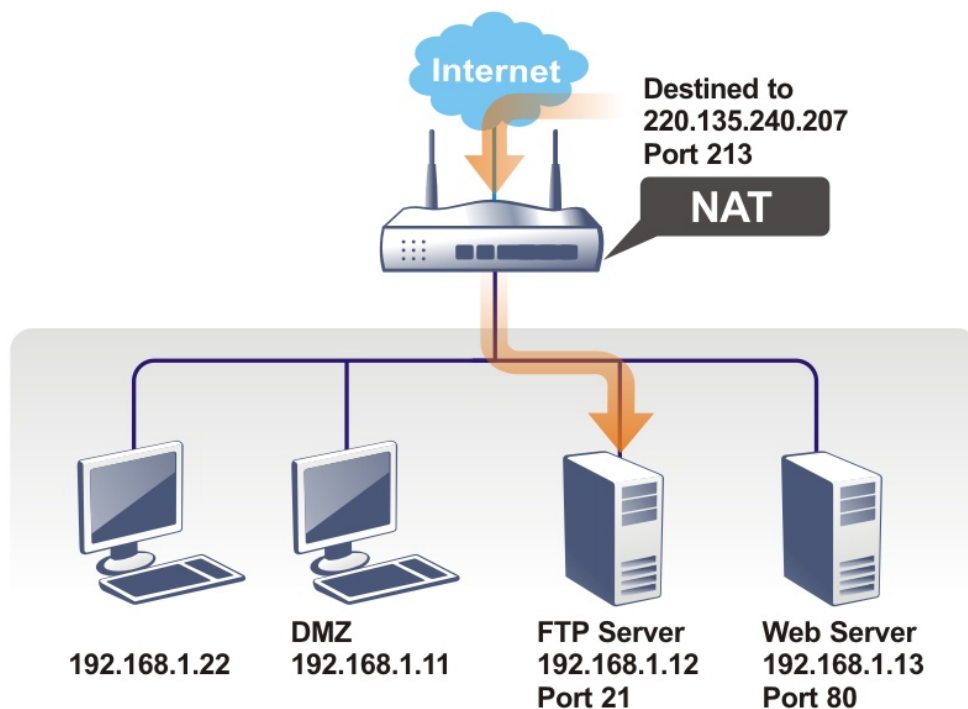
On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by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

Web User Interface



II-4-1 Port Redirection

Port Redirection is usually set up for server related service inside the local network (LAN), such as web servers, FTP servers, E-mail servers etc. Most of the case, you need a public IP address for each server and this public IP address/domain name are recognized by all users. Since the server is actually located inside the LAN, the network well protected by NAT of the router, and identified by its private IP address/port, the goal of Port Redirection function is to forward all access request with public IP address from external users to the mapping private IP address/port of the server.



The port redirection can only apply to incoming traffic.

To use this function, please go to NAT page and choose Port Redirection web page. The Port Redirection Table provides 40 port-mapping entries for the internal hosts.

NAT >> Port Redirection

Port Redirection | [Set to Factory Default](#) |

Index	Enable	Service Name	WAN Interface	Protocol	Public Port	Source IP	Private IP
<u>1.</u>	<input type="checkbox"/>		All			Any	
<u>2.</u>	<input type="checkbox"/>		All			Any	
<u>3.</u>	<input type="checkbox"/>		All			Any	
<u>4.</u>	<input type="checkbox"/>		All			Any	
<u>5.</u>	<input type="checkbox"/>		All			Any	
<u>6.</u>	<input type="checkbox"/>		All			Any	
<u>7.</u>	<input type="checkbox"/>		All			Any	
<u>8.</u>	<input type="checkbox"/>		All			Any	
<u>9.</u>	<input type="checkbox"/>		All			Any	
<u>10.</u>	<input type="checkbox"/>		All			Any	

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

Note:

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

Each item is explained as follows:

Item	Description
Index	Display the number of the profile.
Enable	Check the box to enable the port redirection 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.
Source IP	Display the IP object of the source IP.
Private IP	Display the IP address of the internal host providing the service.

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

NAT >> Port Redirection

Index No. 1

<input type="checkbox"/> Enable	
Mode	Single ▾
Service Name	<input type="text"/>
Protocol	TCP ▾
WAN Interface	ALL ▾
Public Port	<input type="text" value="0"/>
Source IP	IP Object ▾ None ▾
Private IP	<input type="text"/>
Private Port	<input type="text" value="0"/>

Note:

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

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable such port redirection setting.
Mode	Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select Range. In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered, the system will calculate and display the ending IP of private IP automatically.
Service Name	Enter the description of the specific network service.
Protocol	Select the transport layer protocol (TCP or UDP).
WAN Interface	Select the WAN interface used for port redirection. 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. Enter the required number on the first box (as the starting port) and the second box (as the ending port).
Source IP	Use the drop down list to specify an IP object. Or click IP Object link to create a new one for applying.
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). The second one will be assigned automatically later.
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.

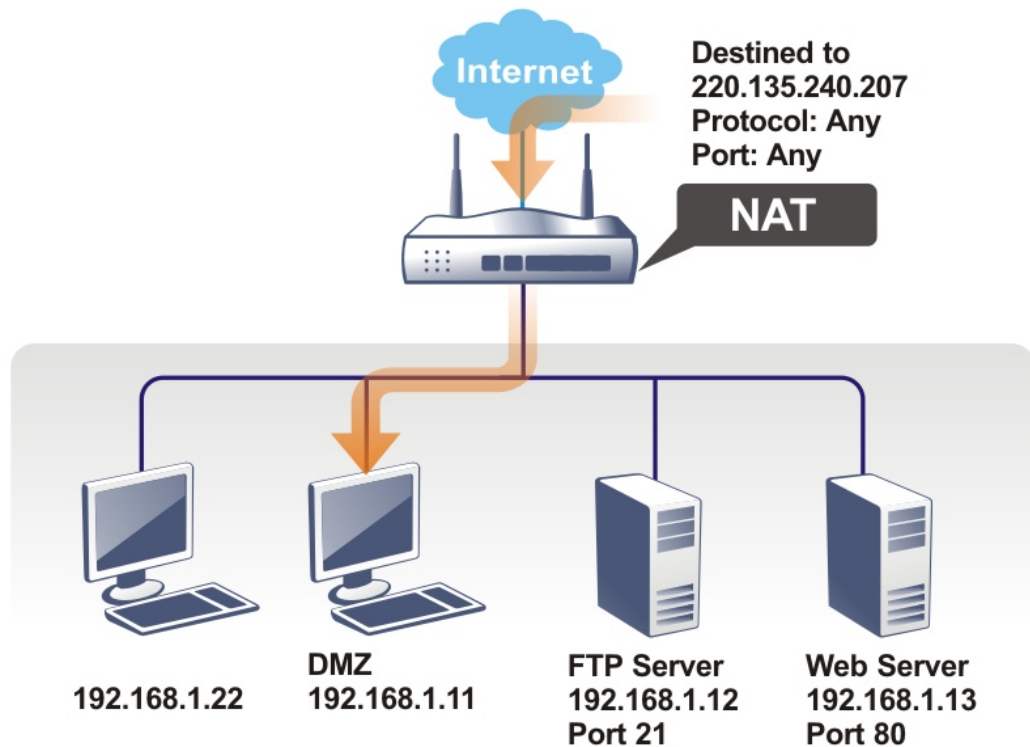
System Maintenance >> Management



IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup						
Router Name <input type="text" value="DrayTek"/>								
<input type="checkbox"/> Default:Disable Auto-Logout <input type="checkbox"/> Enable Validation Code in Internet/LAN Access		Management Port Setup <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports						
Internet Access Control <input type="checkbox"/> Allow management from the Internet Domain name allowed <input type="text"/> <input type="checkbox"/> FTP Server <input type="checkbox"/> HTTP Server <input type="checkbox"/> Enforce HTTPS Access <input checked="" type="checkbox"/> HTTPS Server <input type="checkbox"/> Telnet Server <input type="checkbox"/> TR069 Server <input type="checkbox"/> SSH Server <input checked="" type="checkbox"/> Disable PING from the Internet		Telnet Port <input type="text" value="23"/> (Default: 23) HTTP Port <input type="text" value="80"/> (Default: 80) HTTPS Port <input type="text" value="443"/> (Default: 443) FTP Port <input type="text" value="21"/> (Default: 21) TR069 Port <input type="text" value="8069"/> (Default: 8069) SSH Port <input type="text" value="22"/> (Default: 22)						
Access List from the Internet List <table border="1"> <thead> <tr> <th>index</th> <th>in</th> <th>IP / Mask</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="text" value="IP Object"/></td> <td><input type="text"/></td> </tr> </tbody> </table>		index	in	IP / Mask	1	<input type="text" value="IP Object"/>	<input type="text"/>	TLS/SSL Encryption Setup <input checked="" type="checkbox"/> Enable TLS 1.2 <input checked="" type="checkbox"/> Enable TLS 1.1 <input checked="" type="checkbox"/> Enable TLS 1.0 <input type="checkbox"/> Enable SSL 3.0
index	in	IP / Mask						
1	<input type="text" value="IP Object"/>	<input type="text"/>						
		AP Management <input checked="" type="checkbox"/> Enable AP Management						

II-4-2 DMZ Host

As mentioned above, Port Redirection can redirect incoming TCP/UDP or other traffic on particular ports to the specific private IP address/port of host in the LAN. However, other IP protocols, for example Protocols 50 (ESP) and 51 (AH), do not travel on a fixed port. Vigor router provides a facility DMZ Host that maps ALL unsolicited data on any protocol to a single host in the LAN. Regular web surfing and other such Internet activities from other clients will continue to work without inappropriate interruption. DMZ Host allows a defined internal user to be totally exposed to the Internet, which usually helps some special applications such as Netmeeting or Internet Games etc.



The security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

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

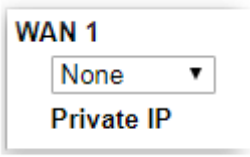
NAT >> DMZ Host Setup

DMZ Host Setup

WAN1	WAN2	WAN3
WAN 1		
None ▼		
Private IP		Choose IP

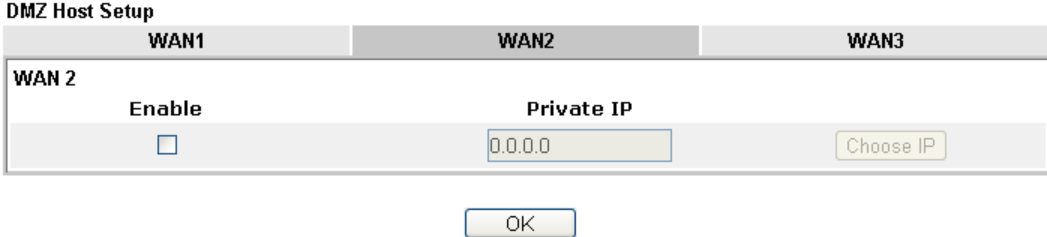
OK

Available settings are explained as follows:

Item	Description
	Choose Private IP first.
Private IP	Enter the private IP address of the DMZ host, or click Choose PC to select one.
Choose IP	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 screen. Click OK to save the setting.

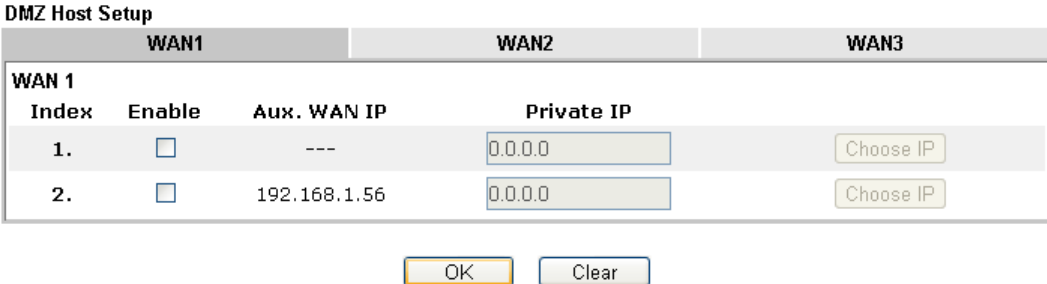
DMZ Host for WAN2, or WAN3 is slightly different with WAN1. See the following figure.

NAT >> DMZ Host Setup



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



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 IP	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 screen. Click OK to save the setting.
-----------	---

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

II-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	Enable	Comment	Source IP	Local IP Address
1.	<input type="checkbox"/>		Any	
2.	<input type="checkbox"/>		Any	
3.	<input type="checkbox"/>		Any	
4.	<input type="checkbox"/>		Any	
5.	<input type="checkbox"/>		Any	
6.	<input type="checkbox"/>		Any	
7.	<input type="checkbox"/>		Any	
8.	<input type="checkbox"/>		Any	
9.	<input type="checkbox"/>		Any	
10.	<input type="checkbox"/>		Any	

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

Note:

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

Available settings are explained as follows:

Item	Description
Index	Click the index number to edit or clear the corresponding entry.
Enable	Check to enable this entry.
Comment	Specify the name for the defined network service.
Source IP	Display the name of IP object used by such entry.
Aux. WAN IP	Display the IP alias setting used by such index. If no IP alias setting exists, such field will not appear.
Local IP Address	Display the private IP address of the local host offering the service.

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

Enable Open Ports

Comment

Source IP IP Object None

Private IP Choose IP

	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	TCP/UDP	0	0	2.	TCP/UDP	0	0
3.	TCP/UDP	0	0	4.	TCP/UDP	0	0
5.	TCP/UDP	0	0	6.	TCP/UDP	0	0
7.	TCP/UDP	0	0	8.	TCP/UDP	0	0
9.	TCP/UDP	0	0	10.	TCP/UDP	0	0

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Enable Open Ports	Check to enable this entry.
Comment	Make a name for the defined network application/service.
WAN Interface	Specify the WAN interface that will be used for this entry.
Source IP	Use the drop down list to specify an IP object. Or click IP Object link to create a new one for applying.
WAN IP	Specify the WAN IP address that will be used for this entry. This setting is available when WAN IP Alias is configured.
Private IP	Enter the private IP address of the local host or click Choose PC to select one. Choose IP - 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.

II-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	Enable	Comment	Triggering Protocol	Source IP	Triggering Port	Incoming Protocol	Incoming Port	
<u>1.</u>	<input type="checkbox"/>			Any				
<u>2.</u>	<input type="checkbox"/>			Any				
<u>3.</u>	<input type="checkbox"/>			Any				
<u>4.</u>	<input type="checkbox"/>			Any				
<u>5.</u>	<input type="checkbox"/>			Any				
<u>6.</u>	<input type="checkbox"/>			Any				
<u>7.</u>	<input type="checkbox"/>			Any				
<u>8.</u>	<input type="checkbox"/>			Any				
<u>9.</u>	<input type="checkbox"/>			Any				
<u>10.</u>	<input type="checkbox"/>			Any				

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

Available settings are explained as follows:

Item	Description
Index	Click the index number to edit or clear the corresponding entry.
Enable	Check to enable this entry.
Comment	Display the text which memorizes the application of this rule.
Triggering Protocol	Display the protocol of the triggering packets.
Source IP	Display the name of the IP object.
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.

Click the index number link to open the configuration page.

NAT >> Port Triggering

No. 1

Enable

Service: User Defined ▾

Comment:

Source IP: IP Group ▾ None ▾

Triggering Protocol: Any

Triggering Port: IP Object

Incoming Protocol: IP Group

Incoming Port: ---

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

Available settings are explained as follows:

Item	Description
Enable	Check to enable this entry.
Service	Choose the predefined service to apply for such trigger profile.
Comment	Enter the text to memorize the application of this rule.
Source IP	Use the drop down list to specify an IP object. Or click IP Object link to create a new one for applying.
Triggering Protocol	Select the protocol (TCP, UDP or TCP/UDP) for such triggering profile.
Triggering Port	Enter the port or port range for such triggering profile.
Incoming Protocol	When the triggering packets received, it is expected the incoming packets will use the selected protocol. Select the protocol (TCP, UDP or TCP/UDP) for the incoming data of such triggering profile.
Incoming Port	Enter the port or port range for the incoming packets.

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

II-4-5 ALG

ALG means Application Layer Gateway. There are two methods provided by Vigor router, RTSP (Real Time Streaming Protocol) ALG and SIP (Session Initiation Protocol) ALG, for processing the packets of voice and video.

RTSP ALG makes RTSP message, RTCP message, and RTP packets of voice and video be transmitted and received correctly via NAT by Vigor router.

However, SIP ALG makes SIP message and RTP packets of voice be transmitted and received correctly via NAT by Vigor router.

NAT >> ALG

ALG (Application Layer Gateway) | [Set to Factory Default](#) |

Enable ALG

<input type="checkbox"/> Enable	Protocol	Listen Port		TCP	UDP
<input type="checkbox"/>	SIP	5060	(1~65535)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	RTSP	554	(1~65535)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Available settings are explained as follows:

Item	Description
Enable ALG	Check to enable such function.
Listen Port	Type a port number for SIP or RTSP protocol.
TCP	Check the box to make correspond protocol message packet from TCP transmit and receive via NAT.
UDP	Check the box to make correspond protocol message packet from UDP transmit and receive via NAT.

II-5 Applications

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.

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 Vigor2762 Series will respond the specified private IP address.

Schedule

The Vigor router has a built-in 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.

RADIUS/TACACS+

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.

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.

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.

Web User Interface



II-5-1 Dynamic DNS

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. Open Applications>>Dynamic DNS.
3. Check Enable Dynamic DNS Setup.

Applications >> Dynamic DNS Setup

A screenshot of the Dynamic DNS Setup configuration page. The page title is "Dynamic DNS Setup" with a "Set to Factory Default" link. There is a checkbox for "Enable Dynamic DNS Setup" and buttons for "View Log" and "Force Update". Below this is a text input for "Auto-Update interval" set to "14400" with "Min(s) (180~14400)" to its right. A table titled "Accounts:" has columns for "Index", "Enable", and "Domain Name". The table contains six rows with indices 1 through 6, each with an unchecked "Enable" checkbox and an empty "Domain Name" field. At the bottom are "OK" and "Clear All" buttons.

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).
Enable	Check the box to enable such account.
Domain Name	Display the domain name that you set on the setting page of DDNS setup.

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

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

Index : 1

Enable Dynamic DNS Account

WAN Interface:

Service Provider:

Service Type:

Domain Name:

Login Name:

Password:

Wildcards

Backup MX

Mail Extender:

Determine 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	<p>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.</p> <p>WAN1/WAN2/WAN3 Only - While connecting, the router will use WAN1/WAN2/WAN3 as the only channel for such account.</p>
Service Provider	Select the service provider for the DDNS account.
Service Type	<p>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.</p> <p>Note that such option is not available when Customized is selected as Service Provider.</p>
Domain Name	<p>Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.</p> <p>Note that such option is not available when Customized is selected as Service Provider.</p>

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 Enter 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> <ul style="list-style-type: none"> ● WAN IP - If it is selected and the WAN IP of Vigor router is private, DDNS update will take place right away. ● 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.

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

DrayDDNS Settings

DrayDDNS, a new DDNS service developed by DrayTek, can record multiple WAN IP (IPv4) on single domain name. It is convenient for users to use and easily to set up. Each Vigor Router is available to register one domain name.

Choose DrayTek Global as the service provider, the web page will be displayed as follows:

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

Index : 1

Enable Dynamic DNS Account

Service Provider:

Status: Activated [Start Date:2019-02-01 Expire Date:2020-02-01]

Domain Name: .drayddns.com

Domain not exists! Re-establish on [MyVigor website](#).

Determine WAN IP: IPv4 IPv6

WAN Interfaces: WAN 1 WAN 2 WAN 3

Let's Encrypt certificate

Status: Empty

Auto Update:

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).
Service Provider	Choose DrayTek Global as the service provider. Wizard - This button is available when DrayTek Global is selected as

	<p>Service Provider. To activate the DrayTek's DDNS service, click it to enable license issued by DrayTek through Wizards>>Service Activation Wizard.</p> <p>Refer to section A-1 How to use DrayDDNS? for detailed information.</p>
Status	Display if the license is activated or not.
Determine 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> <ul style="list-style-type: none"> ● WAN IP - If it is selected and the WAN IP of Vigor router is private, DDNS update will take place right away. ● 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.
WAN Interfaces	WAN1/WAN2/WAN3 - While connecting, the router will use WAN1/WAN2/WAN3 as the channel for such account.
Let's Encrypt certificate	<p>Create - Click it to generate a certificate issued by Let's Encrypt for applying to such DDNS account.</p> <p>Auto Update - Check the box to make the system update the certificate automatically.</p>

Disable the Function and Clear all Dynamic DNS Accounts

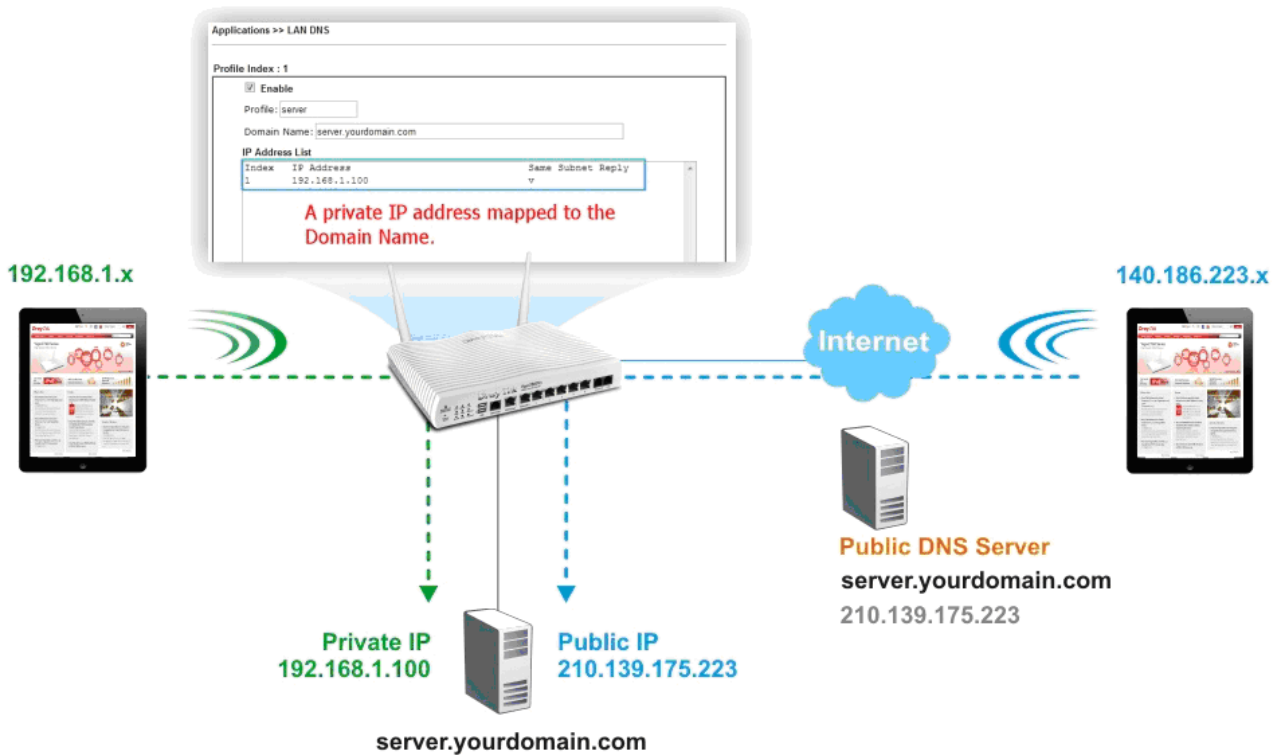
Uncheck Enable Dynamic DNS Setup, and click Clear All button to disable the function and clear all accounts from the router.

Delete a Dynamic DNS Account

Click the Index number you want to delete and then click Clear All button to delete the account.

II-5-2 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 Vigor2762 Series will respond the specified private IP address.



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 |

Index	Enable	Profile	Domain Name	Forwarding	DNS Server
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.	<input type="checkbox"/>			-	

<< 1-10 | 11-20 | 21-30 | 31-40 | 41-50 | 51-60 | 61-70 | 71-80 | 81-90 | 91-100 | 101-110 | 111-120 >>

OK

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profiles and recover to factory settings.

Index	Click the number below Index to access into the setting page.
Enable	Check the box to enable the selected profile.
Profile	Display the name of the LAN DNS profile.
Domain Name	Display the domain name of the LAN DNS profile.
Forwarding	Display that such profile is conditional DNS forwarding or not.
DNS Server	Display the IP adres of the DNS Server.

To create a LAN DNS profile:

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

Applications >> LAN DNS / DNS Forwarding

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.

CNAME(Alias Domain Name):

IP Address List

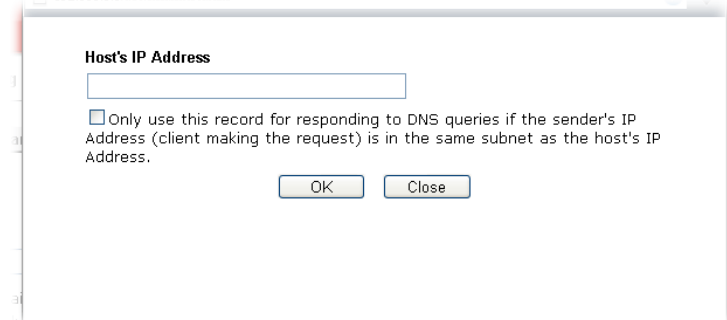
Index	IP Address	Same Subnet Reply

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable such profile.
Profile	Type a name for such profile. Note: If you type a name here for LAN DNS and click OK to save the configuration, the name also will be applied to conditional DNS forwarding automatically.
Domain Name	Enter the domain name for such profile.
CNAME (Alias Domain Name)	CNAME is abbreviation of Canonical name record. Such option is used to record the domain name or the host alias. Add - Click it to add a new host with specified reference.
IP Address List	The IP address listed here will be used for mapping with the domain name specified above. In general, one domain name

maps with one IP address. If required, you can configure two IP addresses mapping with the same domain name.

Add - Click it to open a dialog to Enter the host's IP address.

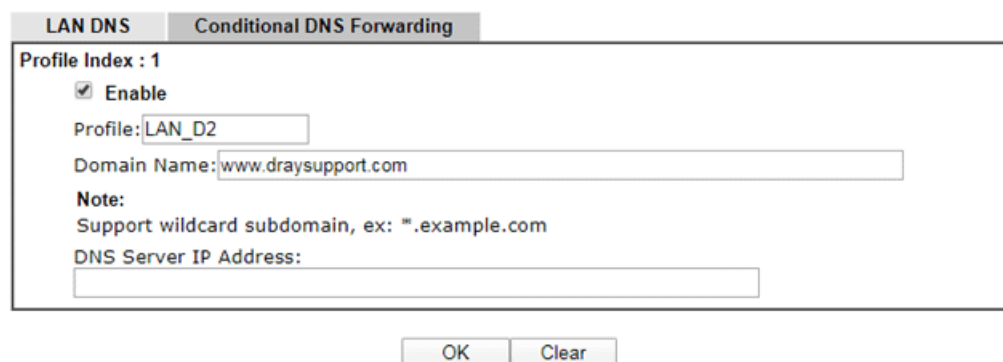


- Only use this record... - Different LAN PCs can share the same domain name. However, you have to check this box to make the router identify & respond the IP address for the DNS query coming from different LAN PC.

Delete - Click it to remove an existed IP address on the 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



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	Enter the domain name for such profile.
DNS Server IP Address	Enter 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.

II-5-3 DNS Security

DNS security is able to ensure that the incoming data is not falsified and the source of the data is secure and correct to prevent from DNS attack by someone.

II-5-3-1 General Setup

All of WAN interfaces of Vigor router can be configured with DNS Security enabled respectively.

Application >> DNS Security



DNS Security

General Setup		Domain Diagnosis		Refresh
Interface	Enable	Primary DNS	Secondary DNS	Bogus DNS Reply
WAN1	<input type="checkbox"/>	---	---	Pass ▼
WAN2	<input type="checkbox"/>	---	---	Pass ▼
WAN3	<input type="checkbox"/>	---	---	Pass ▼

Note:



The DNS server supports DNSSEC



The DNS server does not support DNSSEC, function may not work as expected even if it is enabled

OK

Available settings are explained as follows:

Item	Description
Interface	There are four WAN interfaces allowed to be set with DNS security enabled.
Enable	Check the box to enable the DNS security management.
Primary DNS	Display the IP address of primary DNS obtained from DHCP server or specified by Static WAN.
Secondary DNS	Display the IP address of secondary DNS obtained from DHCP server or specified by Static WAN.
Bogus DNS Reply	Sometime, Vigor router might encounter packets from bogus DNS inquiry. There are two ways to reply such DNS inquiry. Drop - Discard the packets. Pass - Accept the packets and let them pass through Vigor router.

II-5-3-2 Domain Diagnose

This page is used to configure settings for manually detecting if the domain is secure not.

Application >> DNS Security



DNS Security

General Setup | **Domain Diagnosis** | **DNS Cache**

Domain: IPv4 IPv6

Interface:

DNS Server:

Note:
If the domain has not been queried before, it will take a few seconds to process.

Result | [Clear](#) |

Domain Name	IP Address	Interface	Verify Result

Available settings are explained as follows:

Item	Description
Domain	Enter the domain name or IP address (IPv4/IPv6) that you want to query.
Interface	Specify the interface required for executing diagnose.
DNS Server	Enter the IP address of the DNS Server which will diagnose the domain specified above.
Diagnose	Click it to perform the diagnosis for the domain.
Result	The diagnosed information will be displayed on such field.

II-5-4 Schedule

The Vigor router has a built-in 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 : Current System Time | [System time set](#) | [Set to Factory Default](#) |

Index	Enable	Comment	Time	Frequency
1	<input type="checkbox"/>			Sun. <input type="checkbox"/>
2	<input type="checkbox"/>			Sun. <input type="checkbox"/>
3	<input type="checkbox"/>			Sun. <input type="checkbox"/>
4	<input type="checkbox"/>			Sun. <input type="checkbox"/>
5	<input type="checkbox"/>			Sun. <input type="checkbox"/>
6	<input type="checkbox"/>			Sun. <input type="checkbox"/>
7	<input type="checkbox"/>			Sun. <input type="checkbox"/>
8	<input type="checkbox"/>			Sun. <input type="checkbox"/>
9	<input type="checkbox"/>			Sun. <input type="checkbox"/>
10	<input type="checkbox"/>			Sun. <input type="checkbox"/>
11	<input type="checkbox"/>			Sun. <input type="checkbox"/>
12	<input type="checkbox"/>			Sun. <input type="checkbox"/>
13	<input type="checkbox"/>			Sun. <input type="checkbox"/>
14	<input type="checkbox"/>			Sun. <input type="checkbox"/>
15	<input type="checkbox"/>			Sun. <input type="checkbox"/>

Force on Force down

Available settings are explained as follows:

Item	Description
Current System Time	Display the time Vigor router used.
System time set	Click it to access into the time setup page (System Maintenance>>Time and Date).
Set to Factory Default	Clear all profiles and recover to factory settings.
Index	Click the index number link to access into the setting page of schedule.
Enable	Check the box to enable such schedule profile.
Comment	Display the name of the time schedule.
Time	Display the valid time period by time bar.

Frequency	Display which day(s) will be always on and which day(s) will be always off of the schedule profile by color boxes. ● - If it lights in green, it means such schedule is active.
-----------	--

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, say Index No. 1.
2. The detailed settings of the call schedule with index 1 are shown below.

Applications >> Schedule

Index No. 1 Current System Time 2000 Jan 1 Sat 21 : 14 : 49 | System time set |

Enable Schedule Setup

Comment

Start Date (yyyy-mm-dd) 2000 ▾ -1 ▾ -1 ▾

Start Time (hh:mm) 1 ▾ : 1 ▾

Duration Time (hh:mm) 22 ▾ : 0 ▾

End Time (hh:mm) 23 ▾ : 01 ▾

Action

How Often

Once

Weekdays

Sun Mon Tue Wed Thu Fri Sat

Monthly, on date 1 ▾

Cycle duration: 1 ▾ days (Cycle will start on the Start Date.)

Note:

Comment can only contain A-Z a-z 0-9 , . { } - _ () ^ \$! ~ ` |

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.
End Time (hh:mm)	It will be calculated automatically when Start Time and Duration Time are configured well.
Action	Specify which action Call Schedule should apply during the period of the schedule. Force On -Force the connection to be always on. Force Down -Force the connection to be always down.

How Often	<p>Specify how often the schedule will be applied.</p> <ul style="list-style-type: none"> ● Once -The schedule will be applied just once ● Weekdays -Specify which days in one week should perform the schedule. ● Monthly, on date - The router will only execute the action applied such schedule on the date (1 to 28) of a month. ● Cycle duration - Type a number as cycle duration. Then, any action applied such schedule will be executed per several days. For example, “3” is selected as cycle duration. That means, the action applied such schedule will be executed every three days since the date defined on the Start Date.
-----------	--

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.

II-5-5 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.

Vigor router can be operated as a RADIUS client. Therefore, this page is used to configure settings for external RADIUS server. Then LAN user of Vigor router will be authenticated by such server for network application.

RADIUS Setup

Enable

Comments:

Primary Server

Primary Server

Secret

Authentication Port

Retry times(1~3)

Secondary Server

Secondary Server

Secret

Authentication Port

Retry times(1~3)

RADIUS Server Status Log

[Refresh](#) | [Clear](#) |

Available settings are explained as follows:

Item	Description
Enable	Check to enable RADIUS client feature.
Comments	Enter a brief description.
Primary Server	<p>Primary Server - Enter the IP address of RADIUS server.</p> <p>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. The maximum length of the shared secret you can set is 36 characters.</p> <p>Authentication Port - The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.</p> <p>Retry - Enter a times number for sending the access request to the RADIUS server. When reaching the threshold of retry number, Vigor system will switch and send the request to the other RADIUS server (e.g., secondary server).</p>

Secondary Server	<p>Secondary Server - Enter the IP address of RADIUS server.</p> <p>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. The maximum length of the shared secret you can set is 36 characters.</p> <p>Authentication Port - The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.</p> <p>Retry - Enter a times number for sending the access request to the RADIUS server. When reaching the threshold of retry number, Vigor system will switch and send the request to the primary RADIUS server.</p>
RADIUS Server Status Log	Display the record of current status of RADIUS server.

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

II-5-6 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.



Info

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

<input type="checkbox"/> Enable UPnP Service	Default WAN
<input type="checkbox"/> Enable Connection Control Service	Default WAN
<input type="checkbox"/> Enable Connection Status Service	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 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.

II-5-7 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.

II-5-7-1 General Setting

Applications >> IGMP

General setting	Working status
<input type="checkbox"/> IGMP Proxy IGMP Proxy acts as a multicast proxy for hosts on the LAN side. Enable IGMP proxy to access any multicast group. This function takes no effect when Bridge Mode is enabled .	
Interface <input type="text" value="WAN1"/>	
IGMP version <input type="text" value="Auto"/>	
General Query Interval <input type="text" value="125"/> (seconds)	
Add PPP header <input type="checkbox"/>	
(Encapsulate IGMP in PPPoE)	
Enable IGMP syslog <input type="checkbox"/>	
<input type="checkbox"/> IGMP Snooping Enable: Forwards multicast traffic only to ports that are members of that group. Disable: Treats multicast traffic the same as broadcast traffic.	
<input type="checkbox"/> IGMP Fast Leave The router stops forwarding multicast traffic to a LAN port as soon as it receives a leave message from that port. Each LAN port should have no more than one IGMP host connected.	

Available settings are explained as follows:

Item	Description
IGMP Proxy	<p>Check this box to enable this function. The application of multicast will be executed through WAN /PVC/VLAN port. In addition, such function is available in NAT mode.</p> <p>Interface - Specify an interface for packets passing through.</p> <p>IGMP version - At present, two versions (v2 and v3) are supported by Vigor router. Choose the correct version based on the IPTV service you subscribe.</p> <p>General Query Interval - Vigor router will periodically check which IP obtaining IPTV service by sending query. It might cause inconvenience for client. Therefore, set a suitable time (unit: second) as the query interval to limit the frequency of query sent by Vigor router.</p> <p>Add PPP header - Check this box if the interface type for IGMP is PPPoE. It depends on the specifications regulated by each ISP. If you have no idea to enable or disable, simply contact your ISP providers.</p> <p>Enable IGMP syslog - Check the box to send the record related to the IGMP server to Syslog.</p>

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.
IGMP Fast Leave	Check this box to make the router stop forwarding multicast traffic to a LAN port as soon as it receives a leave message from that port. Each LAN port should have one IGMP host connected.

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

II-5-7-2 Working Group

Applications >> IGMP

General setting	Working status
-----------------	-----------------------

| [Refresh](#) |

Multicast Group Table

Index	Group ID	P1	P2	P3

IGMP Device Table

Index	MAC Address	IP Address	Interface	IGMP Version

Available settings are explained as follows:

Item	Description
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 P3	It indicates the LAN port used for the multicast group.

II-5-8 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.

Wake on LAN

Wake by: MAC Address ▼

IP Address: --- ▼

MAC Address: : : : : : Wake Up!

Result

Note:

Wake on LAN integrates with [Bind IP to MAC](#) function; only bound PCs can wake up through IP.

Available settings are explained as follows:

Item	Description
Wake by	If you choose to be woken by MAC Address, you have to Enter the correct MAC address of the host in MAC Address boxes.
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.

II-5-9 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.

II-5-9-1 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.

SMS Alert		Mail Alert		Set to Factory Default	
Index	Enable	SMS Provider	Recipient Number	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 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.
Enable	Click 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 Number	Enter the phone number of the one who will receive the SMS.
Notify Profile	Use the drop down list to choose a message profile. The recipient will get the content stated in the message profile. You can click the Notify Profile link to define the content of the SMS.
Schedule (1-15)	Enter 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.

II-5-9-2 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.

SMS Alert		Mail Alert		Set to Factory Default	
Index	Enable	Mail Service	Mail Address	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 same Mail Server.

Available settings are explained as follows:

Item	Description
Index	Check the box to enable such profile.
Enable	Click the box to enable such profile.
Mail Service	Use the drop down list to choose mail service object. All of the available objects are created in Object Settings>>SMS/Mail Service Option. If there is no object listed, click Mail Service link to define a new one with specified service provider.
Mail Address	Enter the e-mail address of the one who will receive the notification message.
Notify Profile	Use the drop down list to choose a message profile. The recipient will get the content stated in the message profile. You can click the Notify Profile link to define the content of the mail message.
Schedule (1-15)	Enter 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.

II-5-10 Bonjour

Bonjour is a service discovery protocol which is a built-in service in Mac OS X; for Windows or Linux platform, there is correspondent software to enable this function for free.

Usually, users have to configure the router or personal computers to use above services. Sometimes, the configuration (e.g., IP settings, port number) is complicated and not easy to complete. The purpose of Bonjour is to decrease the settings configuration (e.g., IP setting). If the host and user's computer have the plug-in Bonjour driver install, they can utilize the service offered by the router by clicking the router name icon. In short, what the Clients/users need to know is the name of the router only.

To enable the Bonjour service, click **Application>>Bonjour** to open the following page. Check the box(es) of the server service(s) that you want to share to the LAN clients.

Applications >> Bonjour



Bonjour Setup

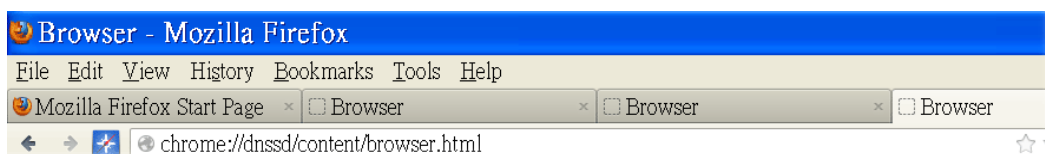
<input type="checkbox"/> Enable Bonjour Service
<input type="checkbox"/> HTTP Server
<input type="checkbox"/> Telnet Server
<input type="checkbox"/> FTP Server
<input type="checkbox"/> SSH Server
<input type="checkbox"/> LPR Printer Server

OK

Cancel

Below shows an example for applying the Bonjour feature that Vigor router can be used as the FTP server.

1. Here, we use Firefox and DNSSD to discover the service in such case. Therefore, just ensure the Bonjour client program and DNSSD for Firefox have been installed on the computer.



- Open the web browser, Firefox. If Bonjour and DNSSD have been installed, you can open the web page (DNSSD) and see the following results.

Interface	Name	Type	Domain	Service Info
2	DS1010Plus	_http._tcp.	local.	Select a service on the left to view further details.
2	DS1010Plus(WebDAV)	_http._tcp.	local.	
2	HP LaserJet 1300	_ipp._tcp.	local.	
2	tctseng-virtual-machine	_udisks-ssh._tcp.	local.	
2	tctseng-virtual-machine [00:0c:29:78:bc:24]	_workstation._tcp.	local.	
2	tomkao-desktop [00:0c:29:26:09:5d]	_workstation._tcp.	local.	

- Open System Maintenance>>Management. Type a name as the Router Name and click OK.

- Next, open Applications>>Bonjour. Check the service that you want to use via Bonjour.

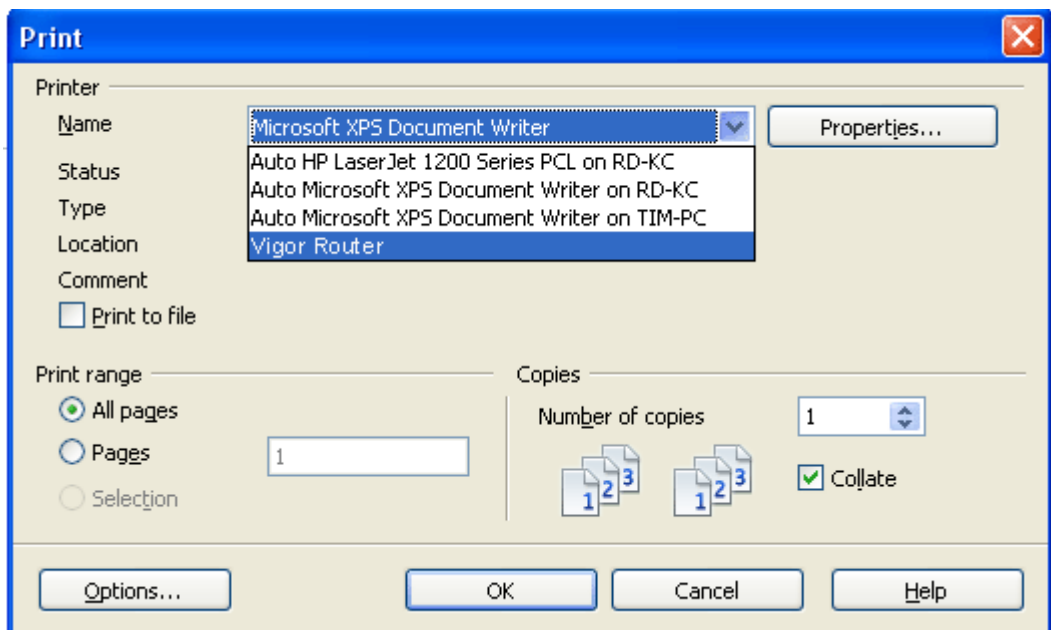
- Open the DNSSD page again. The available items will be changed as the follows. It means the Vigor router (based on Bonjour protocol) is ready to be used as a printer server, FTP server, SSH Server, Telnet Server, and HTTP Server.

DNSSD for Firefox

Browser Configuration Options Diagnostic Information

Interface	Name	Type	Domain	Service Info
2	DS1010Plus	_http._tcp.	local.	Select a service on the left to view further details.
2	DS1010Plus(WebDAV)	_http._tcp.	local.	
2	HP LaserJet 1300	_ipp._tcp.	local.	
2	Vigor Router	_ftp._tcp.	local.	
2	Vigor Router	_http._tcp.	local.	
2	Vigor Router	_printer._tcp.	local.	
2	Vigor Router	_ssh._tcp.	local.	
2	Vigor Router	_telnet._tcp.	local.	
2	tctseng-virtual-machine	_udisks-ssh._tcp.	local.	
2	tctseng-virtual-machine [00:0c:29:78:bc:24]	_workstation._tcp.	local.	
2	tomkao-desktop [00:0c:29:26:09:5d]	_workstation._tcp.	local.	

- Now, any page or document can be printed out through Vigor router (installed with a printer).



II-6 Routing

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.



Info

For more detailed information about using policy route, refer to SUPPORT >> TECH SUPPORT >> KNOWLEDGE BASE on www.draytek.com.

Web User Interface



II-6-1 Static Route

Go to Routing 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.

II-6-1-1 Static Route for IPv4

Routing >> Static Route Setup

IPv4			IPv6			Set to Factory Default	View Routing Table
Index	Enable	Destination Address	Index	Enable	Destination Address		
<u>1.</u>	<input type="checkbox"/>	???	<u>6.</u>	<input type="checkbox"/>	???		
<u>2.</u>	<input type="checkbox"/>	???	<u>7.</u>	<input type="checkbox"/>	???		
<u>3.</u>	<input type="checkbox"/>	???	<u>8.</u>	<input type="checkbox"/>	???		
<u>4.</u>	<input type="checkbox"/>	???	<u>9.</u>	<input type="checkbox"/>	???		
<u>5.</u>	<input type="checkbox"/>	???	<u>10.</u>	<input type="checkbox"/>	???		

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

Available settings are explained as follows:

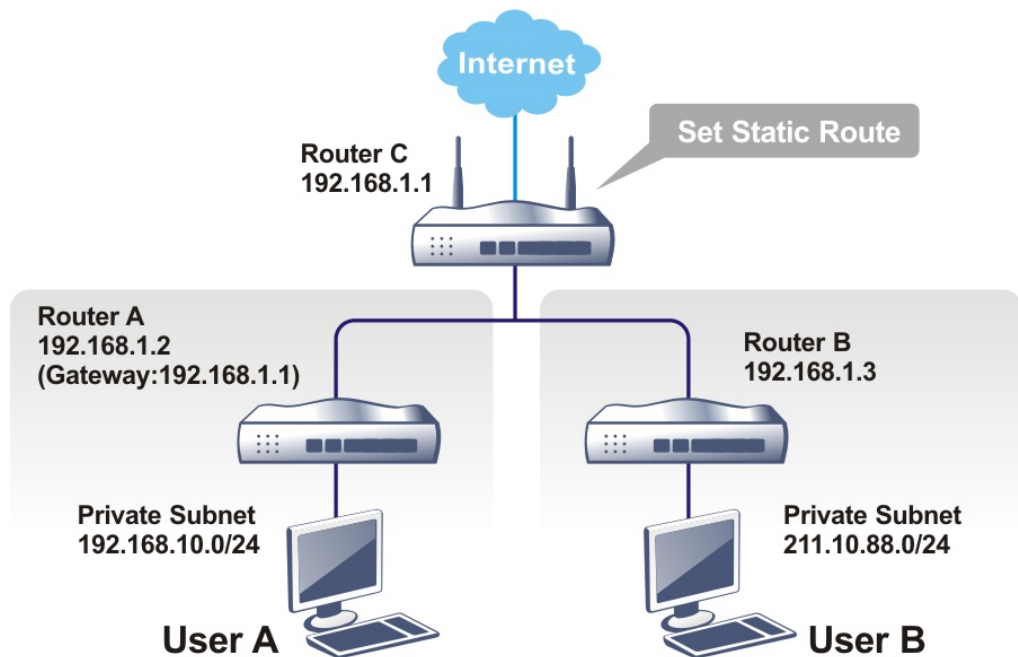
Item	Description
Index	The number (1 to 20) under Index allows you to open next page to set up static route.
Enable	Click the box to enable such profile.
Destination Address	Displays the destination address of the static route.
Set to Factory Default	Clear all of the settings and return to factory default settings.
Viewing Routing Table	Displays the routing table for your reference.

Add Static Routes to Private and Public Networks

Here is an example (based on IPv4) 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.



Info

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

- Click the **Routing >> 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**.

Routing >> Static Route Setup

Index No. 1

<input checked="" type="checkbox"/> Enable	
Destination IP Address	192.168.10.0
Subnet Mask	255.255.255.255 / 32
Gateway IP Address	192.168.1.2
Network Interface	LAN1

Note:

WAN4, WAN5, WAN6 are PVCs or VLANs that can be configured on the **Multi-PVC/VLAN** page.

OK Cancel Delete

Available settings are explained as follows:

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

- 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. Click **OK**.

Routing >> Static Route Setup

Index No. 2

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

Note:

WAN4, WAN5, WAN6 are PVCs or VLANs that can be configured on the **Multi-PVC/VLAN** page.

OK Cancel Delete

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

Diagnostics >> View Routing Table

IPv4

Key	Destination	Gateway	Interface
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
S~	211.100.88.0/ 255.255.255.0	via 192.168.1.3	LAN1

Key

C: Connected S: Static R: RIP *: default ~: private

II-6-1-2 Static Route for IPv6

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

Routing >> Static Route Setup

IPv4		IPv6		Set to Factory Default	View IPv6 Routing Table
Index	Enable	Destination Address	Index	Enable	Destination Address
<u>1.</u>	<input type="checkbox"/>	::/0	<u>11.</u>	<input type="checkbox"/>	::/0
<u>2.</u>	<input type="checkbox"/>	::/0	<u>12.</u>	<input type="checkbox"/>	::/0
<u>3.</u>	<input type="checkbox"/>	::/0	<u>13.</u>	<input type="checkbox"/>	::/0
<u>4.</u>	<input type="checkbox"/>	::/0	<u>14.</u>	<input type="checkbox"/>	::/0
<u>5.</u>	<input type="checkbox"/>	::/0	<u>15.</u>	<input type="checkbox"/>	::/0
<u>6.</u>	<input type="checkbox"/>	::/0	<u>16.</u>	<input type="checkbox"/>	::/0
<u>7.</u>	<input type="checkbox"/>	::/0	<u>17.</u>	<input type="checkbox"/>	::/0
<u>8.</u>	<input type="checkbox"/>	::/0	<u>18.</u>	<input type="checkbox"/>	::/0
<u>9.</u>	<input type="checkbox"/>	::/0	<u>19.</u>	<input type="checkbox"/>	::/0
<u>10.</u>	<input type="checkbox"/>	::/0	<u>20.</u>	<input type="checkbox"/>	::/0

<< [1 - 20](#) | [21 - 40](#) >> [Next](#) >>

OK Cancel

Available settings are explained as follows:

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

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

LAN >> Static Route Setup

Index No. 1

Enable

Destination IPv6 Address / Prefix Len: /

Gateway IPv6 Address:

Network Interface:

OK Cancel Delete

Available settings are explained as follows:

Item	Description
Enable	Click it to enable this profile.
Destination IPv6 Address / Prefix Len	Enter the IP address with the prefix length for this entry.
Gateway IPv6 Address	Enter the gateway address for this entry.
Network Interface	Use the drop down list to specify an interface for this static route.

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

II-6-2 Route Policy

II-6-2-1 General Setup

Routing >> Route Policy



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

Index	Enable	Comment	Protocol	Interface	Priority	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End	Move Up	Move Down
1	<input 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 value for such route policy profile.
Src IP Start	Displays the IP address for the start of the source IP.
Src IP End	Displays the IP address for the end of the source IP.
Dest IP Start	Displays the IP address for the start of the destination IP.
Dest IP End	Displays the IP address for the end of the destination IP.
Dest Port Start	Displays the IP address for the start of the destination port.
Dest Port End	Displays the IP address for the end of the destination port.
Move UP/Move Down	Use Up or Down link to move the order of the policy.
Wizard Mode	Allows to configure frequently used settings of route policy via three setting pages
Advance Mode	Allows to configure detailed settings of route policy.

To use Wizard Mode, simple do the following steps:

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

Routing >> 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 - Enter the source IP start for the specified WAN interface.</p> <p>Src IP End - Enter 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	Any - Any IP can be treated as the destination IP. Dest IP Start- Enter the destination IP start for the specified WAN interface. Dest IP End - Enter 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.
----------------	---

- Click Next to get the following page.

Routing >> Route Policy

Index: 1 Interface

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

Interface

Interface Address

Available settings are explained as follows:

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

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

Routing >> 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.

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

Index: 1 Configuration Summary

Criteria	
Source IP	Any
Destination IP	192.168.1.60 ~ 192.168.1.65
Interface	
WAN1	
More options	
Force NAT	
<input type="button" value=" < Back"/> <input type="button" value=" Next >"/> <input type="button" value=" Finish"/> <input type="button" value=" Cancel"/>	

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

To use Advance Mode, do the following steps:

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

Routing >> Route Policy

Index: 2

Enable

Comment

Criteria

Protocol

Source

Destination

Destination Port

Send via if Criteria Matched

Interface WAN/LAN

VPN

Gateway Default Gateway

Specific Gateway

Packet Forwarding to WAN/LAN via Force NAT

Force Routing

Failover to WAN/LAN

VPN

Route Policy

Gateway Default Gateway

Specific Gateway

Priority

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.
Comment	Type a brief explanation for such profile.
Protocol	Use the drop-down menu to choose a proper protocol for the WAN interface.
Source	<p>Any - Any IP can be treated as the source IP.</p> <p>IP Range - Define a range of IP address as source IP addresses.</p> <ul style="list-style-type: none"> ● Start - Type an address as the starting IP for such profile. ● End - Type an address as the ending IP for such profile. <p>IP Subnet - Define a subnet containing IP address and mask address.</p> <ul style="list-style-type: none"> ● Network - Type an IP address here. ● Mask - Use the drop down list to choose a suitable mask

	<p>for the network.</p> <p>IP Object / IP Group- Use the drop down list to choose a preconfigured IP object/group.</p>
Destination	<p>Any - Any IP can be treated as the destination IP.</p> <p>IP Range - Define a range of IP address as destination IP addresses.</p> <ul style="list-style-type: none"> ● Start - Type an address as the starting IP for such profile. ● End - Type an address as the ending IP for such profile. <p>IP Subnet - Define a subnet containing IP address and mask address.</p> <ul style="list-style-type: none"> ● Network - Type an IP address here. ● Mask - Use the drop down list to choose a suitable mask for the network. <p>Domain Name - Specify a domain name as the destination.</p> <ul style="list-style-type: none"> ● Select - Click it to choose an existing domain name defined in Objects Setting>>String Object. ● Delete - Remove current used domain name. ● Add - Create a new domain name as the destination. <p>IP Object / IP Group- Use the drop down list to choose a preconfigured IP object/group.</p> <p>Country Object - Use the drop down list to choose a preconfigured object. Then all IPs within that country will be treated as the destination IP.</p>
Destination Port	<p>Any - Any port number can be treated as the destination port.</p> <p>Dest Port Range -</p> <ul style="list-style-type: none"> ● Start - Enter the destination port start for the destination IP. ● End - Enter 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.
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> <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.

	<ul style="list-style-type: none"> ● 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.
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>

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

II-6-2-2 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.

Diagnostics >> Route Policy Diagnosis

Test how the packets will be routed

- Mode** Analyze a single packet
 Analyze multiple packets by uploading an input file

Packet Information

Protocol

Src IP

Dst IP

Dst Port

Analyze

or

Diagnostics >> Route Policy Diagnosis

Test how the packets will be routed

- Mode** Analyze a single packet
 Analyze multiple packets by uploading an input file

Input File

未選擇檔案

([download](#) an example input file)

Analyze

Available settings are explained as follows:

Item	Description																																				
Mode	<p>Analyze a single packet - Choose such mode to make Vigor router analyze how a single packet will be sent by a route policy.</p> <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>Protocol - Specify a protocol (ICMP/UDP/TCP/ANY) 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> <div data-bbox="715 981 1380 1299" data-label="Image"> </div> <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> <div data-bbox="699 1456 1404 1825" data-label="Table"> <p>Load-Balance/Route Policy >> Diagnose</p> <p>Mode</p> <ul style="list-style-type: none"> analyze how a packet will be sent analyze how multiple packets as specified in the input file will be sent <p>Input File</p> <p>(download an example input file)</p> <p>Analysis</p> <table border="1"> <thead> <tr> <th>Profile</th> <th>Proto</th> <th>Src IP</th> <th>Dst IP</th> <th>Dst Port</th> <th>Matched Route</th> <th>Priority</th> <th>Matched Policy</th> <th>Priority</th> <th>Failovered</th> <th>Final Result</th> <th>Reason</th> </tr> </thead> <tbody> <tr> <td>LA-branch</td> <td>ICMP</td> <td>192.168.1.10</td> <td>10.10.10.10</td> <td>N/A</td> <td>No Match</td> <td>N/A</td> <td>No Match</td> <td>N/A</td> <td>No</td> <td>(null)</td> <td>The packet was dropped because neither "route" "policy" matches</td> </tr> <tr> <td>NY-</td> <td>TCP</td> <td>192.168.1.10</td> <td>10.10.10.10</td> <td>8080</td> <td>No Match</td> <td>N/A</td> <td>No Match</td> <td>N/A</td> <td>No</td> <td>(null)</td> <td>The packet was dropped because...</td> </tr> </tbody> </table> </div> <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>	Profile	Proto	Src IP	Dst IP	Dst Port	Matched Route	Priority	Matched Policy	Priority	Failovered	Final Result	Reason	LA-branch	ICMP	192.168.1.10	10.10.10.10	N/A	No Match	N/A	No Match	N/A	No	(null)	The packet was dropped because neither "route" "policy" matches	NY-	TCP	192.168.1.10	10.10.10.10	8080	No Match	N/A	No Match	N/A	No	(null)	The packet was dropped because...
Profile	Proto	Src IP	Dst IP	Dst Port	Matched Route	Priority	Matched Policy	Priority	Failovered	Final Result	Reason																										
LA-branch	ICMP	192.168.1.10	10.10.10.10	N/A	No Match	N/A	No Match	N/A	No	(null)	The packet was dropped because neither "route" "policy" matches																										
NY-	TCP	192.168.1.10	10.10.10.10	8080	No Match	N/A	No Match	N/A	No	(null)	The packet was dropped because...																										

Application Notes

A-1 How to set up Address Mapping with Route Policy?

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.

This document introduces how to set up address mapping with Route Policy. When a WAN interface has multiple public IP addresses, Administrator may specify the outgoing IP for certain internal IP address by a Route Policy.

1. Set up WAN IP Alias. Go to WAN >> Internet Access >> Details Page, and click on WAN IP Alias button.

Index	Enable	Aux. WAN IP
1.	<input checked="" type="checkbox"/>	---
2.	<input checked="" type="checkbox"/>	172.17.1.1
3.	<input checked="" type="checkbox"/>	172.17.2.2
4.	<input type="checkbox"/>	0.0.0.0
5.	<input type="checkbox"/>	0.0.0.0
6.	<input type="checkbox"/>	0.0.0.0
7.	<input type="checkbox"/>	0.0.0.0
8.	<input type="checkbox"/>	0.0.0.0

<< 1-8 | 9-16 | 17-24 | 25-32 >> **Next** >>

- (1) Check Enable.
- (2) Enter the WAN IP address.
- (3) Click OK to save.

After setting up the WAN IP Alias, the IP addresses will be shown in the drop-down list of Interface in Route Policy setting.

- Go to Routing>>Route policy. Create a Route Policy for specific IP address to send from specific WAN IP Address.

Load-Balance/Route Policy

Index: 1

Enable

Comment Floor_1

Criteria

Protocol Any

Source IP Range

Start: 192.168.1.20 End: 192.168.1.30

Destination Any

Destination Port Any

Send via if Criteria Matched

Interface WAN/LAN WAN1

VPN 2-172.17.1.1

Gateway Default Gateway VPN 1.test1

Specific Gateway

Packet Forwarding to WAN via Force NAT

Force Routing

Failover to WAN/LAN Default WAN

VPN VPN 1.test1

Route Policy Index 1

Gateway Default Gateway

Specific Gateway 0.0.0.0

Priority

Failback

New sessions affected by this Policy will be sent via primary interface once that interface resumes service; while existing sessions will remain on the failovered interface.

- Enable this policy.
 - Enter Source IP as the range of private IP address.
 - Leave the Destination IP and Port as Any.
 - Select Interface as WAN, and then select Interface address from the drop-down list. (The List can be edited in WAN IP Alias setting.)
 - Enable Failover to other WAN so the traffic will be sent via other Interface when the path fails. But do not enable this option if you want the traffic only to use a designated IP address.
 - Click OK to save.
- After the above configuration, packet source from the range between 192.168.1.20 and 192.168.1.30 sent to the Internet will use the public IP 172.17.1.1.

A-2 How to use destination domain name in a route policy?

Route Policy supports using a domain name as destination criteria. It provides a more direct way to set up route policies if the network administrator is trying to specify the gateway for the traffic that destined for a certain website.

To use a destination domain name as criteria, just select Domain Name as Destination in Criteria, and enter the domain name in the empty field.

Criteria

Protocol: Any

Source: IP Range

Start: 192.168.1.20 End: 192.168.1.30

Destination: Domain Name

-server1.draytek.com [Select] [Delete]

Add

Destination Port: Any

Or you may click Select, and use a string that is pre-defined in Objects Settings >> String Object as the domain name.

192.168.1.1/loc/strobjslt.htm

Objects Setting >> String Object

Index	String
<input type="radio"/>	1 Floor_1
<input type="radio"/>	32 Floor_2
<input type="radio"/>	33 sdapot
<input checked="" type="radio"/>	34 portal.draytek.com
<input type="radio"/>	65 Floor_3
<input type="radio"/>	66 Draytek Hotspot
<input type="radio"/>	67 portal.draytek.com
<input type="radio"/>	102 Floor_1

OK Cancel

Index: 1

Enable

Comment: Floor_1

Criteria

Protocol: Any

Source: IP Range

Start: 192.168.1.20 End: 192.168.1.30

Destination: Domain Name

-server1.draytek.com [Select] [Delete]

Add

Destination Port: Any

Send via if Criteria Matched

Click Add too add more domain names, we can set up to 5 domain names in one route policy.

Start: 192.168.1.20 End: 192.168.1.30

Destination: Domain Name

34 - portal.draytek.com [Select] [Delete]

-server2.draytek.com [Select] [Delete]

-server3.draytek.com [Select] [Delete]

-server4.draytek.com [Select] [Delete]

Add(up to 5)

Destination Port: Any

Send via if Criteria Matched

Auto-create String Objects

If you manually enter the domain name in a route policy, after clicking OK to apply the route policy, those domain names will be given a number.

Start: 192.168.1.20 End: 192.168.1.30

Destination: Domain Name

34	- portal.draytek.com	Select	Delete
103	- server2.draytek.com	Select	Delete
104	- server3.draytek.com	Select	Delete
105	- server4.draytek.com	Select	Delete

Add(up to 5)

Destination Port: Any

Send via if Criteria Matched

That means the router has automatically created string objects for those domain names, so that they can be used in other route policies or other functions.

Objects Setting >> String Object

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

Index	String	Clear
101		<input type="checkbox"/>
102	Floor_1	<input type="checkbox"/>
103	server2.draytek.com	<input type="checkbox"/>
104	server3.draytek.com	<input type="checkbox"/>
105	server4.draytek.com	<input type="checkbox"/>

[Add](#)

<< [1-10](#) | [11-20](#) | [21-30](#) | [31-40](#) | [41-50](#) | [51-60](#) | [61-70](#) | [71-80](#) | [81-90](#) | [91-100](#) | [101-105](#) >> << [Back](#)

Part III Wireless LAN



Wireless

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.

III-1 Wireless LAN

This function is used for “n / ac” models only.

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 Vigor2762 wireless series router (with “n” in model name) 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.

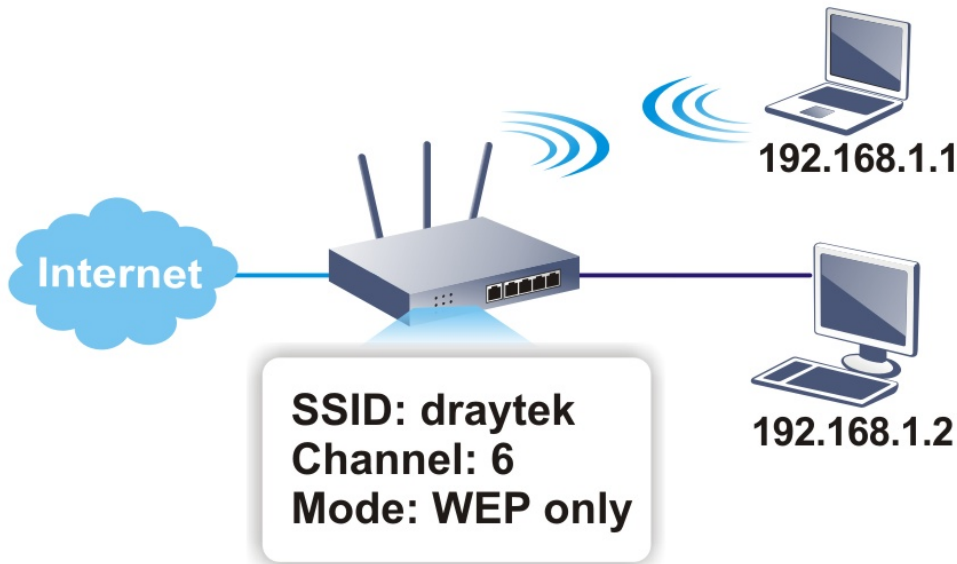
Vigor2762 wireless router is a highly integrated wireless local area network (WLAN) for 2.4 GHz 802.11n WLAN applications. Vigor2762 “n / ac” series router supports 802.11n up to 300 Mbps for 40 MHz channel operations.



Info

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.

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

It 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

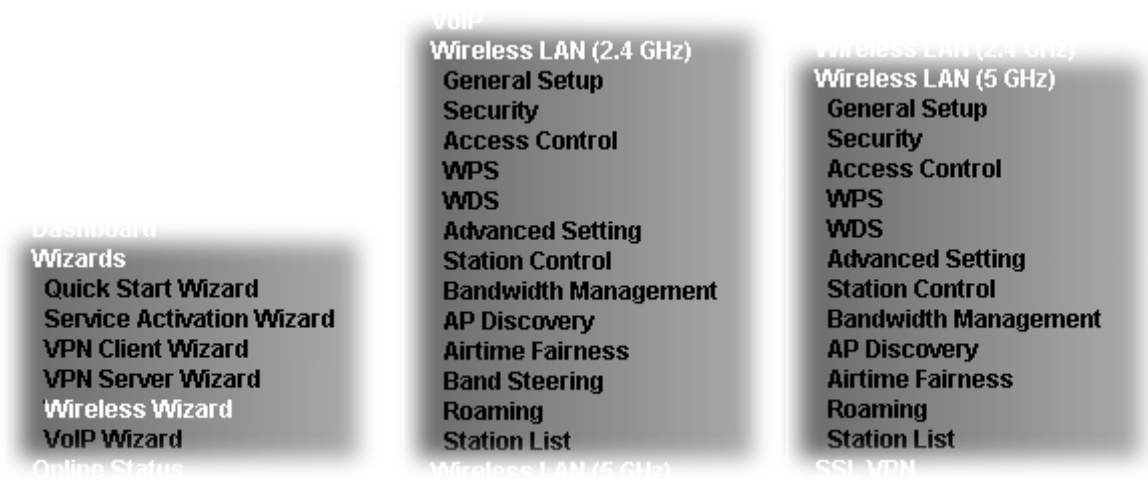
It will display all the stations in your wireless network and the status of their connection.

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.



Web User Interface



III-1-1 Wireless Wizard

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

Follow the steps listed below:

1. Open Wizards>>Wireless Wizard.
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

Wireless 2.4GHz Settings

Name:

Mode:

Channel:

Security Key:

Wireless 5GHz Settings

Use the same SSID and Security Key as above

Name:

Mode:

Channel:

Security Key:

Note:
The host AP configured here will be used for home or internal company use.

Available settings are explained as follows:

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

Name	Enter the SSID name of this router for wireless 2.4GHz. The default name is defined with DrayTek. Change the name if required.
Mode	Available modes are different based on 2.4GHz and / or 5GHz supported by Vigor router.
Channel	Means the channel of frequency of the wireless LAN. The default channel is 6 (for 2.4GHz) or 36 (for 5GHz). 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	The wireless mode offered by this wizard is WPA2/PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
Next	Click it to get into the next setting page.
Cancel	Exit the wireless wizard without saving any changes.

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

Wireless Wizard

Guest AP Configuration

Wireless 2.4GHz Settings

Enable Disable

SSID:

Security Key:

Bandwidth Limit: Enable Total Upload kbps Total Download kbps

Wireless 5GHz Settings

Enable Disable

Use the same SSID and Security Key as above

SSID:

Security Key:

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

Available settings are explained as follows:

Item	Description
Enable/Disable	Click it to enable or disable settings in this page.
SSID	Enter the SSID name of this router. (SSID1)
Security Key	The wireless mode offered by this wizard is WPA2/PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either 8~63 ASCII characters, such as 012345678(or 64

	Hexadecimal digits leading by 0x, such as "0x321253abcde...").
Bandwidth Limit	It controls the data transmission rate through wireless connection. Total Upload - Check Enable and Enter the transmitting rate for data upload. Default value is 30,000 kbps. Total Download - Enter the transmitting rate for data download. Default value is 30,000 kbps.
Use the same SSID and Security Key as above	Check the box to use the same settings configured above.
Next	Click it to get into the next setting page.
Cancel	Exit the wireless wizard without saving any changes.

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

Wireless Wizard

Configuration Summary

Wireless 2.4GHz Settings	Wireless 5GHz Settings
Mode: Mixed(11b+11g+11n) Channel: Channel 6, 2437MHz	Mode: Mixed (11a+11n+11ac) Channel: Channel 149, 5745MHz
Host AP SSID Name: DrayTek Security Key: 898988812	Host AP SSID Name: DrayTek_5G Security Key: 33322211132
Guest AP Status: Enabled SSID Name: DrayTek_Guest Security Key: 789456456 Bandwidth Limit: Disabled	Guest AP Status: Enabled SSID Name: DrayTek_5G_Guest Security Key: 963852741

6. Click Finish to complete the wireless settings configuration.

III-1-2 General Setup

By clicking the Wireless LAN>> 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(2.4GHz) >> General Setup

General Setting (IEEE 802.11)

Enable Wireless LAN

Radio

Mode: Mixed(11b+11g+11n) ▼

Channel: Channel 6, 2437MHz ▼

SSID

Index	Enable	SSID	Hide SSID	Isolate Member	Isolate VPN
1	<input checked="" type="checkbox"/>	DrayTek	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	DrayTek_Guest	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	Max: 31 characters	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	Max: 31 characters	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Schedule

Schedule Profile

Schedule 1: None ▼

Schedule 2: None ▼

Schedule 3: None ▼

Schedule 4: None ▼

Note:

1. Isolate Member: Prevent the clients associated with this SSID from accessing each other.
2. Isolate VPN: Block the wireless clients from accessing the VPN network and prevent wireless traffic being sent to VPN connections.
3. Only the action "Force Down" in the Schedule Profile will be applied to WLAN, other actions will be ignored.

OK
Cancel

Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Mode	<p>For 2.4GHz: At present, the router can connect to 11b Only, 11g Only, 11n Only(2.4 GHz), Mixed (11b+11g), Mixed (11g+11n), and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.</p> <p>For 5GHz: At present, the router can connect to 11a Only, 11n Only(5 GHz), Mixed (11a+11n), and Mixed (11a+11n+11ac) stations simultaneously. Simply choose Mixed (11a+11n+11ac) mode.</p> <p>In which, 802.11b/g operates on 2.4G band, 802.11a operates on 5G band, 802.11n operates on either 2.4G or 5G band, and 802.11ac operates on 5G band only.</p>
Channel	Means the channel of frequency of the wireless LAN. The default channel is 6 (for 2.4GHz) / 36 (for 5GHz). You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency,

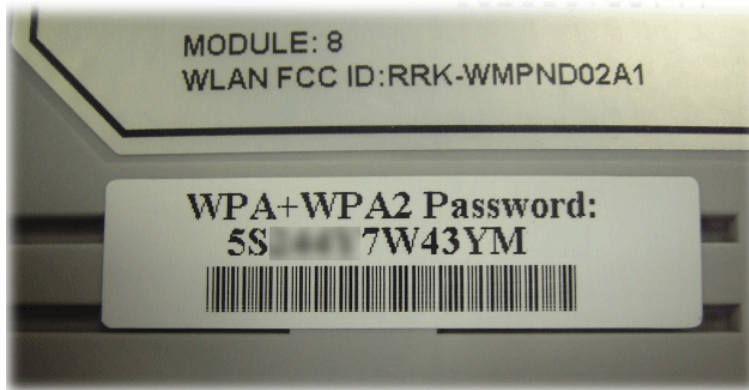
	please select Auto to let system determine for you.
SSID	Means the identification of the wireless LAN. SSID can be any text numbers or various special characters.
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity.
Isolate	Member -Check this box to make the wireless clients (stations) with the same SSID not accessing for each other. VPN - Check this box to make the wireless clients (stations) with different VPN not accessing for each other.
Schedule Profile	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.

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

III-1-3 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 password (PSK) of default security mode 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, a new web page will appear so that you could configure the settings of WPA and WEP.

Wireless LAN(2.4GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID			
DrayTek			
Mode:			
Mixed(WPA+WPA2)/PSK			
<u>WPA</u>			
Encryption Mode:			
TKIP for WPA/AES for WPA2			
Pre-Shared Key(PSK):			
●●●●●●●●●●			
Password Strength:			
<input type="button" value="Weak"/> <input type="button" value="Medium"/> <input type="button" value="Strong"/>			
EAPOL Key Retry:			
<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Note:			
Type 8~63 ASCII characters, for example: "cfgs01a2...".			
For strong passwords:			
1. Use at least 12 characters.			
2. Include at least 3 of the following 4 types of characters: digits, uppercase letters, lowercase letters, and non-alphanumeric characters (such as \$ % ^).			
<u>WEP</u>			
Encryption Mode:			
64-Bit			
<input checked="" type="radio"/> Key 1 :			
<input type="text"/>			
<input type="radio"/> Key 2 :			
<input type="text"/>			
<input type="radio"/> Key 3 :			
<input type="text"/>			
<input type="radio"/> Key 4 :			
<input type="text"/>			
Note:			
Please configure the RADIUS Server if 802.1X is used.			
For 64 bit WEP key configurations, please insert 5 ASCII characters, for example: "AB312".			
For 128 bit WEP key configurations, please insert 13 ASCII characters.			

Available settings are explained as follows:

Item	Description
Mode	<p>There are several modes provided for you to choose.</p> <p> Info You should also set RADIUS Server simultaneously if 802.1x mode is selected.</p> <p>Disable - Turn off the encryption mechanism.</p> <p>WEP-Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p>WEP/802.1x Only - Accepts only WEP clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.</p> <p>WPA/802.1x Only- Accepts only WPA clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.</p> <p>WPA2/802.1x Only- Accepts only WPA2 clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.</p> <p>Mixed (WPA+WPA2/802.1x only) - Accepts WPA and WPA2 clients simultaneously and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.</p> <p>WPA/PSK-Accepts only WPA clients and the encryption key should be entered in PSK.</p> <p>WPA2/PSK-Accepts only WPA2 clients and the encryption key should be entered in PSK.</p> <p>Mixed (WPA+ WPA2)/PSK - Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.</p>
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>Pre-Shared Key (PSK) - Either 8~63 ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").</p> <p>Password Strength - The system will display the password strength (represented with the word of weak, medium or strong) of the PSK specified above.</p> <p>EAPOL Key Retry - If enabled, EAPOL (Extensible Authentication Protocol over LAN) key will be tried for 3 times, in default.</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>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</p>

	can be entered in ASCII or Hexadecimal. Check the key you wish to use.
--	--

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

III-1-4 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(5GHz) >> 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(Limit: 64 entries)

Index	Attribute	MAC Address	Apply SSID	Comment

Client's MAC Address : : : : : :

Apply SSID : SSID 1 SSID 2 SSID 3 SSID 4

Attribute : s: Isolate the station from LAN

Comment :

Backup Access Control: Upload From File: 未選擇檔案

Note:

Support AP ACL configuration file restoration.

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.
Comment	Type a brief description for the specified client's MAC address.
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.
Backup Access Control	Settings on this web page can be saved as a file which can be restored in the future by this device or other device.
Upload From File	Restore wireless access control settings and applied onto this device.

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

III-1-5 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.



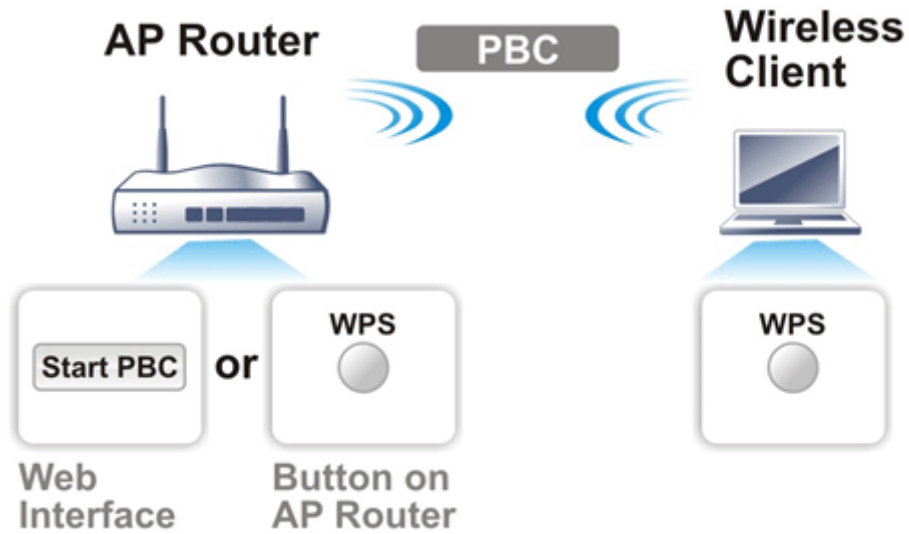
Info

WPS is available for the wireless station with WPS supported.

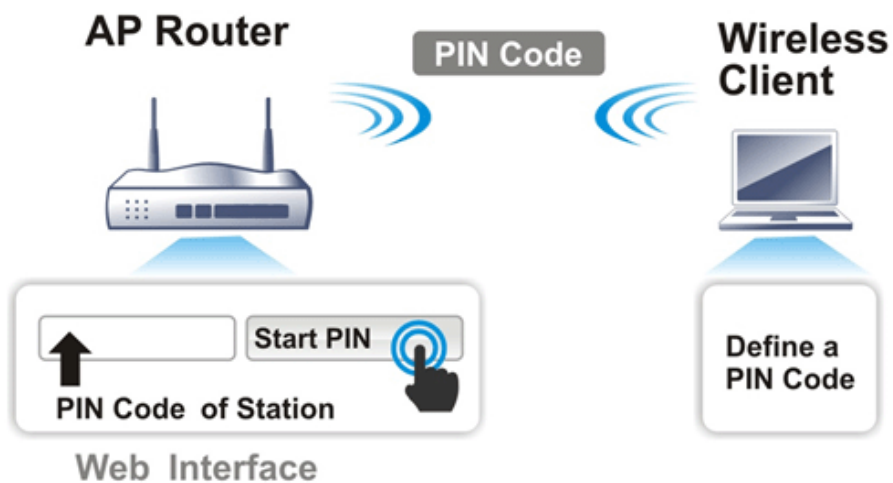
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for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

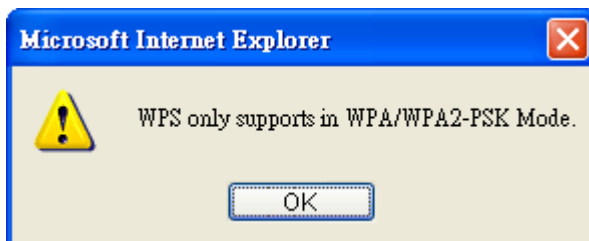
- On the side of Vigor 3220 series which served as an AP, press WPS button once on the front panel of the router or click Start PBC on web configuration interface. On the side of a station with network card installed, press Start PBC button of network card.



- 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(5GHz) >> WPS (Wi-Fi Protected Setup)

Enable WPS

Wi-Fi Protected Setup Information

WPS Status	Configured
SSID	DrayTek_5G
Authentication Mode	Mixed(WPA+WPA2)/PSK

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: Ready

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)

III-1-6 WDS

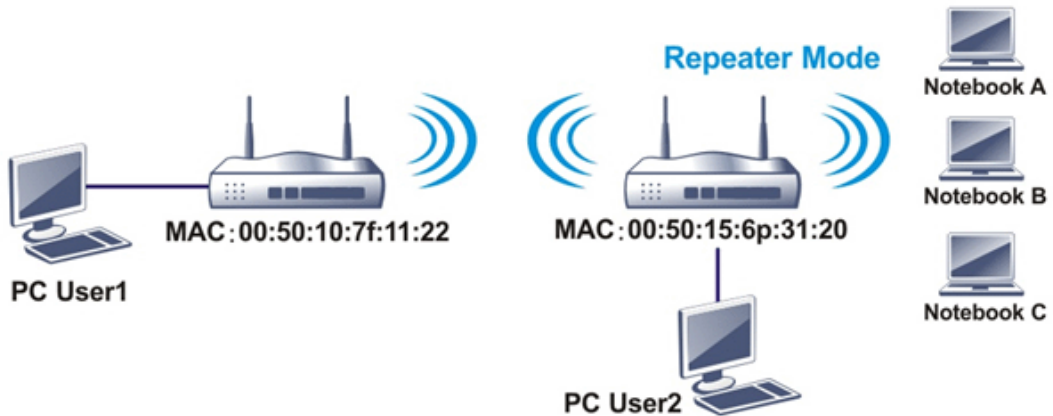
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

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

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

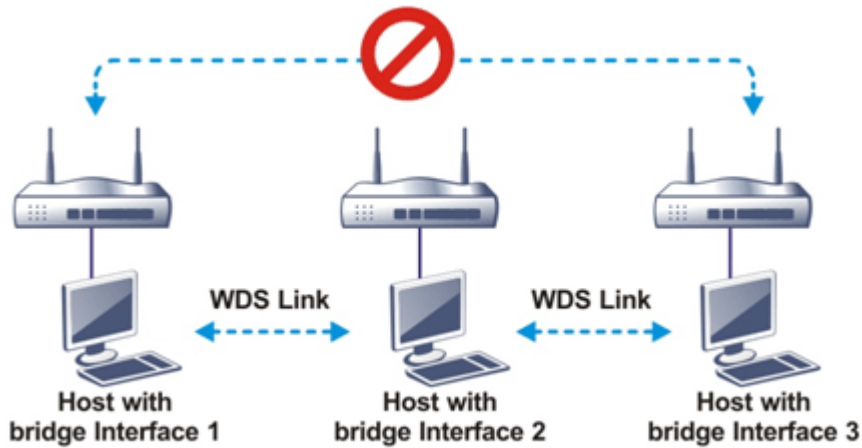


The application for the WDS-Repeater mode is depicted as below:



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

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



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

Wireless LAN(2.4GHz) >> WDS Settings

[Set to Factory Default](#)

WDS Settings

<p>Mode: Disable</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: <input style="width: 100%;" type="text" value="Max: 66 characters"/></p> <hr/> <p>Note:</p> <p>WPA and WPA2 are not compatible with DrayTek WPA.</p> <p>Type 8~63 ASCII characters, for example: "cfs01a2..."</p>	<p>Bridge</p> <p>Enable <input type="checkbox"/></p> <p>Peer MAC Address</p> <p><input type="text" value=" : : : : :"/></p> <p><input type="text" value=" : : : : :"/></p> <p><input type="text" value=" : : : : :"/></p> <p><input type="text" value=" : : : : :"/></p> <hr/> <p>Note:</p> <p>Disable unused links to get better performance.</p> <hr/> <p>Repeater</p> <p>Enable <input type="checkbox"/></p> <p>Peer MAC Address</p> <p><input type="text" value=" : : : : :"/></p> <p><input type="text" value=" : : : : :"/></p> <p><input type="text" value=" : : : : :"/></p> <p><input type="text" value=" : : : : :"/></p> <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> <hr/> <p>Note:</p> <p>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	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.
Security	There are three types for security, Disable, WEP and Pre-shared key. The setting you choose here will make the following WEP or Pre-shared key field valid or not. Choose one of the types for the router.
Pre-shared Key	Type - There are some types for you to choose. WPA and WPA2 are used for WDS devices (e.g.2920n wireless router, you can set the encryption mode as WPA or WPA2 to establish your WDS system between AP and the router. Key - Type 8 ~ 63 ASCII characters or 64 hexadecimal digits leading by "0x".
Bridge / Repeater	If you choose Repeater as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Similarly, if you want to invoke the peer MAC address, remember to check Enable box in the front of the MAC address after typing.
Access Point Function	Click Enable to make this router serve as an access point; click Disable to cancel this function.
Status	It allows user to send "hello" message to peers. Yet, it is valid only when the peer also supports this function.

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

III-1-7 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(2.4GHz) >> Advanced Setting

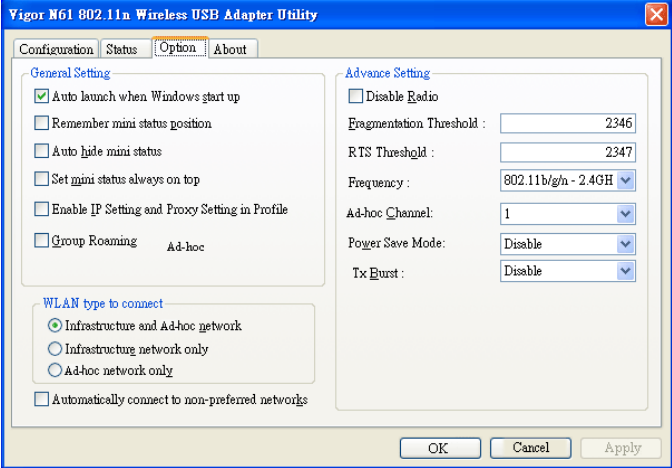

HT Physical Mode

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				
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				
Country Code	<input type="text"/>	(Reference)				

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 happen 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- Vigor Router will use 20Mhz for data transmission and receiving between the AP and the stations. 20/40 - Vigor Router will scan for nearby wireless AP, and then use 20MHz if the number of AP is more than 10, or use 40MHz if it's not. 40- Vigor Router will use 40Mhz for data transmission and receiving between the AP and the stations.
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

	<p>802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. Click Enable to use Long Preamble if needed to communicate with this kind of devices.</p>
<p>Packet-OVERDRIVE</p>	<p>This feature can enhance the performance in data transmission about 40%* more (by checking Tx Burst). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.</p> <p>Note: Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose Enable for TxBURST on the tab of Option).</p>  <p>Tx Burst : Disable Disable Enable</p> <p> Info * means the real transmission rate depends on the environment of the network.</p>
<p>Tx Power</p>	<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>
<p>WMM Capable</p>	<p>To apply WMM parameters for wireless data transmission, please click the Enable radio button.</p>
<p>APSD Capable</p>	<p>The default setting is Disable.</p>
<p>Rate Adaptation Algorithm</p>	<p>Wireless transmission rate is adapted dynamically. Usually, performance of “new” algorithm is better than “old”.</p>
<p>Fragment Length (256 - 2346)</p>	<p>Set the Fragment threshold. Do not modify default value if you don't know what it is, default value is 2346.</p>
<p>RTS Threshold (1 - 2347)</p>	<p>Minimize the collision (unit is bytes) between hidden stations to improve wireless performance.</p> <p>Set the RTS threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2347.</p>

Country Code	Vigor router broadcasts country codes by following the 802.11d standard. However, some wireless stations will detect / scan the country code to prevent conflict occurred. If conflict is detected, wireless station will be warned and is unable to make network connection. Therefore, changing the country code to ensure successful network connection will be necessary for some clients.
--------------	--

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

III-1-8 Station Control

Station Control is used to specify the duration for the wireless client to connect and reconnect Vigor router. If such function is not enabled, the wireless client can connect Vigor router until the router shuts down.

Such feature is especially useful for free Wi-Fi service. For example, a coffee shop offers free Wi-Fi service for its guests for one hour every day. Then, the connection time can be set as “1 hour” and reconnection time can be set as “1 day”. Thus, the guest can finish his job within one hour and will not occupy the wireless network for a long time.

Wireless LAN(5GHz) >> Station Control

SSID 1	SSID 2	SSID 3	SSID 4
SSID	DrayTek_5G		
Enable	<input type="checkbox"/>		
Connection Time	1 hour		
Reconnection Time	1 day		
Display All Station Control List			
Hotspot Web Portal			

Note:

Once the feature is enabled, the connection time quota will apply to each wireless client (identified by MAC address).

OK Cancel

Available settings are explained as follows:

Item	Description
SSID	Display the SSID that the wireless station will use it to connect with Vigor router.
Enable	Check the box to enable the station control function.
Connection Time / Reconnection Time	Use the drop down list to choose the duration for the wireless client connecting /reconnecting to Vigor router. Or, Enter the duration manually when you choose User defined.
Display All Station Control List	All the wireless stations connecting to Vigor router by using such SSID will be listed on Station Control List.
Hotspot Web Portal	Click it to access into Hotspot Web Portal page for modifying the settings if required.

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

III-1-9 Bandwidth Management

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 Bandwidth Management to make the bandwidth usage more efficient.

Wireless LAN(5GHz) >> Bandwidth Management

SSID 1	SSID 2	SSID 3	SSID 4
SSID:	DrayTek_5G		
Enable	<input checked="" type="checkbox"/>		
Bandwidth Limit Type	Auto Adjustment ▾		
Total Upload Limit(Kbps)	<input type="text" value="30000"/>		
Total Download Limit(Kbps)	<input type="text" value="30000"/>		

Note:

1. Download: Traffic going to any station.Upload: Traffic being sent from a wireless station.
2. Allow auto adjustment could make the best utilization of available bandwidth.

Available settings are explained as follows:

Item	Description
SSID	Display the specific SSID name.
Enable	Check this box to enable the bandwidth management for clients.
Bandwidth Limit Type	Auto Adjustment - Bandwidth limit is determined by the system automatically. Per Station Limit - Bandwidth limit is determined according to the limitation of the wireless client.
Total Upload Limit	It is available when Auto Adjustment is selected. Type a value to define the maximum data traffic (uploading) for all of the wireless clients connecting to Vigor2762.
Total Download Limit	It is available when Auto Adjustment is selected. Type a value to define the maximum data clientstations connecting to Vigor2762.
Upload Limit	It is available when Per Station Limit is selected. Type a value to define the maximum data traffic (uploading) for each wireless client connecting to Vigor2762.
Download Limit	It is available when Per Station Limit is selected Type a value to define the maximum data traffic (downloading) for each wireless client connecting to Vigor2762.

After finishing this web page configuration, please click OK to save the settings

III-1-10 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(2.4GHz) >> Access Point Discovery

Access Point List

Index	BSSID	Channel	RSSI	SSID	Authentication

See [Statistics](#).

Add to WDS Settings :

AP's MAC address : : : : :

Bridge Repeater

Note:

1. During the scanning process (~5 seconds), no station is allowed to connect with the router.
2. AP Discovery can only support up to 32 APs displayed on the screen.

Available settings are explained as follows:

Item	Description																													
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button.																													
Statistics	It displays the statistics for the channels used by APs. <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <p style="font-size: small;">Wireless LAN >> Site Survey Statistics</p> <hr/> <p style="font-size: x-small;">Recommended channels for usage: 1 2 3 4 5 6 7 8 9 10 11 12 13</p> <div style="border: 1px solid black; padding: 5px; margin: 5px auto; width: fit-content;"> <p style="font-size: x-small; text-align: center;">AP number v.s. Channel</p> <table style="width: 100%; text-align: center; border-collapse: collapse;"> <tr> <td style="border: 1px solid black; width: 20px; height: 20px;"></td> <td style="border: 1px solid black; width: 20px; height: 20px;"></td> <td style="border: 1px solid black; width: 20px; height: 20px;"></td> <td style="border: 1px solid black; width: 20px; height: 20px;"></td> <td style="border: 1px solid black; width: 20px; height: 20px;"></td> <td style="border: 1px solid black; width: 20px; height: 20px;"></td> <td style="border: 1px solid black; width: 20px; height: 20px;"></td> <td style="border: 1px solid black; width: 20px; height: 20px;"></td> <td style="border: 1px solid black; width: 20px; height: 20px;"></td> <td style="border: 1px solid black; width: 20px; height: 20px;"></td> <td style="border: 1px solid black; width: 20px; height: 20px;"></td> <td style="border: 1px solid black; width: 20px; height: 20px;"></td> <td style="border: 1px solid black; width: 20px; height: 20px;"></td> <td style="border: 1px solid black; width: 20px; height: 20px;"></td> <td style="border: 1px solid black; width: 20px; height: 20px;"></td> </tr> <tr> <td style="font-size: x-small;">1</td> <td style="font-size: x-small;">2</td> <td style="font-size: x-small;">3</td> <td style="font-size: x-small;">4</td> <td style="font-size: x-small;">5</td> <td style="font-size: x-small;">6</td> <td style="font-size: x-small;">7</td> <td style="font-size: x-small;">8</td> <td style="font-size: x-small;">9</td> <td style="font-size: x-small;">10</td> <td style="font-size: x-small;">11</td> <td style="font-size: x-small;">12</td> <td style="font-size: x-small;">13</td> <td style="font-size: x-small;">14</td> </tr> </table> <p style="font-size: x-small; text-align: center;">Channel</p> <p style="text-align: center;"><input type="button" value="Cancel"/></p> </div> </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	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.																													

III-1-11 Airtime Fairness

Airtime fairness is essential in wireless networks that must support critical enterprise applications.

Most of the applications are either symmetric or require more downlink than uplink capacity; telephony and email send the same amount of data in each direction, while video streaming and web surfing involve more traffic sent from access points to clients than the other way around. This is essential for ensuring predictable performance and quality-of-service, as well as allowing 802.11n and legacy clients to coexist on the same network. Without airtime fairness, offices using mixed mode networks risk having legacy clients slow down the entire network or letting the fastest client(s) crowd out other users.

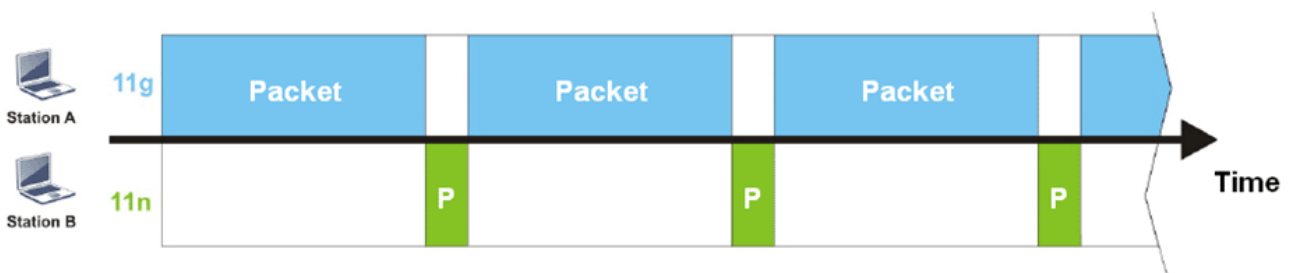
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

The wireless channel can be accessed by only one wireless station at the same time.

The principle behind the IEEE802.11 channel access mechanisms is that each station has *equal probability* to access the channel. When wireless stations have similar data rate, this principle leads to a fair result. In this case, stations get similar channel access time which is called airtime.

However, when stations have various data rate (e.g., 11g, 11n), the result is not fair. The slow stations (11g) work in their slow data rate and occupy too much airtime, whereas the fast stations (11n) become much slower.

Take the following figure as an example, both Station A(11g) and Station B(11n) transmit data packets through Vigor router. Although they have equal probability to access the wireless channel, Station B(11n) gets only a little airtime and waits too much because Station A(11g) spends longer time to send one packet. In other words, Station B(fast rate) is obstructed by Station A(slow rate).



To improve this problem, Airtime Fairness is added for Vigor router. Airtime Fairness function tries to assign *similar airtime* to each station (A/B) by controlling TX traffic. In the following figure, Station B(11n) has higher probability to send data packets than Station A(11g). By this way, Station B(fast rate) gets fair airtime and it's speed is not limited by Station A(slow rate).



It is similar to automatic Bandwidth Limit. The dynamic bandwidth limit of each station depends on instant active station number and airtime assignment. Please note that Airtime Fairness of 2.4GHz and 5GHz are independent. But stations of different SSIDs function together, because they all use the same wireless channel. IN SPECIFIC ENVIRONMENTS, this function can reduce the bad influence of slow wireless devices and improve the overall wireless performance.

Suitable environment:

- (1) Many wireless stations.
- (2) All stations mainly use download traffic.
- (3) The performance bottleneck is wireless connection.

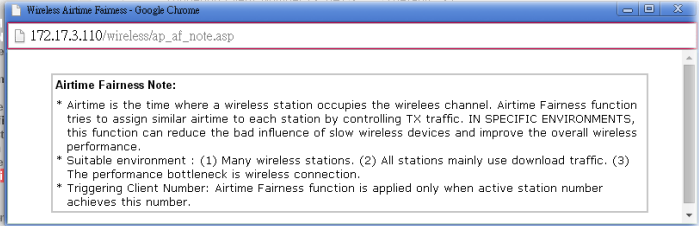
Wireless LAN(5GHz) >> Airtime Fairness

Enable **Airtime Fairness**
 Triggering Client Number (2 ~ 64) (Default: 2)

Note:

Please enable or disable this function according to the real situation and user experience. It is NOT suitable for all environments.

Available settings are explained as follows:

Item	Description
Enable Airtime Fairness	<p>Try to assign similar airtime to each wireless station by controlling TX traffic.</p> <p>Airtime Fairness - Click the link to display the following screen of airtime fairness note.</p>  <p>Triggering Client Number -Airtime Fairness function is applied only when active station number achieves this number.</p>

After finishing this web page configuration, please click OK to save the settings.

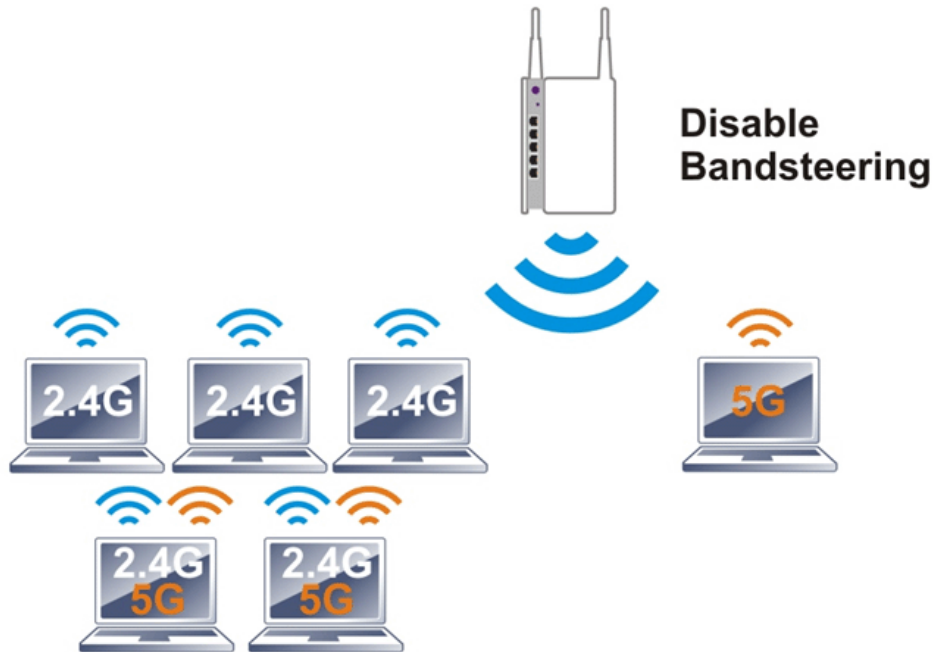


Info

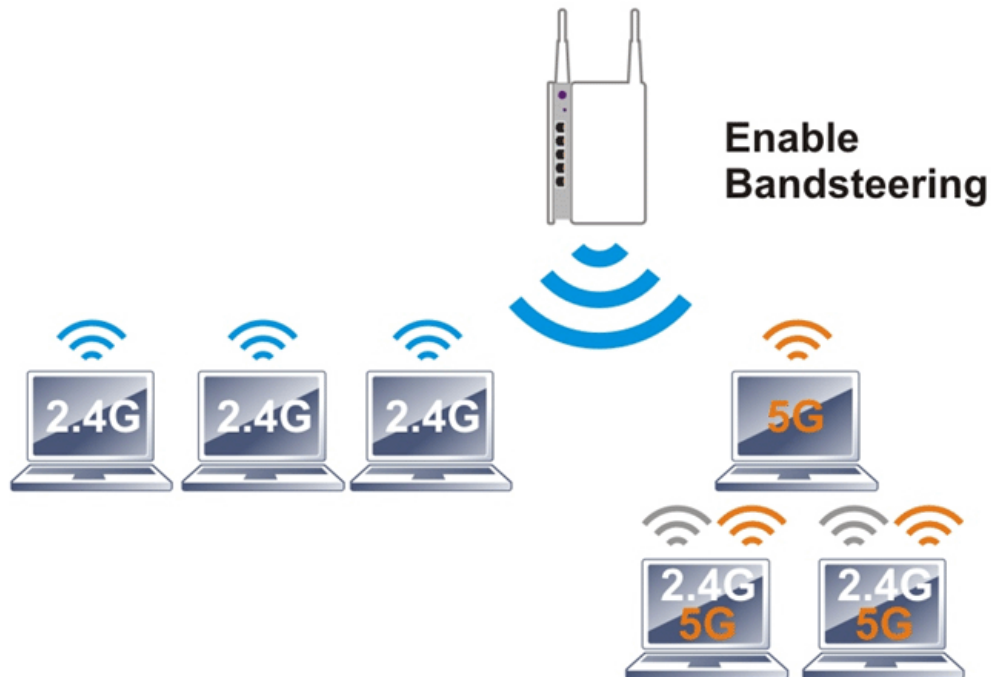
Airtime Fairness function and Bandwidth Limit function should be mutually exclusive. So their webs have extra actions to ensure these two functions are not enabled simultaneously.

III-1-12 Band Steering

Band Steering detects if the wireless clients are capable of 5GHz operation, and steers them to that frequency. It helps to leave 2.4GHz band available for legacy clients, and improves users experience by reducing channel utilization.



If dual-band is detected, the AP will let the wireless client connect to less congested wireless LAN, such as 5GHz to prevent from network congestion.



Info

To make Band Steering work successfully, SSID and security on 2.4GHz also

MUST be broadcasted on 5GHz.

Open Wireless LAN (2.4GHz)>>Band Steering to get the following web page:

Wireless LAN(2.4GHz) >> Band Steering

<input type="checkbox"/> Enable Band Steering Check Time for WLAN Client 5G Capability <input type="text" value="15"/> second(s) (1 ~ 60) (Default: 15)

Note:

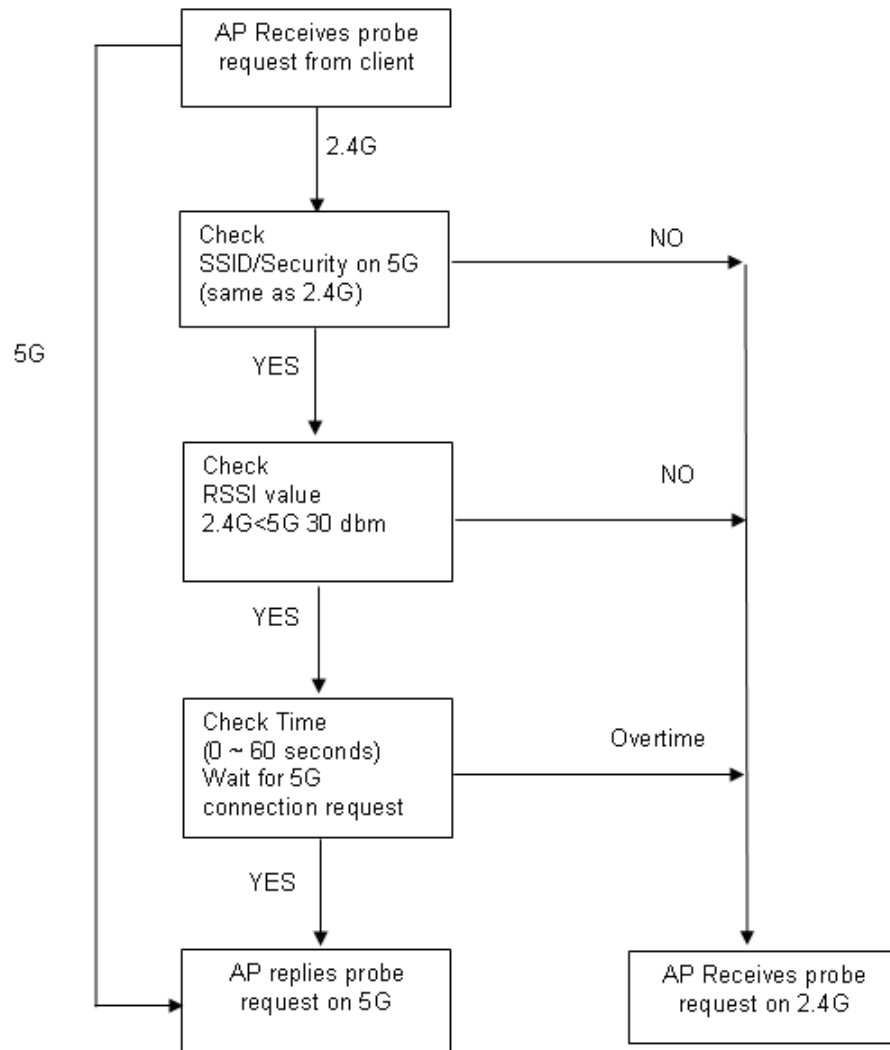
Please setup at least one pair of 2.4GHz and 5GHz Wireless LAN with the same SSID and security.

Available settings are explained as follows:

Item	Description
Enable Band Steering	If it is enabled, Vigor router will detect if the wireless client is capable of dual-band or not within the time limit. Check Time.... - If the wireless station does not have the capability of 5GHz network connection, the system shall wait and check for several seconds (15 seconds, in default) to make the 2.4GHz network connection. Specify the time limit for Vigor router to detect the wireless client.

After finishing this web page configuration, please click OK to save the settings.

Below shows how Band Steering works.



How to Use Band Steering?

1. Open Wireless LAN(2.4GHz)>>Band Steering.
2. Check the box of Enable Band Steering and use the default value (15) for check time setting.

Wireless LAN(2.4GHz) >> Band Steering

<input type="checkbox"/> Enable Band Steering Check Time for WLAN Client 5G Capability <input type="text" value="15"/> second(s) (1 ~ 60) (Default: 15)

Note:

Please setup at least one pair of 2.4GHz and 5GHz Wireless LAN with the same SSID and security.

3. Click OK to save the settings.

- Open Wireless LAN (2.4GHz)>>General Setup and Wireless LAN (5GHz)>> General Setup. Configure SSID as *DrayTek2762_BandSteering* for both pages. Click OK to save the settings.

Wireless LAN(2.4GHz) >> General Setup

General Setting (IEEE 802.11)

Enable Wireless LAN

Radio

Mode: ▼

Channel: ▼

SSID

Index	Enable	SSID	Hide SSID	Isolate Member	Isolate VPN
1	<input checked="" type="checkbox"/>	<input type="text" value="DrayTek2762_BandSteering"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="text" value="DrayTek_Guest"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="text" value="Max: 31 characters"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="text" value="Max: 31 characters"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Same value for 2.4GHz and 5GHz

Wireless LAN(5GHz) >> General Setup

General Setting (IEEE 802.11)

Enable Wireless LAN

Radio

Mode: ▼

Channel: ▼

SSID

Index	Enable	SSID	Hide SSID	Isolate Member	Isolate VPN
1	<input checked="" type="checkbox"/>	<input type="text" value="DrayTek2762_BandSteering"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="text" value="DrayTek_5G_Guest"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="text" value="Max: 31 characters"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="text" value="Max: 31 characters"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Schedule

- Open Wireless LAN (2.4GHz)>>Security and Wireless LAN (5GHz)>>Security. Configure Security as 12345678 for both pages. Click OK to save the settings.

Wireless LAN(2.4GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
Mode: Mixed(WPA+WPA2)/PSK			
<u>WPA</u>			
Encryption Mode: TKIP for WPA/AES for WPA2			
Pre-Shared Key(PSK): *****			
Password Strength: Weak Medium Strong			
Strong password requirements: <ol style="list-style-type: none"> Have at least 7 characters, including numbers and letters. Have at least one upper-case letter and one lower-case letter. Including non-alphanumeric characters is a plus. Type 8~63 ASCII character or 64 Hexadecimal digits leading by "0x", for example "cfigs01a2..." or "0x655abcd....".			
<u>WEP</u>			
Encryption Mode: 64-Bit			
<input checked="" type="radio"/> Key 1 : *****			
<input type="radio"/> Key 2 : *****			
<input type="radio"/> Key 3 : *****			

Same value for 2.4GHz and 5GHz

Wireless LAN(5GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
Mode: Mixed(WPA+WPA2)/PSK			
<u>WPA</u>			
Encryption Mode: TKIP for WPA/AES for WPA2			
Pre-Shared Key(PSK): *****			
Password Strength: Weak Medium Strong			
Strong password requirements: <ol style="list-style-type: none"> Have at least 7 characters, including numbers and letters. Have at least one upper-case letter and one lower-case letter. Including non-alphanumeric characters is a plus. Type 8~63 ASCII character or 64 Hexadecimal digits leading by "0x", for example "cfigs01a2..." or "0x655abcd....".			
<u>WEP</u>			
Encryption Mode: 64-Bit			
<input checked="" type="radio"/> Key 1 : *****			
<input type="radio"/> Key 2 : *****			
<input type="radio"/> Key 3 : *****			

- Now, Vigor router will let the wireless clients connect to less congested wireless LAN, such as 5GHz to prevent from network congestion.

III-1-13 Roaming

The network signal for a single wireless access point might be limited by its coverage range. Therefore, if you want to expand the wireless network in a large exhibition with a quick method, you can install multiple access points with enabling the Roaming feature for each AP to reach the purpose of expanding wireless signals seamlessly.

These access points connecting for each other shall be verified by pre-authentication. This page allows you to enable the roaming feature and the pre-authentication.

Wireless LAN(2.4GHz) >> Roaming

Router-assisted Client Roaming Parameters

<input checked="" type="radio"/> Disable RSSI Requirement			
<input type="radio"/> Strictly Minimum RSSI	-73	dBm (42 %)	(Default: -73)
<input type="radio"/> Minimum RSSI	-66	dBm (60 %)	(Default: -66)
with Adjacent AP RSSI over	5	dB	(Default: 5)

Available settings are explained as follows:

Item	Description
Disable RSSI Requirement	When the link rate of wireless station is too low or the signal received by the wireless station is too worse, Vigor router will automatically detect (based on the link rate and RSSI requirement) and cut off the network connection for that wireless station to assist it to connect another Wireless AP to get better signal. This option is to disable the roaming mechanism.
Strictly Minimum RSSI	Vigor router uses RSSI (received signal strength indicator) to decide to terminate the network connection of wireless station. When the signal strength is below the value (dBm) set here, Vigor router will terminate the network connection for that wireless station.
Minimum RSSI	Minimum RSSI - When the signal strength of the wireless station is below the value (dBm) set here and adjacent AP (must be DrayTek AP and support such feature too) with higher signal strength value (defined in the field of With Adjacent AP RSSI over) is detected by Vigor router, Vigor router will terminate the network connection for that wireless station. Later, the wireless station can connect to the adjacent AP (with better RSSI). <ul style="list-style-type: none"> With Adjacent AP RSSI over - Specify a value as a threshold.

After finishing this web page configuration, please click OK to save the settings.

III-1-14 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(5GHz) >> Station List

Station List

Station List				
General				
Advanced				
Neighbor				
Index	Status	IP Address	MAC Address	Associated with
<input type="button" value="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.				
<hr/>				
Add to Access Control :				
Client's MAC address <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>				

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.

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.

This page is left blank.

Part IV VoIP



VoIP

Voice over IP network (VoIP) enables you to use your broadband Internet connection to make toll quality voice calls over the Internet.

IV-1 VoIP

Voice over IP network (VoIP) enables you to use your broadband Internet connection to make toll quality voice calls over the Internet.



Info

This function is used for “V” models.

There are many different call signaling protocols, methods by which VoIP devices can talk to each other. The most popular protocols are SIP, MGCP, Megaco and H.323. These protocols are not all compatible with each other (except via a soft-switch server).

The Vigor V models support the SIP protocol as this is an ideal and convenient deployment for the ITSP (Internet Telephony Service Provider) and softphone and is widely supported. SIP is an end-to-end, signaling protocol that establishes user presence and mobility in VoIP structure. Every one who wants to talk using his/her SIP Uniform Resource Identifier, “SIP Address”. The standard format of SIP URI is

`sip: user:password @ host: port`

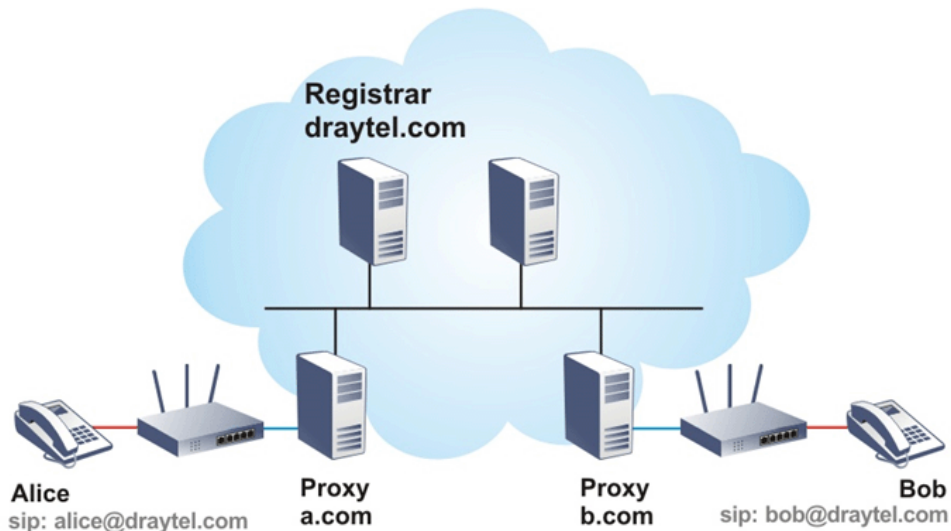
Some fields may be optional in different use. In general, “host” refers to a domain. The “userinfo” includes the user field, the password field and the @ sign following them. This is very similar to a URL so some may call it “SIP URL”. SIP supports peer-to-peer direct calling and also calling via a SIP proxy server (a role similar to the gatekeeper in H.323 networks), while the MGCP protocol uses client-server architecture, the calling scenario being very similar to the current PSTN network.

After a call is setup, the voice streams transmit via RTP (Real-Time Transport Protocol). Different codecs (methods to compress and encode the voice) can be embedded into RTP packets. Vigor V models provide various codecs, including G.711 A/ μ -law, G.723, G.726 and G.729 A & B. Each codec uses a different bandwidth and hence provides different levels of voice quality. The more bandwidth a codec uses the better the voice quality, however the codec used must be appropriate for your Internet bandwidth.

Calling via SIP Servers

First, the Vigor V models of yours will have to register to a SIP Registrar by sending registration messages to validate. Then, both parties’ SIP proxies will forward the sequence of messages to caller to establish the session.

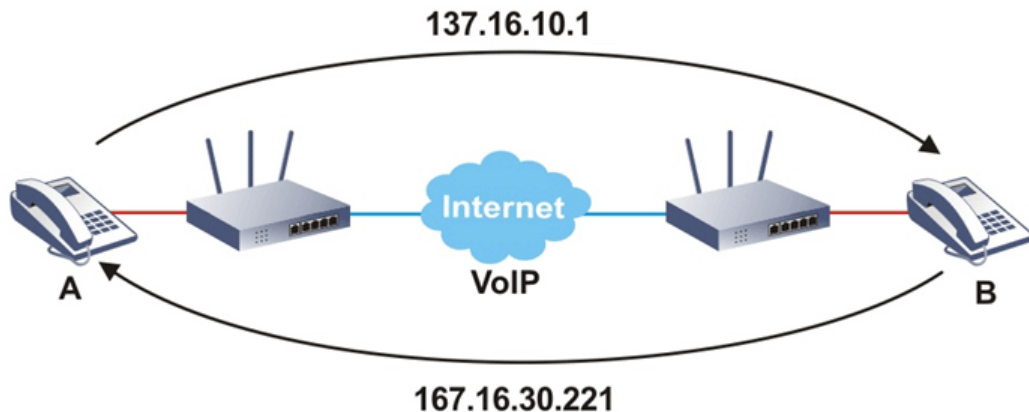
If you both register to the same SIP Registrar, then it will be illustrated as below:



The major benefit of this mode is that you don't have to memorize your friend's IP address, which might change very frequently if it's dynamic. Instead of that, you will only have to use dial plan or directly dial your friend's account name if you are with the same SIP Registrar.

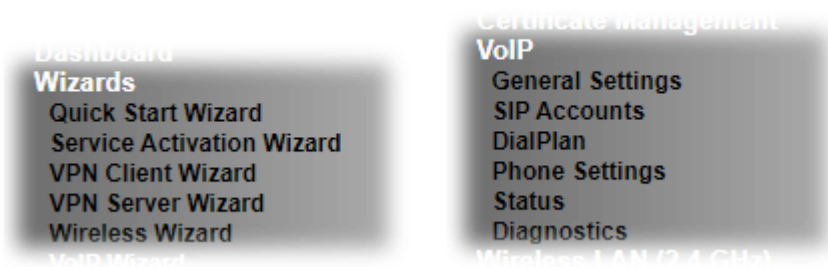
Peer-to-Peer

Before calling, you have to know your friend's IP Address. The Vigor VoIP Routers will build connection between each other.



Vigor V models firstly apply efficient codecs designed to make the best use of available bandwidth, but Vigor V models also equip with automatic QoS assurance. QoS Assurance assists to assign high priority to voice traffic via Internet. You will always have the required inbound and outbound bandwidth that is prioritized exclusively for Voice traffic over Internet but you just get your data a little slower and it is tolerable for data traffic.

Web User Interface



IV-1-1 VoIP Wizard

Vigor router offers a quick method to configure settings for VoIP application. Follow the steps listed below.



Info

This wizard is available for “V” model only.

1. Open Wizards>>VoIP Wizard.
2. The screen of VoIP Wizard will be shown as follows.

VoIP Wizard

Set VoIP service provider domain

VoIP service provider	draytel.org ▼	draytel.org	(63 char max).
SIP Port	5060		

Set Account quickly

Phone 1 (default mapping to Account 1)			
Account Number/Name	---		(63 char max).
Password			(127 char max).
Phone 2 (default mapping to Account 2)			
<input checked="" type="checkbox"/> use the same Account as phone1			
Account Number/Name	---		(63 char max).
Password			(127 char max).

Available settings are explained as follows:

Item	Description
Set VoIP service provider domain	VoIP service provider - Use the drop down list to choose the ISP which offers the VoIP service for your router. SIP Port - Use the default setting (5060).
Set Account quickly	Account Number/Name - Enter the account number/name registered to your ISP. Password - Enter the password for the account registered to your ISP.

	Use the same Account as phone 1 - If you don't need to configure Phone 2 settings, simply check this box.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the VoIP wizard.

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

VoIP Wizard

Please confirm your settings:

VoIP Service Provider	draytel.org
SIP Port	5060
Phone 1 Account	5633s
Phone 2 Account	5633s

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save current settings.

4. Click Finish. A page of VoIP Wizard Setup OK!!! will appear.

VoIP Wizard Setup OK!

IV-1-2 General Settings

Open VoIP>>General Settings.



The following page will appear. Check the box of Enable VoIP and click OK to open the configuration page. If not, no settings will be displayed.

VoIP >> General Settings

Enable VoIP

Note:
 If VoIP is disabled, there will be no power supplied to the FXS ports.

OK

After checking the box and click OK, the following page appears for you to configure secure phone, IP call; and set NAT Traversal Setting, RTP for the VoIP function.

VoIP >> General Settings

Enable VoIP

Note:
 If VoIP is disabled, there will be no power supplied to the FXS ports.

Secure Phone

 Enable Secure Phone (ZRTP+SRTP)
 Enable SAS Voice Prompt

NAT Traversal Setting

STUN Server

External IP

SIP PING Interval sec

RTP

 Symmetric RTP

Dynamic RTP Port Start

Dynamic RTP Port End

RTP TOS

IP Call

 Enable IP Call

OK

Available settings are explained as follows:

Item	Description
Secure Phone	Enable Secure Phone - It allows users to have encrypted RTP stream with the peer side using the same protocol

	(ZRTP+SRTP). Check this box to have secure call. Enable SAS Voice Prompt - If it is enabled, SAS prompt will be heard for both ends every time. If it is disabled, no SAS prompt will be heard any more.
NAT Traversal Setting	STUN Server - Type in the IP address or domain of the STUN server. External IP - Type in the gateway IP address. SIP PING interval - The default value is 150 (sec). It is useful for a Nortel server NAT Traversal Support.
RTP	Symmetric RTP - Check this box to invoke the function. To make the data transmission going through on both ends of local router and remote router not misleading due to IP lost (for example, sending data from the public IP of remote router to the private IP of local router), you can check this box to solve this problem. Dynamic RTP Port Start - Specifies the start port for RTP stream. The default value is 10050. Dynamic RTP Port End - Specifies the end port for RTP stream. The default value is 15000. RTP TOS - It decides the level of VoIP package. Use the drop down list to choose any one of them.
IP Call	Enable IP Call - It allows that a user could dial outgoing IP Calls; and Vigor router could receive the incoming IP Calls.

Application for Secure Phone

Enable SAS Voice Prompt, for ex: if vigor router A calls vigor router B with checking Enable Secure Phone and Enable SAS Voice Prompt, then:

1. After the connection established, vigor router A will send SAS voice prompt to A and vigor router B will send the SAS voice prompt to B.
2. Then the RTP traffic is secured until the call ends.
3. If vigor router A wants to call vigor router B again next time, both A and B will not hear any voice prompt again even checking Enable SAS Voice Prompt on web UI. It means only the first call between them will have voice prompt.

Enable SAS Voice Prompt, for ex: if vigor router A calls vigor router B with checking Enable Secure Phone but not Enable SAS Voice Prompt, then:

1. After the connection established, vigor router A will NOT send SAS voice prompt to vigor router A and vigor router B will NOT send the SAS voice prompt to vigor router B.
2. Even no voice prompt, but the RTP traffic is still secured until the call ends.

Info

If the incoming or outgoing calls do not match any entry on the phonebook, the router will try to make the call "being protected". But, if the call ends up "unprotected"(e.g. peer side does not support ZRTP+SRTP), the router will not play out a warning message.

IV-1-3 SIP Accounts

In this section, you set up your own SIP settings. When you apply for an account, your SIP service provider will give you an Account Name or user name, SIP Registrar, Proxy, and Domain name. (The last three might be the same in some case). Then you can tell your folks your SIP Address as in Account Name@ Domain name

As Vigor VoIP Router is turned on, it will first register with Registrar using AuthorizationUser@Domain/Realm. After that, your call will be bypassed by SIP Proxy to the destination using AccountName@Domain/Realm as identity.



Info

Selection items for Ring Port will differ according to the router you have.

VoIP >> SIP Accounts



SIP Accounts List

Refresh

Index	Profile	Domain/Realm	Proxy	Account Name	Codec	Ring Port	Status
1				---	G.729A/B	<input type="checkbox"/> Phone1 <input type="checkbox"/> Phone2	-
2				---	G.729A/B	<input type="checkbox"/> Phone1 <input type="checkbox"/> Phone2	-
3				---	G.729A/B	<input type="checkbox"/> Phone1 <input type="checkbox"/> Phone2	-
4				---	G.729A/B	<input type="checkbox"/> Phone1 <input type="checkbox"/> Phone2	-
5				---	G.729A/B	<input type="checkbox"/> Phone1 <input type="checkbox"/> Phone2	-
6				---	G.729A/B	<input type="checkbox"/> Phone1 <input type="checkbox"/> Phone2	-
7				---	G.729A/B	<input type="checkbox"/> Phone1 <input type="checkbox"/> Phone2	-
8				---	G.729A/B	<input type="checkbox"/> Phone1 <input type="checkbox"/> Phone2	-
9				---	G.729A/B	<input type="checkbox"/> Phone1 <input type="checkbox"/> Phone2	-
10				---	G.729A/B	<input type="checkbox"/> Phone1 <input type="checkbox"/> Phone2	-
11				---	G.729A/B	<input type="checkbox"/> Phone1 <input type="checkbox"/> Phone2	-
12				---	G.729A/B	<input type="checkbox"/> Phone1 <input type="checkbox"/> Phone2	-

R: success registered on SIP server
-: fail to register on SIP server

[Alias List](#)

OK

Available settings are explained as follows:

Item	Description
Index	Click this link to access into next page for setting SIP account.
Profile	Display the profile name of the account.
Domain/Realm	Display the domain name or IP address of the SIP registrar server.
Proxy	Display the domain name or IP address of the SIP proxy server.
Account Name	Display the account name of SIP address before @.
Codec	Display the codec type for the account.
Ring Port	Specify which port will ring when receiving a phone call.
Status	Show the status for the corresponding SIP account. R means

such account is registered on SIP server successfully. - means the account is failed to register on SIP server.

Click any index link to access into the following page for configuring SIP account.

VoIP >> SIP Accounts

SIP Account Index No. 1

Profile Name	<input type="text"/> (11 char max.)
Register via	None <input type="checkbox"/> Call without Registration
SIP Port	5060
Domain/Realm	Max: 255 characters
Proxy	Max: 255 characters
<input type="checkbox"/> Act as outbound proxy	
Display Name	Max: 23 characters
Account Number/Name	---
<input type="checkbox"/> Authentication ID	Max: 63 characters
Password	Max: 127 characters
Expiry Time	1 hour <input type="text"/> 3600 sec
NAT Traversal Support	None
Mapping to Alias List	None
Call Forwarding	Disable
SIP URL	<input type="text"/>
Time Out	30 sec
Ring Port	<input type="checkbox"/> Phone1 <input type="checkbox"/> Phone2
Ring Pattern	1
Prefer Codec	G.729A/B (8Kbps) <input type="checkbox"/> Single Codec
Packet Size	20ms
Voice Active Detector	Off

OK Cancel Clear

Available settings are explained as follows:

Item	Description
Profile Name	Assign a name for this profile for identifying. You can type similar name with the domain. For example, if the domain name is <i>draytel.org</i> , then you might set <i>draytel-1</i> in this field.
Register via	If you want to make VoIP call without register personal information, please choose None and check the box to achieve the goal. Some SIP server allows user to use VoIP function without registering. For such server, please check the box of Call without Registration. Choosing Auto is recommended. The system will select a proper way for your VoIP call.
SIP Port	Set the port number for sending/receiving SIP message for building a session. The default value is 5060. Your peer must set the same value in his/her Registrar.
Domain/Realm	Set the domain name or IP address of the SIP Registrar server.
Proxy	Set domain name or IP address of SIP proxy server. By the time you can type :port number after the domain name to specify that port as the destination of data transmission (e.g., <i>nat.draytel.org:5065</i>)
Act as Outbound Proxy	Check this box to make the proxy acting as outbound proxy.
Display Name	The caller-ID that you want to be displayed on your friend's

	screen.
Account Number/Name	Enter your account name of SIP Address, e.g. every text before @.
Authentication ID	Check the box to invoke this function and enter the name or number used for SIP Authorization with SIP Registrar. If this setting value is the same as Account Name, it is not necessary for you to check the box and set any value in this field.
Password	The password provided to you when you registered with a SIP service.
Expiry Time	The time duration that your SIP Registrar server keeps your registration record. Before the time expires, the router will send another register request to SIP Registrar again.
NAT Traversal Support	<p>If the router (e.g., broadband router) you use connects to internet by other device, you have to set this function for your necessity.</p> <ul style="list-style-type: none"> ● None - Disable this function. ● Stun - Choose this option if there is Stun server provided for your router. ● Manual - Choose this option if you want to specify an external IP address as the NAT transversal support. ● Nortel - If the soft-switch that you use supports Nortel solution, you can choose this option.
Call Forwarding	<p>There are four options for you to choose. Disable is to close call forwarding function. Always means all the incoming calls will be forwarded into SIP URL without any reason. Busy means the incoming calls will be forwarded into SIP URL only when the local system is busy. No Answer means if the incoming calls do not receive any response, they will be forwarded to the SIP URL by the time out.</p> <p>SIP URL - Type in the SIP URL (e.g., aaa@draytel.org or abc@iptel.org) as the site for call forwarded.</p> <p>Time Out - Set the time out for the call forwarding. The default setting is 30 sec.</p>
Ring Port	Set Phone 1 and/or Phone 2 as the default ring port(s) for this SIP account.
Ring Pattern	Choose a ring tone type for the VoIP phone call.
Prefer Codec	<p>Select one of five codecs as the default for your VoIP calls. The codec used for each call will be negotiated with the peer party before each session, and so may not be your default choice. The default codec is G.729A/B; it occupies little bandwidth while maintaining good voice quality.</p> <p>If your upstream speed is only 64Kbps, do not use G.711 codec. It is better for you to have at least 256Kbps upstream if you would like to use G.711.</p> <p>Single Codec - If the box is checked, only the selected Codec will be applied.</p>
Packet Size	The amount of data contained in a single packet. The default value is 20 ms, which means the data packet will contain 20 ms voice information.
Voice Active Detector	This function can detect if the voice on both sides is active or not. If not, the router will do something to save the

	bandwidth for other using. Click On to invoke this function; click off to close the function.
--	--

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

IV-1-4 DialPlan

This page allows you to set phone book, digit map, call barring, regional settings and PSTN setup for the VoIP function. Click the links on this page to access into next pages for detailed settings.

IV-1-4-1 Phone Book

In this section, you can set your VoIP contacts in the “phonebook”. It can help you to make calls quickly and easily by using “speed-dial” Phone Number. There are 60 index entries in the phonebook for you to store all your friends and family members’ SIP addresses.

VoIP >> DialPlan Setup

Phone Book		Digit Map	Call Barring	Regional		
Index	Phone Number	Display Name	SIP URL	Dial Out Account	Secure Phone	Status
1.				Default	None	x
2.				Default	None	x
3.				Default	None	x
4.				Default	None	x
5.				Default	None	x
6.				Default	None	x
7.				Default	None	x
8.				Default	None	x
9.				Default	None	x
10.				Default	None	x
11.				Default	None	x
12.				Default	None	x
13.				Default	None	x
14.				Default	None	x
15.				Default	None	x
16.				Default	None	x
17.				Default	None	x
18.				Default	None	x
19.				Default	None	x
20.				Default	None	x

<< [1-20](#) | [21-40](#) | [41-60](#) >>

[Next](#) >>

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

Click any index number to display the dial plan setup page.

VoIP >> DialPlan Setup

Phone Book Index No. 1

Enable
 Phone Number
 Display Name
 SIP URL @
 Dial Out Account
 Secure Phone

Available settings are explained as follows:

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

Enable	Click this to enable this entry.
Phone Number	The speed-dial number of this index. This can be any number you choose, using digits 0-9 and * .
Display Name	The Caller-ID that you want to be displayed on your friend's screen. This let your friend can easily know who's calling without memorizing lots of SIP URL Address.
SIP URL	Enter your friend's SIP Address.
Dial Out Account	Choose one of the SIP accounts for this profile to dial out. It is useful for both sides (caller and callee) that registered to different SIP Registrar servers. If caller and callee do not use the same SIP server, sometimes, the VoIP phone call connection may not succeed. By using the specified dial out account, the successful connection can be assured.
Secure Phone	ZRTP+SRTP - It allows users to have encrypted RTP stream with the peer side using the same protocol (ZRTP+SRTP). Check this box to have secure call.
Cancel	Return to previous web page.

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



Info

If the incoming or outgoing calls do not match any entry on the phonebook, the router will try to make the call "being protected". But, if the call ends up "unprotected"(e.g. peer side does not support ZRTP+SRTP), the router will not play out a warning message.

IV-1-4-2 Digit Map

For the convenience of user, this page allows users to edit prefix number for the SIP account with adding number, stripping number or replacing number. It is used to help user have a quick and easy way to dial out through VoIP interface.

VoIP >> DialPlan Setup



Phone Book		Digit Map		Call Barring		Regional			
#	Enable	Match Prefix	Mode	OP Number	Min Len	Max Len	Route	Move Up	Move Down
1	<input checked="" type="checkbox"/>	03	Replace	8863	7	8	VoIP1		Down
2	<input checked="" type="checkbox"/>	886	Strip	886	9	10	VoIP2	UP	Down
3	<input type="checkbox"/>		None		0	0	None	UP	Down
4	<input type="checkbox"/>		None		0	0	None	UP	Down
5	<input type="checkbox"/>		None		0	0	None	UP	Down
6	<input type="checkbox"/>		None		0	0	None	UP	Down
7	<input type="checkbox"/>		None		0	0	None	UP	Down
8	<input type="checkbox"/>		None		0	0	None	UP	Down
9	<input type="checkbox"/>		None		0	0	None	UP	Down
10	<input type="checkbox"/>		None		0	0	None	UP	Down
11	<input type="checkbox"/>		None		0	0	None	UP	Down
12	<input type="checkbox"/>		None		0	0	None	UP	Down
13	<input type="checkbox"/>		None		0	0	None	UP	Down
14	<input type="checkbox"/>		None		0	0	None	UP	Down
15	<input type="checkbox"/>		None		0	0	None	UP	Down
16	<input type="checkbox"/>		None		0	0	None	UP	Down
17	<input type="checkbox"/>		None		0	0	None	UP	Down
18	<input type="checkbox"/>		None		0	0	None	UP	Down
19	<input type="checkbox"/>		None		0	0	None	UP	Down
20	<input type="checkbox"/>		None		0	0	None	UP	

Note:

1. The length for Min Len and Max Len fields should be between 0~25.
2. Wildcard '?' is supported.

OK Cancel

Available settings are explained as follows:

Item	Description
Enable	Check this box to invoke this setting.
Match Prefix	It is used to match with the number you dialed and may be modified by the action (add, strip or replace) with the OP Number.
Mode	<p>None - No action.</p> <p>Add - When you choose this mode, the OP number will be added before the match prefix number for calling out through the specific route.</p> <p>Strip - When you choose this mode, the partial or whole match prefix number will be deleted according to the OP number. Take the above picture (Prefix Table Setup web page) as an example, the OP number of 886 will be deleted completely for the match prefix number is set with 886.</p> <p>Replace - When you choose this mode, the OP number will be replaced by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix</p>

	Table Setup web page) as an example, the prefix number of 03 will be replaced by 8863. For example: dial number of “031111111” will be changed to “8863111111” and sent to SIP server.
OP Number	The front number you type here is the first part of the account number that you want to execute special function (according to the chosen mode) by using the prefix number.
Min Len	Set the minimal length of the dial number for applying the prefix number settings. Take the above picture (Prefix Table Setup web page) as an example, if the dial number is between 7 and 9, that number can apply the prefix number settings here.
Max Len	Set the maximum length of the dial number for applying the prefix number settings.
Route	Choose the one that you want to enable the prefix number settings from the saved SIP accounts. Please set up one SIP account first to make this interface available. This item will be changed according to the port settings configured in VoIP>> Phone Settings.
Move UP /Move Down	Click the link to move the selected entry up or down.

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

IV-1-4-3 Call Barring

Call barring is used to block phone calls coming from the one that is not welcomed.

VoIP >> DialPlan Setup



Phone Book	Digit Map	Call Barring	Regional			
Set to Factory Default						
Index	Call Direction	Barring Type	Barring Number/URL/URI	Route	Schedule	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 >>

Block Anonymous

Route Phone1 Phone2

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

Note:
Block the incoming calls which do not have the caller ID.

Block Unknown Domain

Route Phone1 Phone2

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

Note:
If the domain of the incoming call is different from the domain found in SIP accounts, the call should be blocked.

Block IP Address

Route Phone1 Phone2

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

Note:
The incoming calls by means of IP dialing (e.g.#192*168*1*1#) should be blocked.

Additionally, you can set advanced settings for call barring such as Block Anonymous, Block Unknown Domain or Block IP Address.

For Block Anonymous - this function can block the incoming calls without caller ID on the interface (Phone port) specified in the following window. Such control also can be done based on preconfigured schedules.

For Block Unknown Domain - this function can block incoming calls (through Phone port) from unrecognized domain that is not specified in SIP accounts. Such control also can be done based on preconfigured schedules.

For Block IP Address - this function can block incoming calls (through Phone port) coming from IP address. Such control also can be done based on preconfigured schedules.

Click any index number to display the call barring setup page.

VoIP >> DialPlan Setup

Call Barring Index No. 1

<input checked="" type="checkbox"/> Enable	
Call Direction	IN <input type="button" value="v"/>
Barring Type	Specific URI/URL <input type="button" value="v"/>
Specific URI/URL	<input type="text"/>
Route	All <input type="button" value="v"/>
Index(1-15) in Schedule Setup	<input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>

Note: Wildcard '?' is supported.

Available settings are explained as follows:

Item	Description
Enable	Check it to enable this entry.
Call Direction	Determine the direction for the phone call, IN - incoming call, OUT-outgoing call, IN & OUT - both incoming and outgoing calls.
Barring Type	Determine the type of the VoIP phone call, URI/URL or number.
Specific URI/URL or Specific Number	This field will be changed based on the type you selected for barring Type.
Route	All means all the phone calls will be blocked with such mechanism.
Index (1-15) in Schedule	Enter the index of schedule profiles to control the call barring according to the preconfigured schedules. Refer to section Applications>>Schedule for detailed configuration.

IV-1-4-4 Regional

This page allows you to process incoming or outgoing phone calls by regional. Default values (common used in most areas) will be shown on this web page. You *can change* the number based on the region that the router is placed.

VoIP >> DialPlan Setup

Phone Book	Digit Map	Call Barring	Regional
<input checked="" type="checkbox"/> Enable Regional			Set to Factory Default
Last Call Return [Miss]:	<input type="text" value="*69"/>		
Last Call Return [In]:	<input type="text" value="*12"/>	Last Call Return [Out]:	<input type="text" value="*14"/>
Call Forward [All] [Act]:	<input type="text" value="*72"/> +number+#	Call Forward [Deact]:	<input type="text" value="*73"/> +#
Call Forward [Busy] [Act]:	<input type="text" value="*90"/> +number+#	Call Forward [No Ans] [Act]:	<input type="text" value="*92"/> +number+#
Do Not Disturb [Act]:	<input type="text" value="*78"/> +#	Do Not Disturb [Deact]:	<input type="text" value="*79"/> +#
Hide caller ID [Act]:	<input type="text" value="*67"/> +#	Hide caller ID [Deact]:	<input type="text" value="*68"/> +#
Call Waiting [Act]:	<input type="text" value="*56"/> +#	Call Waiting [Deact]:	<input type="text" value="*57"/> +#
Block Anonymous [Act]:	<input type="text" value="*77"/> +#	Block Anonymous [Deact]:	<input type="text" value="*87"/> +#
Block Unknow Domain [Act]:	<input type="text" value="*40"/> +#	Block Unknow Domain [Deact]:	<input type="text" value="*04"/> +#
Block IP Calls [Act]:	<input type="text" value="*50"/> +#	Block IP Calls [Deact]:	<input type="text" value="*05"/> +#
Block Last Calls [Act]:	<input type="text" value="*60"/> +#		

Available settings are explained as follows:

Item	Description
Enable Regional	Check this box to enable this function.
Last Call Return [Miss]	Sometimes, people might miss some phone calls. Please dial number typed in this field to know where the last phone call comes from and call back to that one.
Last Call Return [In]	You have finished an incoming phone call, however you want to call back again for some reason. Please dial number typed in this field to call back to that one.
Last Call Return [Out]	Dial the number typed in this field to call the previous outgoing phone call again.
Call Forward [All][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place.
Call Forward [Deact]	Dial the number typed in this field to release the call forward function.
Call Forward [Busy][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place while the phone is busy.
Call Forward [No Ans][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place while there is no answer of the connected phone.
Do Not Disturb [Act]	Dial the number typed in this field to invoke the function of DND.
Do Not Distrub [Deact]	Dial the number typed in this field to release the DND

	function.
Hide caller ID [Act]	Dial the number typed in this field to make your phone number (ID) not displayed on the display panel of remote end.
Hide caller ID [Deact]	Dial the number typed in this field to release this function.
Call Waiting [Act]	Dial the number typed in this field to make all the incoming calls waiting for your answer.
Call Waiting [Deact]	Dial the number typed in this field to release this function.
Block Anonymous[Act]	Dial the number typed in this field to block all the incoming calls with unknown ID.
Block Anonymous[Deact]	Dial the number typed in this field to release this function.
Block Unknown Domain [Act]	Dial the number typed in this field to block all the incoming calls from unknown domain.
Block Unknown Domain [Deact]	Dial the number typed in this field to release this function.
Block IP Calls [Act]	Dial the number typed in this field to block all the incoming calls from IP address.
Block IP Calls [Deact]	Dial the number typed in this field to release this function.
Block Last Calls [Act]	Dial the number typed in this field to block the last incoming phone call.

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

IV-1-5 Phone Settings

This page allows user to set phone settings for Phone 1 and Phone 2 respectively. However, it changes slightly according to different model you have.

VoIP >> Phone Settings

Index	Port	Call Feature	Tone	Gain (Mic/Speaker)	Default SIP Account	DTMF Relay
1	Phone1	CW,CT,	User Defined	5/5		OutBand
2	Phone2	CW,CT,	User Defined	5/5		OutBand

Available settings are explained as follows:

Item	Description
Phone List	<p>Port - there are two phone ports provided here for you to configure. Phone1/Phone2 allows you to set general settings for PSTN phones.</p> <p>Call Feature - A brief description for call feature will be shown in this field for your reference.</p> <p>Tone - Display the tone settings that configured in the advanced settings page of Phone Index.</p> <p>Gain - Display the volume gain settings for Mic/Speaker that configured in the advanced settings page of Phone Index.</p> <p>Default SIP Account - "draytel_1" is the default SIP account. You can click the number below the Index field to change SIP account for each phone port.</p> <p>DTMF Relay - Display DTMF mode that configured in the advanced settings page of Phone Index.</p>

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

Detailed Settings for Phone Port

Click the number link for Phone port, you can access into the following page for configuring Phone settings.

VoIP >> Phone Settings

Phone1

<p>Call Feature</p> <p><input type="checkbox"/> Hotline <input type="text"/></p> <p><input type="checkbox"/> Session Timer <input type="text" value="90"/> sec</p> <p><input type="checkbox"/> T.38 Fax Function</p> <p>Error Correction Mode <input type="text" value="REDUNDANCY"/></p> <p><input type="checkbox"/> DND(Do Not Disturb) Mode</p> <p>Index(1-15) in Schedule Setup:</p> <p><input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/></p> <p>Note: Action and Idle Timeout settings will be ignored.</p> <p>Index(1-60) in Phone Book as Exception List:</p> <p><input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/></p> <p><input type="checkbox"/> CLIR (hide caller ID)</p> <p><input checked="" type="checkbox"/> Call Waiting</p> <p><input checked="" type="checkbox"/> Call Transfer</p>	<p>Default SIP Account <input type="text" value="v"/></p> <p><input type="checkbox"/> Play dial tone only when account registered</p>
---	--

Available settings are explained as follows:

Item	Description
Hotline	Check the box to enable it. Type in the SIP URL in the field for dialing automatically when you pick up the phone set.
Session Timer	Check the box to enable the function. In the limited time that you set in this field, if there is no response, the connecting call will be closed automatically.
T.38 Fax Function	Check the box to enable T.38 fax function. Error Correction Mode - choose a mode for error correction.
DND (Do Not Disturb) mode	Set a period of peace time without disturbing by VoIP phone call. During the period, the one who dial in will listen busy tone, yet the local user will not listen any ring tone. Index (1-15) in Schedule - Enter the index of schedule profiles to control when the phone will ring and when will not according to the preconfigured schedules. Refer to section Application >>Schedule for detailed configuration. Index (1-60) in Phone Book - Enter the index of phone book profiles. Refer to section DialPlan - Phone Book for detailed configuration.
CLIR (hide caller ID)	Check this box to hide the caller ID on the display panel of the phone set.
Call Waiting	Check this box to invoke this function. A notice sound will appear to tell the user new phone call is waiting for your response. Click hook flash to pick up the waiting phone call.
Call Transfer	Check this box to invoke this function. Click hook flash to initiate another phone call. When the phone call connection

	succeeds, hang up the phone. The other two sides can communicate, then.
Default SIP Account	You can set SIP accounts (up to six groups) on SIP Account page. Use the drop down list to choose one of the profile names for the accounts as the default one for this phone setting. Play dial tone only when account registered - Check this box to invoke the function.

In addition, you can press the Advanced button to configure tone settings, volume gain, MISC and DTMF mode. Advanced setting is provided for fitting the telecommunication custom for the local area of the router installed. Wrong tone settings might cause inconvenience for users. To set the sound pattern of the phone set, simply choose a proper region to let the system find out the preset tone settings and caller ID type automatically. Or you can adjust tone settings manually if you choose User Defined. TOn1, TOff1, TOn2 and TOff2 mean the cadence of the tone pattern. TOn1 and TOn2 represent sound-on; TOff1 and TOff2 represent the sound-off.

VoIP >> Phone Settings

Advance Settings >> Phone 1

Tone Settings						
Region	Taiwan		Caller ID Type			
	Low Freq(Hz)	High Freq(Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)
Dial tone	350	440	0	0	0	0
Ringing tone	440	480	1000	2000	0	0
Busy tone	480	620	500	500	0	0
Congestion tone	480	620	250	250	0	0
Volume Gain			DTMF			
Mic Gain(1-10)	5		DTMF Mode		OutBand (RFC2833)	
Speaker Gain(1-10)	5		Payload Type (RFC2833) (96 - 127)		101	
MISC			<input type="checkbox"/> Replace + digit in caller ID to			
Dial Tone Power Level (1 - 50)	27		00			
Ring Frequency (10 - 50HZ)	25					
Call Waiting Tone Power Level (1 - 30)	13					
Interdigit Timeout (1 - 10 sec)	4					

Available settings are explained as follows:

Item	Description
Region	Select the proper region which you are located. The common settings of Caller ID Type, Dial tone, Ringing tone, Busy tone and Congestion tone will be shown automatically on the page. If you cannot find out a suitable one, please choose User Defined and fill out the corresponding values for dial tone, ringing tone, busy tone, congestion tone by yourself for VoIP phone. Also, you can specify each field for your necessity. It is recommended for you to use the default settings for VoIP communication.
Volume Gain	Mic Gain (1-10)/Speaker Gain (1-10) - Adjust the volume of microphone and speaker by entering number from 1- 10. The

	larger of the number, the louder the volume is.
MISC	<p>Dial Tone Power Level - This setting is used to adjust the loudness of the dial tone. The smaller the number is, the louder the dial tone is. It is recommended for you to use the default setting.</p> <p>Ring Frequency - This setting is used to drive the frequency of the ring tone. It is recommended for you to use the default setting.</p> <p>Call Waiting Tone Power Level - This setting is used to adjust the loudness of the call waiting tone. The smaller the number is, the louder the tone is. It is recommended for you to use the default setting.</p> <p>Interdigit Timeout -Type a value in this field to specify time limit for interdigit.</p>
DTMF	<p>DTMF Mode - There are four DTMF modes for you to choose.</p> <ul style="list-style-type: none"> ● <i>InBand</i> - Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone. ● <i>OutBand</i> - Choose this one then the Vigor will capture the keypad number you pressed and transform it to digital form then send to the other side; the receiver will generate the tone according to the digital form it receive. This function is very useful when the network traffic congestion occurs and it still can remain the accuracy of DTMF tone. ● <i>SIP INFO</i>- Choose this one then the Vigor will capture the DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message. <p>Payload Type (rfc2833) - Type a number from 96 to 127, the default value was 101. This setting is available for the OutBand (RFC2833) mode.</p> <p>Replace + digit in caller ID to - For international phone call, the phone number could add a '+' sign, for example, +8865972727. However, the caller ID (DTMF type especially) can not display '+' at all.</p> <p>Therefore, this function can be enabled to give another number to replace the plus sign, for example, "+" can be replaced by "00". Then the above phone number will become 008865972727. When the callee receives such number, he can use re-dial function to dial back to the caller.</p>

IV-1-6 Status

From this page, you can find codec, connection and other important call status for each port.

VoIP >> Status

Status

Refresh Seconds:

Port	Status	Codec	PeerID	Elapse(hh:mm:ss)	Tx Pkts	Rx Pkts	Rx Loss	Rx Jitter(ms)	In Calls	Out Calls	Miss Calls	Speaker Gain
Phone1	IDLE			00:00:00	0	0	0	0	0	0	0	5
Phone2	IDLE			00:00:00	0	0	0	0	0	0	0	5

Log

Date (mm-dd-yyyy)	Time (hh:mm:ss)	Duration (hh:mm:ss)	In/Out/Miss	Account ID	Peer ID
00-00-0	00:00:00	00:00:00	-	-	-
00-00-0	00:00:00	00:00:00	-	-	-
00-00-0	00:00:00	00:00:00	-	-	-
00-00-0	00:00:00	00:00:00	-	-	-
00-00-0	00:00:00	00:00:00	-	-	-
00-00-0	00:00:00	00:00:00	-	-	-
00-00-0	00:00:00	00:00:00	-	-	-
00-00-0	00:00:00	00:00:00	-	-	-
00-00-0	00:00:00	00:00:00	-	-	-
00-00-0	00:00:00	00:00:00	-	-	-
00-00-0	00:00:00	00:00:00	-	-	-

xxxxxxxx : VoIP is encrypted.
xxxxxxxx : VoIP isn't encrypted.

Available settings are explained as follows:

Item	Description
Refresh Seconds	Specify the interval of refresh time to obtain the latest VoIP calling information. The information will update immediately when the Refresh button is clicked.
Port	It shows current connection status for Phone(s) ports.
Status	It shows the VoIP connection status. IDLE - Indicates that the VoIP function is idle. HANG_UP - Indicates that the connection is not established (busy tone). CONNECTING - Indicates that the user is calling out. WAIT_ANS - Indicates that a connection is launched and waiting for remote user's answer. ALERTING - Indicates that a call is coming. ACTIVE-Indicates that the VoIP connection is launched.
Codec	Indicates the voice codec employed by present channel.
PeerID	The present in-call or out-call peer ID (the format may be IP or Domain).
Elapse(hh:mm:ss)	The format is represented as hours:minutes:seconds.
Tx Pkts	Total number of transmitted voice packets during this connection session.
Rx Pkts	Total number of received voice packets during this connection session.
Rx Loss	Total number of lost packets during this connection session.

Rx Jitter	The jitter of received voice packets.
In Calls	Accumulation for the times of in call.
Out Calls	Accumulation for the times of out call.
Miss Calls	Accumulation for the times of missing call.
Speaker Gain	The volume of present call.
Log	Display logs of VoIP calls.

IV-1-7 Diagnostics

VoIP Diagnostics is used for diagnosing if VoIP phone failure is caused by different tone or caller ID.

VoIP >> Diagnostics

VoIP Diagnostics

<u>Caller ID</u> <u>Tone</u>

IV-1-7-1 Caller ID

VoIP >> VOIP Diagnostics

Send Caller ID

FXS 1	FXS 2	
Current type: FSK_ETSI		
Caller ID used to send : _____		
Item	Types	Status
<input checked="" type="radio"/>	FSK_ETSI	Untest
<input type="radio"/>	FSK_ETSI (UK)	Untest
<input type="radio"/>	FSK_BELLCORE (US/AU)	Untest
<input type="radio"/>	DTMF	Untest
<input type="radio"/>	DTMF (DK)	Untest
<input type="radio"/>	DTMF (SE/NL/FIN)	Untest
<input type="button" value="Set"/> <input type="button" value="Test"/>		

IV-1-7-2 Send Tone

VoIP >> VOIP Diagnostics

Send Tone

FXS 1	FXS 2					
Region <input type="text" value="Taiwan"/>						
	Low Freq(Hz)	High Freq(Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)
Dial tone	<input type="text" value="350"/>	<input type="text" value="440"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Ringing tone	<input type="text" value="440"/>	<input type="text" value="480"/>	<input type="text" value="1000"/>	<input type="text" value="2000"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Busy tone	<input type="text" value="480"/>	<input type="text" value="620"/>	<input type="text" value="500"/>	<input type="text" value="500"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Congestion tone	<input type="text" value="480"/>	<input type="text" value="620"/>	<input type="text" value="250"/>	<input type="text" value="250"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Item	Types		Status			
<input type="radio"/>	Dial Tone		Untest			
<input type="radio"/>	Busy Tone		Untest			
<input type="radio"/>	Congestion Tone		Untest			
<input type="button" value="Set"/> <input type="button" value="Test"/>						

Part V VPN



VPN



SSL VPN



Certificate
Management

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.

It is a form of VPN that can be used with a standard Web browser.

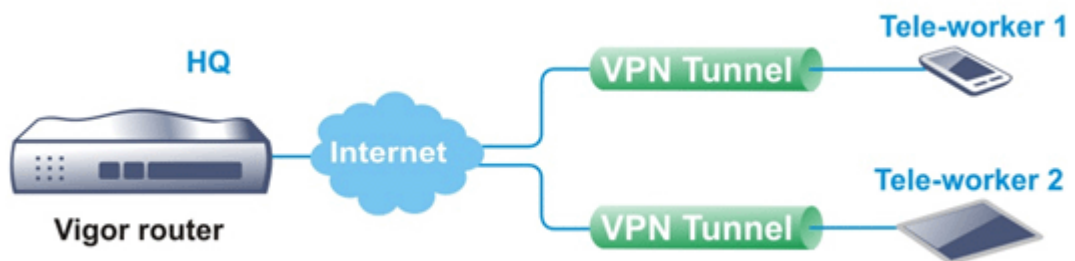
A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is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

V-1 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.

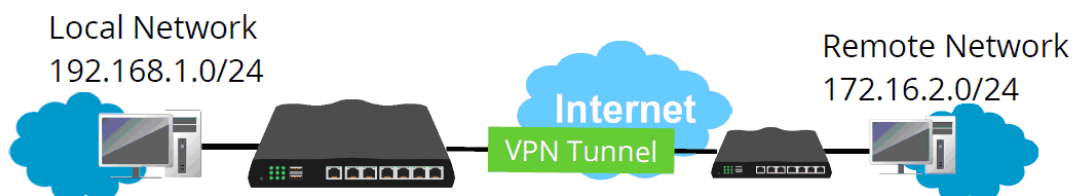
The VPN built is suitable for:

- 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



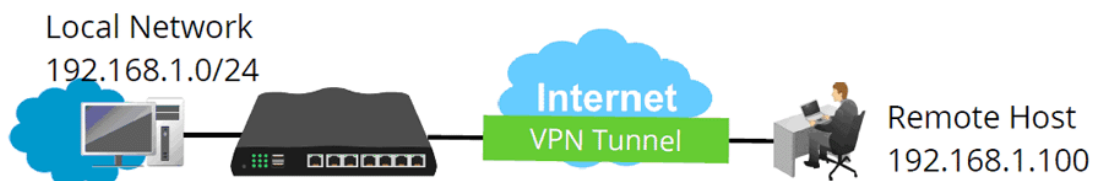
Site-to-Site (LAN-to-LAN)

- A connection between two router's LAN networks.
- Allows employees in branch offices and head office to share the same network resources.

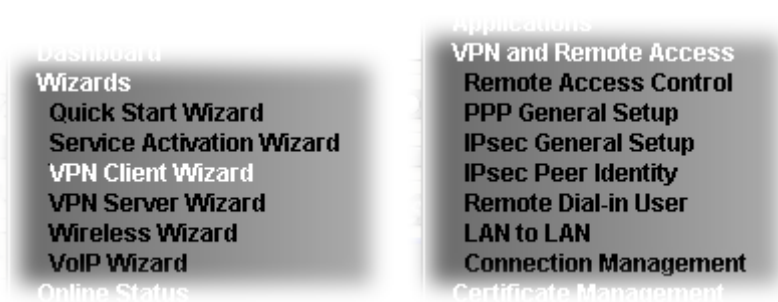


Remote Access (Remote Dial-in)

- A connection between the remote host and router's LAN network. The host will use an IP address in the local subnet.
- Allows employees to access the company's internal resources when they are traveling.



Web User Interface



V-1-1 VPN Client Wizard

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

1. Open Wizards>>VPN Client Wizard. The following page will appear.

VPN Client Wizard

Choose VPN Establishment Environment

LAN-to-LAN VPN Client Mode Selection:

Please choose a LAN-to-LAN Profile:

Note:

1. Please use Route Mode for typical LAN-to-LAN tunnels.
2. If the remote network is only expecting a single client or IP and is not configured to route the subnet then select NAT Mode.
3. If you are unsure of your configuration select Route Mode.

Available settings are explained as follows:

Item	Description
LAN-to-LAN Client Mode Selection	Choose the client mode. Route Mode/NAT Mode - If the remote network only allows you to dial in with single IP, please choose NAT mode, otherwise please choose Route Mode.
Please choose a LAN-to-LAN Profile	There are 32 VPN profiles for users to set.

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

VPN Client Wizard

VPN Connection Setting

Security Ranking:	Throughput Ranking:
Very High L2TP over IPSec	Very High L2TP / PPTP (None Encryption)
High IPSec / SSL	High IPSec
Medium PPTP (Encryption)	Medium L2TP over IPSec / PPTP (Encryption)
Low L2TP / PPTP (None Encryption)	Low SSL

Select VPN Type:

< Back

Next >

Finish

Cancel

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



Info

The following descriptions for VPN Type are based on the Route Mode specified in LAN-to-LAN Client Mode Selection.

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

VPN Client Wizard

VPN Client PPTP Encryption Settings

Profile Name	???
VPN Dial-Out Through	WAN1 First
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
Username	???
Password	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0 / 24
Local Network IP	192.168.1.1
Local Network Mask	255.255.255.0 / 24

< Back Next > Finish Cancel

When you choose IPsec, you will see the following graphic:

VPN Client Wizard

VPN Client IPsec Settings

Profile Name	???
VPN Dial-Out Through	WAN1 First
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
IKE Authentication Method	
<input checked="" type="radio"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input type="radio"/> Digital Signature (X.509)	
Peer ID	None
Local ID	
<input type="radio"/> Alternative Subject Name First	
<input type="radio"/> Subject Name First	
Local Certificate	None
IPsec Security Method	
<input type="radio"/> Medium (AH)	
<input checked="" type="radio"/> High (ESP)	AES with Authentication
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0 / 24
Local Network IP	192.168.1.1
Local Network Mask	255.255.255.0 / 24

< Back Next > Finish Cancel

When you choose L2TP, you will see the following graphic:

VPN Client Wizard

VPN Client L2TP Settings

Profile Name	???
VPN Dial-Out Through	WAN1 First
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
Username	???
Password	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0 / 24
Local Network IP	192.168.1.1
Local Network Mask	255.255.255.0 / 24

< Back Next > Finish Cancel

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

VPN Client Wizard

VPN Client L2TP over IPsec (Nice to Have) Settings

Profile Name	???
VPN Dial-Out Through	WAN1 First
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
IKE Authentication Method	
<input checked="" type="radio"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input type="radio"/> Digital Signature (X.509)	
Peer ID	None
Local ID	
<input type="radio"/> Alternative Subject Name First	
<input type="radio"/> Subject Name First	
Local Certificate	None
IPsec Security Method	
<input type="radio"/> Medium (AH)	
<input checked="" type="radio"/> High (ESP)	AES with Authentication
Username	???
Password	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0 / 24
Local Network IP	192.168.1.1
Local Network Mask	255.255.255.0 / 24

< Back Next > Finish Cancel

When you choose SSL, you will see the following graphic:

VPN Client Wizard

Profile Name	???
VPN Dial-Out Through	WAN1 First
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
Server Port (for SSL Tunnel):	443
Username	???
Password	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0 / 24
Local Network IP	192.168.1.1
Local Network Mask	255.255.255.0 / 24

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	Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only. 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. WAN1 Only /WAN2 Only/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 - If WAN2 failed, the router will use WAN1 for VPN connection. WAN2 Only: Only establish VPN if WAN1 down - If WAN1 failed, the router will use WAN2 for VPN connection.
Always On	Check to enable router always keep VPN connection.
Server IP/Host Name for VPN	Enter the IP address of the server or Enter the host name for such VPN profile.
Server Port (for SSL Tunnel)	Type a port number for SSL tunnel.
IKE Authentication Method	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. Pre-Shared Key- Specify a key for IKE authentication. Confirm Pre-Shared Key- Confirm the pre-shared key.
Digital Signature (X.509)	Click Digital Signature to invoke this function. Peer ID - Choose the peer ID selection from the drop down list.

	<p>Local ID - Choose Alternative Subject Name First or Subject Name First.</p> <p>Local Certificate - Use the drop down list to choose one of the certificates for using. You have to configure one certificate at least previously in Certificate Management >> Local Certificate. Otherwise, the setting you choose here will not be effective.</p>
IPsec Security Method	<p>Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.</p> <p>High - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.</p>
User Name	<p>This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above.</p> <p>The length of the user name is limited to 11 characters.</p>
Password	<p>This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above.</p> <p>The length of the password is limited to 11 characters.</p>
Remote Network IP	<p>Please type one LAN IP address (according to the real location of the remote host) for building VPN connection.</p>
Remote Network Mask	<p>Please Enter the network mask (according to the real location of the remote host) for building VPN connection.</p>
Local Network IP	<p>Please Enter the local network IP for TCP / IP configuration.</p>
Local Network Mask	<p>Please Enter the local network mask for TCP / IP configuration.</p>

- 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 Client Wizard

Please confirm your settings

LAN-to-LAN Index:	1
Profile Name:	3
VPN Connection Type:	PPTP (None Encryption)
VPN Dial-Out Through:	WAN1 First
Always on:	Yes
Server IP/Host Name:	172.16.3.8
Remote Network IP:	172.16.1.8
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.

V-1-2 VPN Server Wizard

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

1. Open Wizards>>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:	1 x ??? ▾
Please choose a Dial-in User Accounts:	8 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

Available settings are explained as follows:

Item	Description
VPN Server Mode Selection	Choose the direction for the VPN server. Site to Site VPN - To set a LAN-to-LAN profile automatically, please choose Site to Site VPN. Remote Dial-in User -You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in via VPN connection.
Please choose a LAN-to-LAN Profile	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.
Please choose a Dial-in User Accounts	This item is available when you choose Remote Dial-in User (Teleworker) as VPN server mode. There are 32 VPN tunnels for users to set.
Allowed Dial-in Type	This item is available after you choose any one of dial-in user account profiles. Next, you have to select suitable dial-in type for the VPN server profile. There are several types provided here (similar to VPN Client Wizard).

	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec <input checked="" type="checkbox"/> L2TP with IPsec Policy <input checked="" type="checkbox"/> SSL Tunnel	<div style="border: 1px solid black; padding: 2px;"> None ▼ None Nice to Have Must </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 Site-to-Site VPN 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 / 24 ▼
Local Network IP	192.168.1.1
Local Network Mask	255.255.255.0 / 24 ▼

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 Server Wizard

VPN Authentication Setting

Profile Name	???
PPTP / L2TP / L2TP over IPsec / SSL Tunnel Authentication	
Username	???
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
Local ID	
<input type="radio"/> Alternative Subject Name First	
<input type="radio"/> Subject Name First	
Peer IP/VPN Client IP	
Peer ID	
Site to Site Information	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0 / 24
Local Network IP	192.168.1.1
Local Network Mask	255.255.255.0 / 24

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such profile. The length of the file is limited to 10 characters.
User Name	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 11 characters.
Password	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 11 characters.
Pre-Shared Key	For IPsec/L2TP IPsec authentication, you have to type a pre-shared key. The length of the name is limited to 64 characters.
Confirm Pre-Shared Key	Enter the pre-shared key again for confirmation.
Digital Signature (X.509)	Check the box of Digital Signature to invoke this function. Peer ID - Choose the peer ID selection from the drop down list. Local ID - Choose Alternative Subject Name First or Subject Name First.
Peer IP/VPN Client IP	Enter the WAN IP address or VPN client IP address for the remote client.
Peer ID	Enter the ID name for the remote client. The length of the name is limited to 47 characters.

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 Enter the network mask (according to the real location of the remote host) for building VPN connection.
Local Network IP	Please Enter the local network IP for TCP / IP configuration.
Local Network Mask	Please Enter the local network mask for TCP / IP configuration.

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 Server Wizard

Please Confirm Your Settings

VPN Environment:	Site to Site VPN (LAN-to-LAN)
Index:	1
Profile Name:	test
Username:	admin123456
Allowed Service:	PPTP+IPsec+L2TP
Peer IP/VPN Client IP:	172.16.3.89
Peer ID:	tersterr
Remote Network IP:	0.0.0.0
Remote Network Mask:	255.255.255.0

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

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

Available settings are explained as follows:

Item	Description
Go to the VPN Connection Management	Click this radio button to access VPN and Remote Access>>Connection Management for viewing VPN Connection status.
Do another VPN Server Wizard Setup	Click this radio button to set another profile of VPN Server through VPN Server Wizard.
View more detailed configuration	Click this radio button to access VPN and Remote Access>>LAN to LAN for viewing detailed configuration.

V-1-3 Remote Access Control

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

VPN and Remote Access >> Remote Access Control Setup

Remote Access Control Setup

<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
<input checked="" type="checkbox"/> Enable OpenVPN 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.

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

V-1-4 PPP General Setup

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

VPN and Remote Access >> PPP General Setup

PPP General Setup

<p>PPP/MP Protocol</p> <p>Dial-In PPP Authentication: <input type="text" value="PAP/CHAP/MS-CHAP/MS-CHAPv2"/></p> <p>Dial-In PPP Encryption(MPPE): <input type="text" value="Optional MPPE"/></p> <p>Mutual Authentication (PAP): <input type="radio"/> Yes <input checked="" type="radio"/> No</p> <p>Username: <input type="text" value="Max: 23 characters"/></p> <p>Password: <input type="text" value="Max: 19 characters"/></p> <p>IP Address Assignment for Dial-In Users when DHCP is disabled.</p> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th></th> <th style="text-align: left;">Start IP Address</th> <th style="text-align: left;">IP Pool Counts</th> </tr> </thead> <tbody> <tr> <td>LAN 1</td> <td><input type="text" value="192.168.1.200"/></td> <td><input type="text" value="50"/></td> </tr> <tr> <td>LAN 2</td> <td><input type="text" value="192.168.2.200"/></td> <td><input type="text" value="50"/></td> </tr> </tbody> </table>		Start IP Address	IP Pool Counts	LAN 1	<input type="text" value="192.168.1.200"/>	<input type="text" value="50"/>	LAN 2	<input type="text" value="192.168.2.200"/>	<input type="text" value="50"/>	<p>PPP Authentication Methods</p> <p><input checked="" type="checkbox"/> Remote Dial-in User</p> <p><input checked="" type="checkbox"/> RADIUS</p> <p>Note:</p> <ol style="list-style-type: none"> 1. Default priority is Remote Dial-in User -> RADIUS. 2. Vigor router also supports Frame-IP-Address from RADIUS server to assign IP address to VPN client. <p>While using Radius Authentication:</p> <p>Assign IP from subnet: <input type="text" value="LAN1"/></p>
	Start IP Address	IP Pool Counts								
LAN 1	<input type="text" value="192.168.1.200"/>	<input type="text" value="50"/>								
LAN 2	<input type="text" value="192.168.2.200"/>	<input type="text" value="50"/>								

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> <ul style="list-style-type: none"> ● Require MPPE (40/128bits) - Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data. ● Maximum MPPE - This option indicates that the router will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.
Mutual Authentication (PAP)	<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</p>

	and Password of the mutual authentication peer. The length of the name/password is limited to 23/19 characters.
IP Address Assignment for Dial-In Users (when DHCP Disable set)	Enter a start IP address for the dial-in PPP connection for LAN1. LAN2 will be available if it is enabled. Refer to LAN>>General Setup for enabling the LAN interface.
PPP Authentication Methods	Select the method(s) to be used for authentication in PPP connection.
While using Radius Authentication	If PPP connection will be authenticated via RADIUS server, it is necessary to specify the LAN profile for the dial-in user to get IP from.

V-1-5 IPsec General Setup

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

There are two phases of IPsec.

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

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

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

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

VPN and Remote Access >> IPsec General Setup

VPN IKE/IPsec General Setup

(Dial-in settings for Remote Dial-In users and LAN-to-LAN VPN Client with Dynamic IP.)

IKE Authentication Method

Certificate:

Preferred Local ID:

General Pre-Shared Key:

Confirm General Pre-Shared Key:

XAuth User Pre-Shared Key:

Confirm XAuth User Pre-Shared Key:

IPsec Security Method

Basic
 Medium
 High

Encryption: AES/3DES/DES
 HMAC: SHA256/SHA1/MD5
 DH Group: G21/G20/G19/G14/G5/G2/G1
 AH: Enable

Available settings are explained as follows:

Item	Description
IKE Authentication	This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and

Method	<p>IPsec-related VPN connections such as L2TP over IPsec and IPsec tunnel. There are two methods offered by Vigor router for you to authenticate the incoming data coming from remote dial-in user, Certificate (X.509) and Pre-Shared Key.</p> <p>Certificate - X.509 certificates can be used for IKE authentication. To set up certificates on the router, go to the Certificate Management section.</p> <p>Preferred Local ID - Specify the preferred local ID information (Alternative Subject Name First or Subject Name First) for IPsec authentication while the client is using the general setting (without a specific Peer IP or ID in the VPN profile).</p> <p>General Pre-Shared Key- Define the PSK key for general authentication.</p> <p>Confirm General Pre-Shared Key- Re-enter the characters to confirm the pre-shared key.</p> <p>XAuth User Pre-Shared Key - Define the PSK key for IPsec XAuth authentication.</p> <p>Confirm XAuth User Pre-Shared Key- Re-enter the characters to confirm the pre-shared key for IPsec XAuth authentication.</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>Available methods include Basic, Medium and High. Each method offers different encryption, HMAC and DH Group.</p> <p>Basic - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.</p> <p>Medium - When this option is selected, the Authentication Header (AH) protocol can be used to provide authentication to IPsec traffic.</p> <p>High - When this option is selected, the Encapsulating Security Payload (ESP) protocol can be used to provide authentication and encryption to IPsec traffic. Three encryption standards are supported for ESP: DES, 3DES and AES, in ascending order of security.</p>

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

V-1-6 IPsec Peer Identity

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

X509 Peer ID Accounts: **| Set to Factory Default |**

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

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.
Enable	Check this box to enable this profile.
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

Enable this account

Profile Name

Accept Any Peer ID

Accept Subject Alternative Name

Type

Domain Name

Accept Subject Name

Country (C)

State (ST)

Location (L)

Organization (O)

Organization Unit (OU)

Common Name (CN)

Email (E)

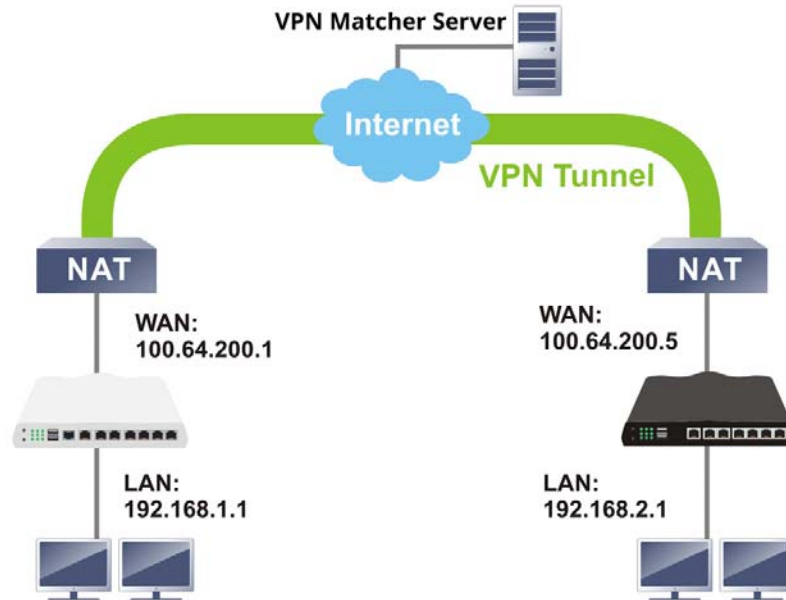
Available settings are explained as follows:

Item	Description
Profile Name	Enter the name of the profile. The maximum length of the name you can set is 32 characters.
Enable this account	Check it to enable such account profile.
Accept Any Peer ID	Click to accept any peer regardless of its identity.
Accept Subject Alternative Name	Click to check one specific field of digital signature to accept the peer with matching value. The field can be IP Address, Domain, or E-mail Address. The box under the Type will appear according to the type you select and ask you to fill in corresponding setting.
Accept Subject Name	Click to check the specific fields of digital signature to accept the peer with matching value. The field includes Country (C), State (ST), Location (L), Organization (O), Organization Unit (OU), Common Name (CN), and Email (E).

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

V-1-7 VPN Matcher Setup

Normally, to establish VPN connection, at least one peer must have a public IP address. The VPN Matcher server can help two Draytek routers behind NAT establish a secure VPN tunnel for data transmission between each other. Refer to the following figure.



There is one limitation for the VPN connection. Both routers must be behind a cone NAT, but not symmetric NAT.

Go to VPN and Remote Access >> VPN Matcher Setup to open the following page.

VPN and Remote Access >> VPN Matcher Setup

Enable
 Disable

VPN Matcher Server: :

Account:

Authkey:

Note: You can get your Authkey on [VPN Matcher Dashboard](#).

NAT Detection

STUN Server

Group Device List

Available settings are explained as follows:

Item	Description
Enable / Disable	Click to enable / disable the function of VPN Matcher Setup.
VPN Matcher Server	The IP address of the DrayTek VPN Matcher server is defined

	as "vpn-matcher.draytek.com" with the port nubmer "31503".
Account	Enter the name of the account for accessing into VPN server.
AuthKey	Enter the authentication key for finding a Vigor router with the same group of this device from the VPN matcher server. Then set a VPN link between Vigor routers on both ends via VPN wizard.
OK	Click to save the settings.
STUN Server	Detect - Click to check if the NAT used by Vigor router is core NAT or not. If not, no VPN can be established.
Group Device List	Get List - After entering the Authkey above, click to get available Vigor router which is within the same group as this device.

V-1-8 OpenVPN

OpenVPN offers a convenient way for users to build VPN between local end and remote end.

With integrating of OpenVPN, Vigor router can help users to achieve more robust, reliable and secure private connections for business needs.

There are two advantages of OpenVPN:

- It can be operated on different systems such as Windows, Linux, and MacOS.
- Based on the standard protocol of SSL encryption, OpenVPN can provide you with a scalable client/server mode, permitting multi-client to connect to a single OpenVPN Server process over a single TCP or UDP port.

V-1-7-1 General Setup

Before establishing OpenVPN connection, general settings for OpenVPN service shall be configured first.

VPN and Remote Access >> OpenVPN

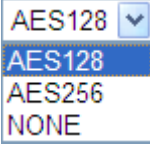


General Setup	Client Config
<input checked="" type="checkbox"/> Enable UDP	
UDP Port	<input type="text" value="1194"/>
<input checked="" type="checkbox"/> Enable TCP	
TCP Port	<input type="text" value="1194"/>
Cipher Algorithm	<input type="text" value="AES128"/>
HMAC Algorithm	<input type="text" value="SHA1"/>
Certificate Authentication	<input type="checkbox"/>

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

OK

Available settings are explained as follows:

Item	Description
Enable UDP	Check the box to enable UDP port setting for OpenVPN. UDP Port - Enter a number.
Enable TCP	Check the box to enable TCP port setting for OpenVPN. TCP Port - Enter a number.
Cipher Algorithm	Two encryptions are supported, AES128 and AES256. 
HMAC Algorithm	The HMAC algorithm only supports SHA1/SHA256.

	<div style="border: 1px solid black; padding: 2px;"> SHA1 ▼ SHA1 SHA256 NONE </div>
Certificate Authentication	<p>If certificate authentication is required for OpenVPN, simply check the box to apply the trusted CA certificate and local certificate for OpenVPN tunnel.</p> <p>Certificate authentication can offer more secure VPN tunnel between the client and the router.</p>

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

V-1-7-2 Client Config

The settings on this page can be downloaded as a file. Later, such file can be imported and applied to remote end's CPE (as VPN client). Then, a private connection via OpenVPN tunnel between the server and the client can be connected successfully.

VPN and Remote Access >> OpenVPN



General Setup	Client Config
Remote Server	<input type="text" value=""/>
Transport Protocol	<input type="text" value="TCP"/>
File Name	<input type="text" value=""/> .ovpn
CA cert	<input type="text" value=""/> .cert
Client cert	<input type="text" value=""/> .cert
Client key	<input type="text" value=""/> .key

Note:

Please make sure the CA files are located in the same folder with .ovpn file.

Export

Available settings are explained as follows:

Item	Description
Remote Server	Use the drop down list to specify an IP address of WAN for VPN connection.
Transport Protocol	Simply choose UDP or TCP as protocol for building OpenVPN connection between the server and the remote client.
Config Finename	Enter a name for the configuration file.
CA cert	Enter the certificate authority (CA) file name obtained from 3rd party provider
Client cert	Each client in an OpenVPN connection must have its certificate and private key. Enter the certificate file name obtained from 3rd party provider
Client key	Enter the private key file name obtained from 3rd party provider

Export	The settings in this page can be saved as a file after clicking such button. Later, the downloaded file can be imported to the VPN client for building OpenVPN connection.
--------	--

V-1-8 Remote Dial-in User

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

The router provides 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	Enable	User	Status	Index	Enable	User	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"/>	???	---

Backup setting to file: <input type="button" value="Backup"/>	Restore From File: <input type="button" value="瀏覽..."/> 未選擇檔案。 <input type="button" value="Restore"/>
--	--

Download Smart VPN Client:

[Smart VPN Client for Windows PC](#)

[Smart VPN Android/iOS App](#)

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.
Enable	Check this box to enable this profile.
User	Display the username for the specific dial-in user of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.
Status	Display the access state of the specific dial-in user. The symbol V and X represent the specific dial-in user to be active and inactive, respectively.

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

VPN and Remote Access >> Remote Dial-in User

Index No. 1

<p>User account and Authentication</p> <p><input type="checkbox"/> Enable this account</p> <p>Idle Timeout <input type="text" value="300"/> second(s)</p> <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"/> IPsec XAuth</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 checked="" type="checkbox"/> OpenVPN Tunnel</p> <p><input checked="" type="checkbox"/> IKEv2 EAP</p> <hr/> <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 <input style="background-color: #e0e0e0;" type="text" value="Max: 19 characters"/></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><input style="background-color: #e0e0e0;" type="text" value="IKE Pre-Shared Key"/> <input style="background-color: #e0e0e0;" type="text" value="Max: 64 characters"/></p> <p><input type="checkbox"/> Digital Signature(X.509)</p> <p><input style="background-color: #e0e0e0;" 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>
--	--

Note:

Username can not contain characters " and '.

Available settings are explained as follows:

Item	Description
User account and Authentication	Enable this account - Check the box to enable this function. 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>	<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>IPsec XAuth - Allow the remote dial-in user to make an IPsec VPN connection through Internet via IPsec XAuth Pre-shared Key and the username/password authentication.</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 - Allow the remote dial-in user to make an SSL VPN connection through Internet.</p> <p>OpenVPN Tunnel - Allow the remote dial-in user to set a VPN connection through OpenVPN.</p> <p>Specify Remote Node -You can specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode).</p> <p>Uncheck the checkbox means 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. <p>User Name - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 23 characters.</p> <p>Password - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 19 characters.</p> <p>Enable Mobile One-Time Passwords (mOTP) - Check this box to make the authentication with mOTP function.</p> <p>PIN Code - Enter the code for authentication (e.g, 1234).</p> <p>Secret - Use the 32 digit-secret number generated by mOTP</p>
-----------------------------	---

	in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).
Subnet	Chose one of the subnet selections for such VPN profile. Assign Static IP Address - Please type a static IP address for the subnet you specified.
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 specifying the IP address of the remote node. Pre-Shared Key - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key. Digital Signature (X.509) - Check the box of Digital Signature to invoke this function and Select one predefined Profiles set in the VPN and Remote Access >>IPsec Peer Identity.
IPsec Security Method	This group of fields is a must for IPsec Tunnels and L2TP with IPsec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method. Medium-Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it. High-Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES. Local ID (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.

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

V-1-9 LAN to LAN

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

VPN and Remote Access >> LAN to LAN



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

Index	Enable	Name	Remote Network	Status	Index	Enable	Name	Remote Network	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"/>	???		---

Backup setting to file: <input type="button" value="Backup"/>	Upload From File: <input type="button" value="瀏覽..."/> 未選擇檔案。 <input type="button" value="Restore"/>
--	---

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 LAN to LAN profile.
Enable	Check this box to enable this profile.
Name	Indicate the name of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.
Status	Indicate the status of individual profiles. The symbol V and X represent the profile to be active and inactive, respectively.

To edit each profile:

- Click each index to edit each profile and you will get the following page. Each LAN-to-LAN profile includes 5 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.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="???"/> <input type="checkbox"/> Enable this profile <hr/> 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 IPsec tunnel alive PING to the IP <input type="text" value=""/>
--	---

2. Dial-Out Settings

Type of Server I am calling <input checked="" type="radio"/> PPTP <input type="radio"/> IPsec Tunnel <input type="text" value="IKEv1"/> <input type="radio"/> IKEv2 EAP <input type="radio"/> IPsec XAuth <input type="radio"/> L2TP with IPsec Policy <input type="text" value="None"/> <input type="radio"/> SSL Tunnel <hr/> Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <input type="text" value=""/> Max: 41 characters Server Port (for SSL Tunnel): <input type="text" value="443"/>	Username <input type="text" value="???"/> Password <input type="text" value=""/> Max: 15 characters PPP Authentication <input type="text" value="PAP/CHAP/MS-CHAP/MS-CHAPv2"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off <hr/> IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key <input type="text" value=""/> Max: 64 characters <input type="radio"/> Digital Signature(X.509) Peer ID <input type="text" value="None"/> Local ID <input type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First Local Certificate <input type="text" value="None"/> <hr/> IPsec Security Method <input type="radio"/> Medium(AH) <input checked="" type="radio"/> High(ESP) <input type="text" value="AES with Authentication"/> <input type="button" value="Advanced"/> <hr/> Schedule Profile <input type="text" value="None"/> <input type="text" value="None"/> <input type="text" value="None"/> <input type="text" value="None"/>
--	---

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 is useful for dial-out only.</p> <ul style="list-style-type: none"> 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. WAN1 Only /WAN2 Only/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 - If WAN2 failed, the router will use WAN1 for VPN connection. WAN2 Only: Only establish VPN if WAN1 down - If WAN1 failed, the router will use WAN2 for VPN

	<p>connection.</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. <p>Call Direction - Specify the allowed call direction of this LAN-to-LAN profile.</p> <ul style="list-style-type: none"> ● Both:-initiator/responder ● Dial-Out- initiator only ● Dial-In- responder only. <p>Always On-Check to enable router always keep VPN connection.</p> <p>Idle Timeout: The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.</p> <p>Enable PING to keep IPsec tunnel 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 IPsec tunnel 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 disconnects 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.
- Must: Specify the IPsec policy to be definitely applied on the L2TP connection.

SSL Tunnel - Build an SSL VPN connection to the server through Internet.

User Name - This field is applicable when you select, PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 49 characters.

Password - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 15 characters.

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 compatibility.

VJ compression - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally set to On to improve bandwidth utilization.

IKE Authentication Method - This group of fields is applicable for IPsec Tunnels and L2TP with IPsec Policy.

- Pre-Shared Key - Input 1-63 characters as pre-shared key.
- Digital Signature (X.509) - Select one predefined Profiles set in the VPN and Remote Access >>IPsec Peer Identity.

Peer ID - Select one of the predefined Profiles set in VPN and Remote Access >>IPsec Peer Identity.

Local ID - Specify a local ID (Alternative Subject Name First or Subject Name First) to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.

- Local Certificate - Select one of the profiles set in Certificate Management>>Local Certificate.

IPsec Security Method - This group of fields is a must for IPsec Tunnels and L2TP with IPsec Policy.

- 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.

Advanced - Specify mode, proposal and key life of each IKE phase, Gateway, etc.

The window of advance setup is shown as below:

IKE advanced settings

Main mode Aggressive mode

IKE phase 1 mode

IKE phase 1 proposal: Auto

IKE phase 2 proposal: HMAC_SHA1/HMAC_MD5

IKE phase 1 key lifetime: 28800 (900 - 86400)

IKE phase 2 key lifetime: 3600 (600 - 86400)

Perfect Forward Secret: Disable Enable

Local ID:

Note: If you select "Auto" in IKE phase 1 proposal, the router will send the following proposals to negotiate with the remote site. The proposals include: DES_(MD5|SHA)_G1, 3DES_MD5_G1, 3DES_MD5_G2, 3DES_(MD5|SHA)_G5, AES128_MD5_(G2|G5), AES256_SHA_(G2|G5), AES256_SHA_G14

OK Close

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.

Schedule Profile - 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.

3. Dial-In Settings

Allowed Dial-In Type <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input checked="" type="checkbox"/> IPsec XAuth <input checked="" type="checkbox"/> L2TP with IPsec Policy None <input checked="" type="checkbox"/> SSL Tunnel <input type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input style="width: 100px;" type="text"/> or Peer ID Max: 47 characters		Username ??? Password(Max 11 char) Max: 11 characters VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key Max: 64 characters <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. 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 / 24 Local Network IP 192.168.1.1 Local Network Mask 255.255.255.0 / 24 <input type="button" value="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)	
<input type="button" value="OK"/> <input type="button" value="Clear"/> <input type="button" value="Cancel"/>					

Available settings are explained as follows:

Item	Description
Dial-In Settings	<p>Allowed Dial-In Type - Determine the dial-in connection with different types.</p> <ul style="list-style-type: none"> ● PPTP - Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below. ● IPsec Tunnel- Allow the remote dial-in user to trigger an IPsec VPN connection through Internet. ● L2TP 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: <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. ● SSL Tunnel- Allow the remote dial-in user to trigger an SSL VPN connection through Internet. <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.</p> <p>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 length of the name is limited to 11 characters.</p> <p>Password - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 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> <ul style="list-style-type: none"> ● 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. <ul style="list-style-type: none"> ■ 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>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.
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</p>

during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.

Remote Network IP/ Remote Network Mask - Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPsec, this is the destination clients IDs of phase 2 quick mode.

Local Network IP / Local Network Mask - Display the local network IP and mask for TCP / IP configuration. You can modify the settings if required.

More - Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Masks through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.

192.168.1.1/doc/121MRt.htm

Profile Index :1

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.

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.

Change default route to this VPN tunnel - Check this box to change the default route with this VPN tunnel.

IPSec VPN with the Same subnet

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.

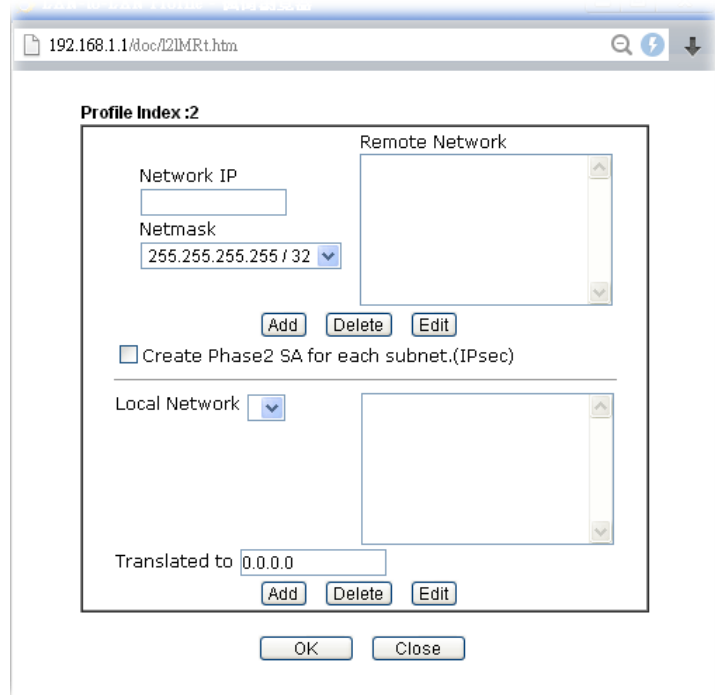
After checking the box of IPSec VPN with the Same subnet, the options under TCP/IP Network Settings will be changed as shown below:

5. TCP/IP Network Settings

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.

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.

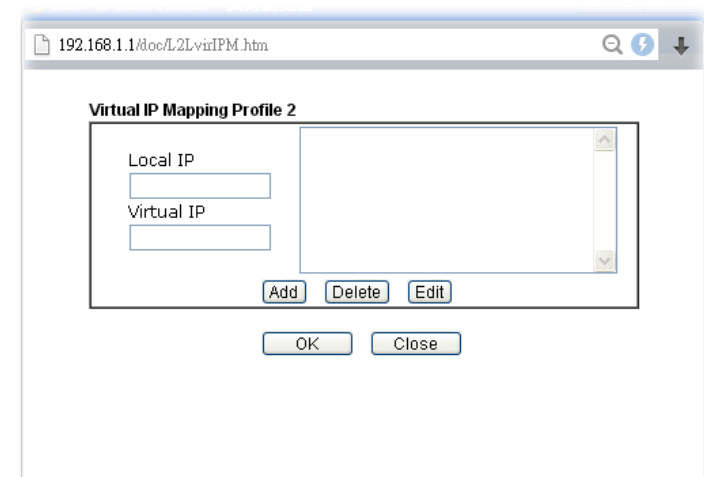
Advanced - Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.



Translated Type - There are two types for you to choose.

- Whole Subnet
- Specific IP Address

Virtual IP Mapping - A pop up dialog will appear for you to specify the local IP address and the mapping virtual IP address.



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

V-1-10 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 |

Dial

VPN Connection Status

All VPN Status		LAN-to-LAN VPN Status		Remote Dial-in User Status				
VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(bps)	Rx Pkts	Rx Rate(bps)	UpTime

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

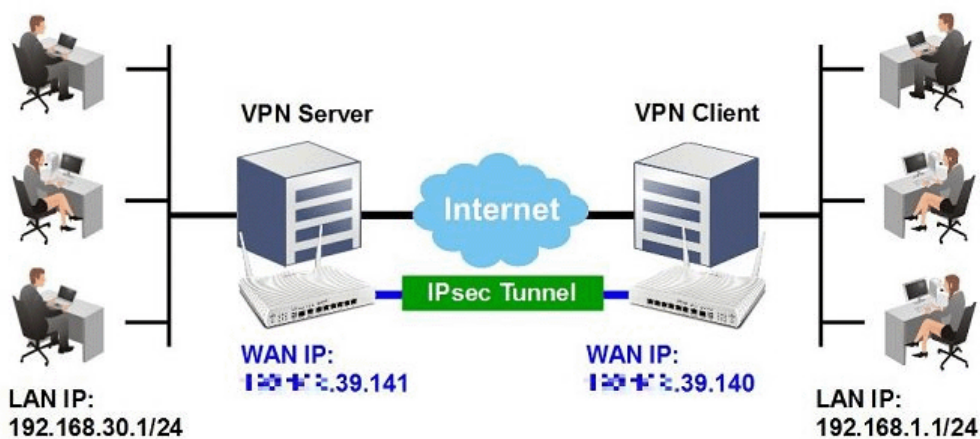
Available settings are explained as follows:

Item	Description
Dial-out Tool	Dial - Click this button to execute dial out function.

Application Notes

A-1 How to Build a LAN-to-LAN VPN Between Vigor Routers via IPsec Main Mode

This document introduces how to set up Main mode IPsec Tunnel between two Vigor Routers. IPsec VPN with Main mode use the IP address of VPN client as identifier, and the IP address must be set on VPN server; therefore, if the VPN client doesn't have a static IP, please use Aggressive mode instead.



VPN Server (Dial-In Site) Setup

1. Create a Dial-In profile for VPN user, go to VPN and Remote Access >> LAN to LAN, click on an available index to add a new profile.

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
<u>1.</u>	???	<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"/>	---

2. Set up the dial-in profile.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="Host"/>	Call Direction <input type="radio"/> Both <input type="radio"/> Dial-Out <input checked="" type="radio"/> Dial-in
<input checked="" type="checkbox"/> Enable this profile	<input type="checkbox"/> Always on
VPN Dial-Out Through <input type="text" value="WAN1 First"/>	Idle Timeout <input type="text" value="300"/> second(s)
Netbios Naming Packet <input type="radio"/> Pass <input type="radio"/> Block	<input type="checkbox"/> Enable PING to keep IPsec tunnel 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.)	

In Common Settings,

- (a) Enter the Profile Name.
- (b) Enable this profile.
- (c) Set Call Direction to Dial-in.

In Dial-In Setting,

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 <input type="checkbox"/> SSL Tunnel	Username <input type="text" value="???"/> Password(Max 11 char) <input type="text"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
<input checked="" type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text" value="39.140"/> or Peer ID <input type="text"/>	IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="text" value="....."/> <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

IKE Authentication Method

Pre-Shared Key <input type="text" value="....."/>
Confirm Pre-Shared Key <input type="text" value="....."/>

- (d) Make sure Allowed Dial-in Type has IPsec Tunnel enabled.
 - (e) Enable Specify Remote VPN Gateway and enter Peer VPN Server IP as the public IP of VPN client router.
 - (f) Click on IKE Pre-Shared Key and enter the Pre-shared Key.
 - (g) Select the IPsec Security Method that are allowed to use.
3. In TCP/IP Network Settings, enter VPN Client's LAN network in Remote Network IP and Remote Network Mask. Click OK to save the profile.

5. TCP/IP Network Settings

My WAN IP	<input type="text" value="0.0.0.0"/>	RIP Direction	Disable
Remote Gateway IP	<input type="text" value="0.0.0.0"/>	From first subnet to remote network, you have to do	Route
Remote Network IP	<input type="text" value="192.168.1.1"/>	<input type="checkbox"/> IPsec VPN with the Same Subnets	
Remote Network Mask	<input type="text" value="255.255.255.0"/>	<input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)	
Local Network IP	<input type="text" value="192.168.30.1"/>		
Local Network Mask	<input type="text" value="255.255.255.0"/>		

VPN Client (Dial-out Site) Setup

1. Create a Dial-out profile to VPN server: Go to VPN and Remote Access >> LAN to LAN, click on an available index to add a new profile.

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
<u>1.</u>	???	<input type="checkbox"/>	---	<u>17.</u>	???	<input type="checkbox"/>	---
<u>2.</u>	???	<input type="checkbox"/>	---	<u>18.</u>	???	<input type="checkbox"/>	---
<u>3.</u>	???	<input type="checkbox"/>	---	<u>19.</u>	???	<input type="checkbox"/>	---

2. Setup the dial-out profile.

In Common Settings,

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="Client"/>	Call Direction <input type="radio"/> Both <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-in
<input checked="" type="checkbox"/> Enable this profile	<input type="checkbox"/> Always on
VPN Dial-Out Through <input type="text" value="WAN1 First"/>	Idle Timeout <input type="text" value="300"/> second(s)
Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block	<input type="checkbox"/> Enable PING to keep IPsec tunnel 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.)	

- (a) Enter a Profile Name.
- (b) Enable this profile.
- (c) Set Call Direction to Dial-Out.

In Dial-out Setting,

2. Dial-Out Settings

- (h) Select IPsec Tunnel for Type of Sever I am Calling.
- (i) Enter VPN Server's WAN IP or domain name in Sever IP/Host Name for VPN.
- (j) Click IKE Pre-Shared Key and enter the same Pre-Shared key as VPN Server.
- (k) Click on Advanced in IPsec Security Method.

In IKE advanced settings,

- (l) Select Main Mode for IKE phase 1 mode.
- (m) Make sure phase 1 and phase 2 proposal are using the security methods which are accepted by VPN server.
- (n) Click OK to save.

- 3. In TCP/IP Network Settings, enter VPN Server's LAN Network in Remote Network IP and Remote Network Mask. Click OK to save the profile.

5. TCP/IP Network Settings

My WAN IP	0.0.0.0	RIP Direction	Disable ▼
Remote Gateway IP	0.0.0.0	From first subnet to remote network, you have to do	
Remote Network IP	192.168.30.1	Route ▼	
Remote Network Mask	255.255.255.0	<input type="checkbox"/> IPsec VPN with the Same Subnets	
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		
	<input type="button" value="More"/>		

VPN Tunnel Establishment

To initiate the VPN connection, go to VPN and Remote Access >> Connection Management on VPN Client, select the profile to VPN Sever and click Dial.

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds : 10 ▼ Refresh

General Mode:	(Client) 39.141 ▼	<input type="button" value="Dial"/>
Backup Mode:	▼	<input type="button" value="Dial"/>
Load Balance Mode:	▼	<input type="button" value="Dial"/>

If all the settings are matched, the VPN will be established, and the statistics will be displayed on the same page.

VPN Connection Status

Current Page: 1 Page No. Go >>

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime
1	IPsec Tunnel (Client) DES-No Auth	39.141 via WAN2	192.168.30.1/24	0	0	2	0	0:0:1 <input type="button" value="Drop"/>

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

V-2 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.

Web User Interface



V-2-1 General Setup

The general settings of the SSL VPN Server and SSL Tunnel are entered on this page.

SSL VPN >> General Setup

SSL VPN General Setup

Bind to WAN	<input checked="" type="checkbox"/> WAN1	<input checked="" type="checkbox"/> WAN2	<input checked="" type="checkbox"/> WAN3
Port	<input type="text" value="443"/>	(Default: 443)	
Server Certificate	<input type="text" value="self-signed"/>		

Note:

1. The settings will act on all SSL applications.
2. Please go to **System Maintenance >> Management** to enable SSLv3.0 .
3. Please go to **System Maintenance >> Self-Signed Certificate** to generate a new "self-signed" certificate.

Available settings are explained as follows:

Item	Description
Bind to WAN	Select the WAN interfaces to accept inbound SSL VPN connections.
Port	The port to be used for SSL VPN server. This is separate from the management port which is configured in System Maintenance>>Management. 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. Specify the certificate to be used for SSL connections. Select a certificate from imported or generated certificates on the router, or choose Self-signed to use the router's built-in default certificate. The selected 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.

V-2-2 User Account

With SSL VPN, Vigor2762 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, Vigor2762 Series allows up to 16 simultaneous incoming users.

SSL VPN authentication and permissions management are implemented through user accounts. SSL VPN user accounts are shared with the remote dial-in user accounts used by other VPN protocols such as PPTP and L2TP, and hence SSL VPN's User Account setup page SSL VPN >> User Account is identical to VPN and Remote Access >> Remote Dial-in user.


SSL VPN >> Remote Dial-in User

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

Index	Enable	User	Status	Index	Enable	User	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"/>	???	---

Backup setting to file: <input type="button" value="Backup"/>	Restore From File: <input type="button" value="瀏覽..."/> 未選擇檔案。 <input type="button" value="Restore"/>
--	--

Download Smart VPN Client:

 [Smart VPN Client for Windows PC](#)

 [Smart VPN Android/iOS App](#)

Click each index to edit one remote user profile.

SSL VPN >> Remote Dial-in User

Index No. 1

<p>User account and Authentication</p> <p><input type="checkbox"/> Enable this account</p> <p>Idle Timeout <input type="text" value="300"/> second(s)</p> <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"/> IPsec XAuth</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 checked="" type="checkbox"/> OpenVPN Tunnel</p> <p><input checked="" type="checkbox"/> IKEv2 EAP</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="width: 100px;" type="text" value="???"/></p> <p>Password <input style="width: 100px;" type="text" value="Max: 19 characters"/></p> <p><input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP)</p> <p>PIN Code <input style="width: 100px;" type="text"/></p> <p>Secret <input style="width: 100px;" type="text"/></p> <hr/> <p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p><input style="width: 100px;" type="text" value="IKE Pre-Shared Key"/> <input style="width: 100px;" type="text" value="Max: 64 characters"/></p> <p><input type="checkbox"/> Digital Signature(X.509)</p> <p><input type="text" value="None"/></p> <hr/> <p>IPsec Security Method</p> <p><input checked="" type="checkbox"/> Medium(AH)</p> <p>High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p> <p>Local ID (optional) <input style="width: 100px;" type="text"/></p>
--	--

Note:
Username can not contain characters " and '.

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> <p>User Name - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the name/password is limited to 23 characters.</p> <p>Password - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the name/password is limited to 19 characters.</p> <p>Enable Mobile One-Time Passwords (mOTP) - Check this box to make the authentication with mOTP function.</p> <ul style="list-style-type: none"> ● PIN Code - Enter the code for authentication (e.g, 1234). ● Secret - Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).
Allowed Dial-In Type	Select the VPN protocols that this user is allowed to use.

Item	Description
	<p>PPTP - Allow the remote dial-in user to establish VPN connections with the PPTP protocol. 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 establish IPSec tunnels.</p> <p>IPsec XAuth - Allow the remote dial-in user to establish an IPsec VPN connection through XAuth server in Internet.</p> <p>L2TP with IPSec Policy - Allow the remote dial-in user to establish L2TP VPN connections. You can select to use L2TP alone or with IPSec. Select one of the following options:</p> <ul style="list-style-type: none"> ● None - Do not apply the IPSec policy. L2TP connections are not encrypted. ● Nice to Have - Attempt to establish an IPsec secure channel first, before starting an L2TP session. If an IPsec secure channel cannot be established with the remote client, fall back to an L2TP connection without encryption. ● Must - Require that an IPsec secure channel be established before starting an L2TP connection. Disconnect if an IPsec secure channel cannot be established. <p>SSL Tunnel - Select to allow the remote dial-in user to initiate SSL VPN tunnels.</p> <p>OpenVPN Tunnel - Select to allow the remote dial-in user to initiate OpenVPN tunnels.</p> <p>IKEv2 EAP - Select to allow the remote dial-in user to initiate IKEv2 tunnels.</p> <p>Specify Remote Node - Select this option to specify the remote IP address, ISDN number or peer ID (used in IKE aggressive mode) used to authenticate the remote dial-in user. If this option is not selected, the authentication and security methods specified in the general settings will be used instead.</p> <p>Netbios Naming Packet</p> <ul style="list-style-type: none"> ● Pass - Select this to allow Netbios name inquiries between the hosts located on both sides of VPN Tunnel. ● Block - Select this to block Netbios name inquiries between remote and local hosts. <p>Multicast via VPN - Some programs might send multicast packets via VPN connection.</p> <ul style="list-style-type: none"> ● Pass - Select this to allow multicast packets to pass through VPN connections. ● Block - Select this to block multicast packets from passing through the VPN connections. This is the default setting.
Subnet	<p>Select a subnet for this VPN profile.</p> <p>Assign Static IP Address -If you would like to assign a static IP address to this user, enter it here.</p>
IKE Authentication Method	<p>All fields in this section, except for Digital Signature (X.509), are applicable to IPSec Tunnels and L2TP connections with IPsec Policy when you specify the IP address of the remote node (Remote Client IP in Specify Remote Node above).</p> <p>Digital Signature (X.509) can be used with IPSec tunnels regardless of the IP address of the remote node is specified or</p>

Item	Description
	<p>not.</p> <p>Pre-Shared Key - Select this checkbox to enable Pre-shared Key function and enter a string of up to 63 characters as the pre-shared key.</p> <p>Digital Signature (X.509) - Select this checkbox to enable X.509 Digital Signature and choose a predefined profile that has been set in VPN and Remote Access >> IPsec Peer Identity.</p>
IPsec Security Method	<p>When the remote node is specified, all fields in this section are required for IPsec Tunnels and L2TP connections with IPsec Policy. Select any combination of Medium, DES, 3DES and AES security methods as desired.</p> <p>Medium-Authentication Header (AH) - Data will be authenticated, but not be encrypted. By default, this option is enabled. You can uncheck it to disable it.</p> <p>High-Encapsulating Security Payload (ESP) - 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.

V-2-3 SSL Portal Online User

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.



Provide SSL VPN

INFO

mike,
(172.17.1.42)
Welcome to DrayTek
SSL VPN!

Timeout after 5 minutes.
[\[Reset\]](#)

Home SSL Web Proxy SSL Tunnel [\[logout\]](#)

Main Page:

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

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

Copyright © 2006, DrayTek Corp. All Rights Reserved.

Next, users can open SSL VPN>> SSL Portal Online User to view logging status of SSL VPN.

SSL VPN >> Online User Status

Refresh Seconds : 10

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 visits 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.

Application Notes

A-1 Vigor Router to Vigor Router – SSL VPN

This document introduces how to establish SSL VPN tunnel between two Vigor Routers.



VPN Server (Dial-in Site) Setup

1. Create a LAN-to-LAN VPN Profile. Go to VPN and Remote Access >> LAN to LAN, click on a profile index to add/edit a profile.

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"/>	---

2. Edit the profile as the following figures.

- (a) Enter Profile Name.
- (b) Enable this profile.
- (c) Set Call Direction as “Dial-in”.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="Server"/> <input checked="" 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 type="radio"/> Both <input type="radio"/> Dial-Out <input checked="" 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 IPsec tunnel alive PING to the IP <input type="text"/>
--	---

- (d) Make sure Allow Dial-in Type has “SSL Tunnel” enabled.
- (e) Enter Username and Password.

3. Dial-In Settings

<p>Allowed Dial-In Type</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input checked="" type="checkbox"/> L2TP with IPsec Policy None <input checked="" type="checkbox"/> SSL Tunnel 	<p>Username <input type="text" value="draytek"/></p> <p>Password(Max 11 char) <input type="password" value="....."/></p> <p>VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off</p> <hr/> <p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p>
---	--

- (f) For Remote Network IP/Mask, enter VPN client's LAN IP and subnet mask.
- (g) Click OK to save the profile.

5. TCP/IP Network Settings

<p>My WAN IP <input type="text" value="0.0.0.0"/></p> <p>Remote Gateway IP <input type="text" value="0.0.0.0"/></p> <p>Remote Network IP <input type="text" value="192.168.2.1"/></p> <p>Remote Network Mask <input type="text" value="255.255.255.0"/></p> <p>Local Network IP <input type="text" value="192.168.1.1"/></p> <p>Local Network Mask <input type="text" value="255.255.255.0"/></p> <p style="text-align: center;"><input type="button" value="More"/></p>	<p>RIP Direction Disable</p> <p>From first subnet to remote network, you have to do</p> <p style="text-align: center;">Route</p> <p><input type="checkbox"/> IPsec VPN with the Same Subnets</p> <hr/> <p><input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)</p>
--	--

- 3. Go to VPN and Remote Access >> Remote Access Control to make sure the SSL VPN Service has enabled.

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

VPN Client (Dial-out Site) Setup

- 4. Create a LAN-to-LAN profile. Go to VPN and Remote Access >> LAN to LAN, click on an available index number.

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"/>	---

5. Edit the VPN profile as the following figures.

- (a) Enter Profile Name.
- (b) Enable this profile.
- (c) Set Call Direction to “Dial-out”.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="Client"/> <input checked="" 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 <small>(for some IGMP,IP-Camera,DHCP Relay..etc.)</small>	Call Direction <input type="radio"/> Both <input checked="" 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 IPsec tunnel alive PING to the IP <input type="text"/>
---	---

- (d) Set Type of Server I am calling to SSL Tunnel.
- (e) Enter Username and Password as the same set in VPN Client in Step 2.
- (f) Enter VPN Server's WAN IP in Server IP/Host Name.

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> PPTP <input type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy <input type="text" value="None"/> <input checked="" type="radio"/> SSL Tunnel Server IP/Host Name for VPN. <small>(such as draytek.com or 123.45.67.89)</small> <input type="text" value="100.100.100.100"/> Server Port (for SSL Tunnel): <input type="text" value="443"/>	Username <input type="text" value="draytek"/> Password(Max 15 char) <input type="text" value="....."/> PPP Authentication <input type="text" value="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 type="text"/> <input type="radio"/> Digital Signature(X.509) Peer ID <input type="text" value="None"/>
---	--

- (g) Enter Remote Network IP/Mask as VPN Server's LAN settings (Note that this has to be the same as Local Network IP/Mask setting in Step 2).
- (h) Click OK to save.

5. TCP/IP Network Settings

My WAN IP <input type="text" value="0.0.0.0"/> Remote Gateway IP <input type="text" value="0.0.0.0"/> <input checked="" type="text" value="192.168.1.1"/> Remote Network Mask <input type="text" value="255.255.255.0"/> Local Network IP <input type="text" value="192.168.2.1"/> Local Network Mask <input type="text" value="255.255.255.0"/> <input type="button" value="More"/>	RIP Direction <input type="text" value="Disable"/> From first subnet to remote network, you have to do <input type="text" value="Route"/> <input type="checkbox"/> IPsec VPN with the Same Subnets <input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)
--	---

Establishing the VPN Tunnel

- To dial the VPN, on VPN Client, go to VPN and Remote Access >> Connection Management, select the profile created previously and click on “Dial”.

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds : 10 ▾ Refresh

General Mode:	(Client) 100.100.100.100 ▾	Dial
Backup Mode:	▾	Dial
Load Balance Mode:	▾	Dial

- If all the credentials are Network administrator may check the VPN that is established and its Up Time from VPN and Remote Access >> Connection Management page.

VPN Connection Status

Current Page: 1

Page No. Go >>

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime	
1 (Server)	SSL Tunnel	100.100.100.100	192.168.2.1/24	103	151	148	1052	0:1:33	Drop

xxxxxxx : Data is encrypted.

xxxxxxx : Data isn't encrypted.

V-3 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.

Web User Interface

VPN and Remote Access
Certificate Management
Local Certificate
Trusted CA Certificate
Certificate Backup
Self-Signed Certificate
VoIP

V-3-1 Local Certificate

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

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

Note:

1. Please setup the "System Maintenance >> **Time and Date**" correctly before signing the local certificate.
2. The Time Zone MUST be setup correctly!!

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"/>
Algorithm	SHA-256 <input type="button" value="v"/>



Info

Please be noted that "Common Name" must be configured with rotuer's WAN IP or domain name.

After clicking GENERATE, the generated information will be displayed on the window below:

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify	
server	/C=TW/ST=Hsinchu/L=Hsinchu/O...	Requesting	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>

Note:

1. Please setup the "System Maintenance >> **Time and Date**" correctly before signing the local certificate.
2. The Time Zone MUST be setup correctly!!

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: 未選擇檔案
 Click [Import](#) to upload the local certificate.

Upload PKCS12 Certificate
 Select a PKCS12 file.
 PKCS12 file: 未選擇檔案
 Password:
 Click [Import](#) to upload the PKCS12 file.

Upload Certificate and Private Key
 Select a certificate file and a matchable Private Key.
 Certificate file: 未選擇檔案
 Key file: 未選擇檔案
 Password:
 Click [Import](#) to upload the local certificate and private key.

Available settings are explained as follows:

Item	Description																
Upload Local Certificate	<p>It allows users to import the certificate which is generated by Vigor router and signed by CA server.</p> <p>If you have done well in certificate generation, the Status of the certificate will be shown as “OK”.</p> <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> <p style="text-align: center; color: red;">Import X509 Local Certificate</p> <p style="text-align: center;">Congratulation!</p> <p style="text-align: center;">Local Certificate has been imported successfully.</p> <p style="text-align: center;">Please click <input type="button" value="Back"/> to view the certificate.</p> </div> <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> <p style="text-align: center; color: red;">X509 Local Certificate Configuration</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Name</th> <th style="text-align: left;">Subject</th> <th style="text-align: left;">Status</th> <th style="text-align: left;">Modify</th> </tr> </thead> <tbody> <tr> <td>draytekdemo</td> <td>/O=Draytek/OU=Draytek Sales/...</td> <td>OK</td> <td><input type="button" value="View"/> <input type="button" value="Delete"/></td> </tr> <tr> <td>---</td> <td>---</td> <td>---</td> <td><input type="button" value="View"/> <input type="button" value="Delete"/></td> </tr> <tr> <td>---</td> <td>---</td> <td>---</td> <td><input type="button" value="View"/> <input type="button" value="Delete"/></td> </tr> </tbody> </table> <p style="text-align: center;"> <input type="button" value="GENERATE"/> <input type="button" value="IMPORT"/> <input type="button" value="REFRESH"/> </p> </div>	Name	Subject	Status	Modify	draytekdemo	/O=Draytek/OU=Draytek Sales/...	OK	<input type="button" value="View"/> <input type="button" value="Delete"/>	---	---	---	<input type="button" value="View"/> <input type="button" value="Delete"/>	---	---	---	<input type="button" value="View"/> <input type="button" value="Delete"/>
Name	Subject	Status	Modify														
draytekdemo	/O=Draytek/OU=Draytek Sales/...	OK	<input type="button" value="View"/> <input type="button" value="Delete"/>														
---	---	---	<input type="button" value="View"/> <input type="button" value="Delete"/>														
---	---	---	<input type="button" value="View"/> <input type="button" value="Delete"/>														
Upload PKCS12 Certificate	<p>It allows users to import the certificate whose extensions are usually .pfx or .p12. And these certificates usually need passwords.</p> <p>Note: PKCS12 is a standard for storing private keys and certificates securely. It is used in (among other things) Netscape and Microsoft Internet Explorer with their import and export options.</p>																
Upload Certificate and	It is useful when users have separated certificates and private																

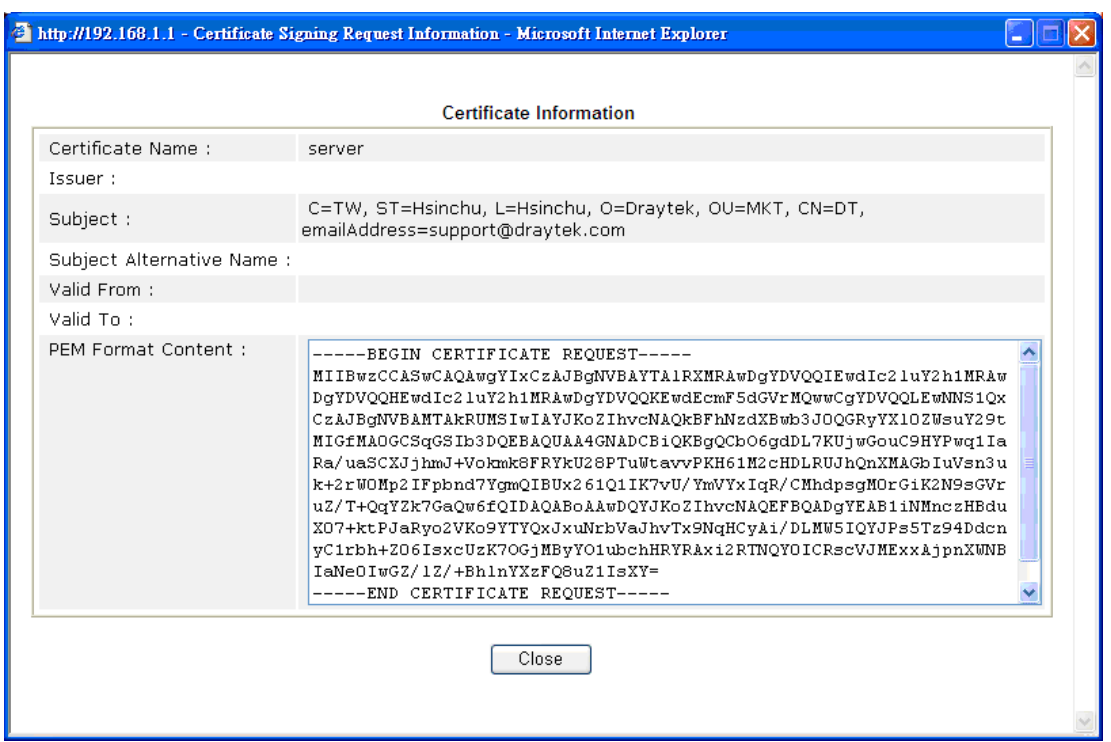
Private Key	keys. And the password is needed if the private key is encrypted.
-------------	---

REFRESH

Click this button to refresh the information listed below.

View

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



Info

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.

Delete

Click this button to remove the selected certificate.

V-3-2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate. In addition, you can build a RootCA certificate if required.

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.



Info

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 Root CA.

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

Creating a RootCA

Click Create to open the following page. 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 >> Root CA Certificate

Generate Root CA

Certificate Name	Root CA
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"/>
Algorithm	SHA-256 <input type="button" value="v"/>

Importing a Trusted CA

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.

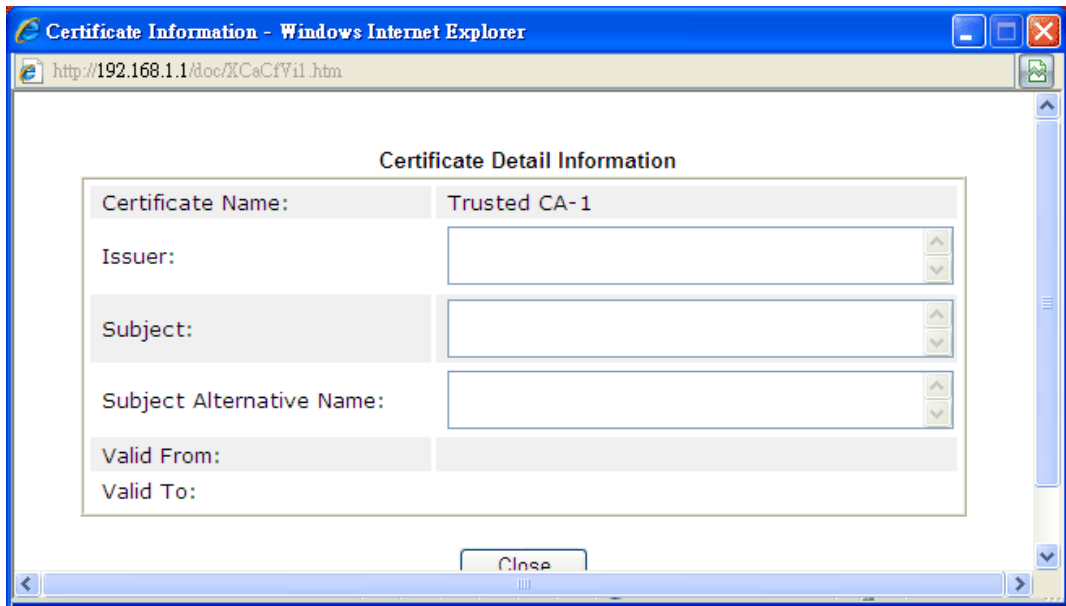
Certificate Management >> Trusted CA Certificate

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.



V-3-3 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 Confirm password.

Also, you can use Restore to retrieve these two settings to the router whenever you want.

Certificate Management >> Certificate Backup

Certificate Backup / Restoration

Backup

Encrypt password:

Confirm password:

Click to download certificates to your local PC as a file.

Restoration

Select a backup file to restore.

未選擇檔案。

Decrypt password:

Click to upload the file.

V-3-4 Self-Signed Certificate

A self-signed certificate is a *unique* identification for the device (e.g., Vigor router) which generates the certificate by itself to ensure the router security. Such self-signed certificate is signed with its own private key.

The self-signed certificate will be applied in SSL VPN, HTTPS, and so on. In addition, it can be created for free by using a wide variety of tools.

Certificate Management >> Self-Signed Certificate

Self-Signed Certificate Information

Certificate Name :	self-signed
Issuer :	C=TW, ST=HsinChu, L=HuKou, O=DrayTek Corp., OU=DrayTek Support, CN=Vigor Router
Subject :	C=TW, ST=HsinChu, L=HuKou, O=DrayTek Corp., OU=DrayTek Support, CN=Vigor Router
Subject Alternative Name :	
Valid From :	Oct 16 10:10:09 2018 GMT
Valid To :	Oct 15 10:10:09 2048 GMT
PEM Format Content :	<pre>-----BEGIN CERTIFICATE----- MIIDijCCAnKgAwIBAgIJAOajSsCMQdP4MAOGCSqGSIb3DQEBCwUAMHgx CzAJBgNV BAYTA1RXMRAdDgYDVQQIDAdIc2luQ2h1MQ4wDAYDVQQHDAVIdUtvvdTEWMBQGA1UE CgwNRHJheVRlayBDb3JwLjEYMBYGA1UECwwPRHJheVRlayBTdXBw3JOMRUwEwYD VQDDAxWwWdvc iBSb3V0ZXIwHhcNMTgxMDE2MTAxMDA5WheNNDgxMDE1MTAxMDA5 WjB4MQswCQYDVQQGEwJUVzZEQMA4GA1UECAwHSHNpbkNodTEOMAwGA1UEBwwFSHVl b3UxZjJhUWVzZG9yYX1UZ2VzZG9yYX1UZ2VzZG9yYX1UZ2VzZG9yYX1UZ2VzZG9y cG9yYDDEVMBGA1UEAwwMVmlnb3IgdW91dGVyMIIBIjANBgkqhkiG9wOBAQEFAAOC AQSA MIIBCgKCAQE Auec5f8WeOSDRs1SfgwMLRvIgsUTKnv6a7aVzThuD+9OG13sd 3BQCRaA7Svmp1Ixu86a6jTbJ1XOtcF7jEvO7kZXLWb4XcZmI IKFYD8axK57oKFW b/wypBSZDz9++52kGiJeH4fmKLj3iKUES/f48DR91PA6L1051kMEaXBgkf/bBRCs dZOEjNqmgwVoxK1FAKYXO2f9pyOJOUtBwdfJHLNLHBr781BVORdOk2ES3C+dft gy39Hc8jwIwDvGzj9CdcMRz2GEhoLuM+IajvkwUsAY61Q1vLqU1Cm6x26t5rg3W NHkKm0WzcBh4tFDHIWQsc0IQKswVucHkLhVMCwIDAQABoxcwFTATBGNVHUEDDAK BggrBgEFBQcDATABgkqhkiG9wOBAQsFAAOC AQEARBWc//KcE57QgNCfoie1bEwI /Oo/pm2NzsygXecf9mMbs5HNqThc/a9KD44ONfYajHXIP3ttmX4D8qdIAXMeB3Un Xqm1Up7rhe9tVymdq/ j694jtGeEVisA1ZsRPzjVD9JR3wuBOr4//1CuNfZRSygd7 8uWQe4kpo31xhZ/ j8Y4IPkMo9MNgrjCrB8WR12NBOKChVBGk3rvQOpYENid6X5u y1B1CKWf4BOKZs1DeCYDsYrSFrzYwhZ3QdrfCgvpZ/AaY9UnUKqrOuXQ2e2UorR2 b+EAGloVbKsfggnLdLeMhT/v6TnWgtTLiTXobmzHLscnswwRacnwTsTzHuFtBA== -----END CERTIFICATE-----</pre>

Note:

1. Please setup the **System Maintenance >> Time and Date** correctly before you try to regenerate a self-signed certificate!!
2. The Time Zone MUST be setup correctly!!

Regenerate

This page is left blank.

Part VI Security



Firewall



CSM

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.

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

VI-1 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:

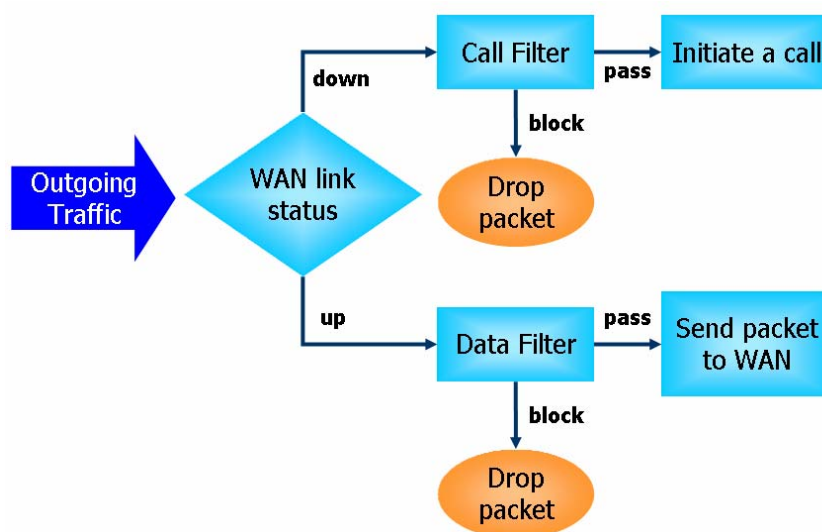
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

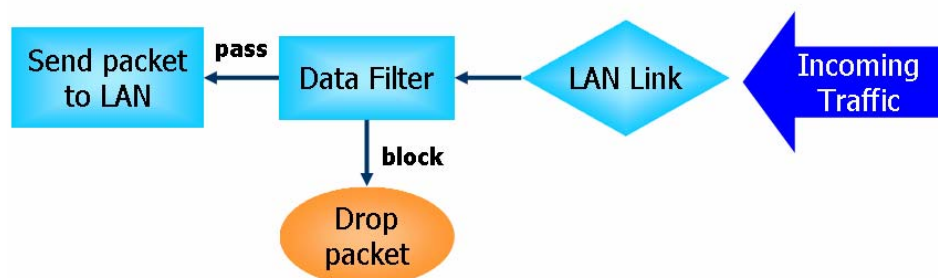
IP Filters

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 only examines the header information also monitors 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.

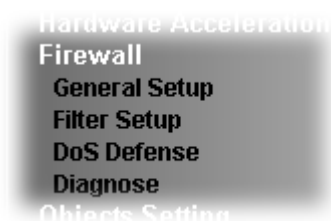
Also the Vigor router monitors the traffic. Any abnormal traffic flow violating the pre-defined parameter, such as the number of thresholds, is identified as an attack and the Vigor router will activate its defense mechanism to mitigate in a real-time manner.

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 | |

Web User Interface

Below shows the menu items for Firewall.



VI-1-1 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	<input checked="" type="radio"/> Enable Start Filter Set: Set#1 ▼ <input type="radio"/> Disable
Data Filter	<input checked="" type="radio"/> Enable Start Filter Set: Set#2 ▼ <input type="radio"/> Disable
<input checked="" type="checkbox"/> Always pass inbound fragmented large packets (required for certain games and streaming)	
<input checked="" type="checkbox"/> Enable Strict Security Firewall	
Block routing connections initiated from WAN <input type="checkbox"/> IPv4 <input checked="" type="checkbox"/> IPv6	

Note:

Packets are filtered by firewall functions in the following order:
1.Data Filter Sets and Rules 2.Block routing connections initiated from WAN 3.Default Rule

OK Cancel

Backup Firewall : <input type="button" value="Backup"/>	Restore Firewall: <input type="button" value="選擇檔案"/> 未選擇任何檔案 <input type="button" value="Restore"/>
---	--

Note:

This will not backup the detail setting of Quality of Service and Schedule.

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.
Always pass inbound fragmented large packets...	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 "Always pass inbound fragmented large packets...". By checking this box, you can play these kinds of on-line games. If security concern is in higher priority, you cannot enable "Always pass inbound fragmented large packets...".
Enable Strict Security Firewall	For the sake of security, the router will execute strict security checking for data transmission. Such feature is enabled in default. All the packets, while transmitting through Vigor router, will be filtered by firewall. If the firewall system (e.g., content filter server) does not make any response (pass or block) for these packets, then the router's firewall will block the packets directly.
Block routing packet from WAN	Usually, IPv6 network sessions/traffic from WAN to LAN will be accepted by IPv6 firewall in default. IPv6 - To prevent remote client accessing into the PCs on LAN, check the box to make the packets (routed from WAN to LAN) via IPv6 being blocked by such router. It is effective only for the packets routed but not for packets translated by NAT. IPv4 - To prevent remote client accessing into the PCs on LAN, check the box to make the incoming packets via IPv4 being blocked by such router. It is effective only for the packets routed but not for packets translated by NAT.
Backup Firewall	Click Backup to save the firewall configuration.
Restore Firewall	Click Select to choose a firewall configuration file. Then click Restore to apply the file.

Default Rule Page

Such page allows you to choose filtering profiles including QoS, Load-Balance policy, WCF, APP Enforcement, URL Content Filter, 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="button" value="v"/>	<input type="checkbox"/>
Sessions Control	0 / 50000 <input type="text"/>	<input type="checkbox"/>
Quality of Service	None <input type="button" value="v"/>	<input type="checkbox"/>
APP Enforcement	None <input type="button" value="v"/>	<input type="checkbox"/>
URL Content Filter	None <input type="button" value="v"/>	<input type="checkbox"/>
Web Content Filter	None <input type="button" value="v"/>	<input type="checkbox"/>
DNS Filter	None <input type="button" value="v"/>	<input type="checkbox"/>

Advance Setting

Backup Firewall :

Restore Firewall: 未選擇檔案

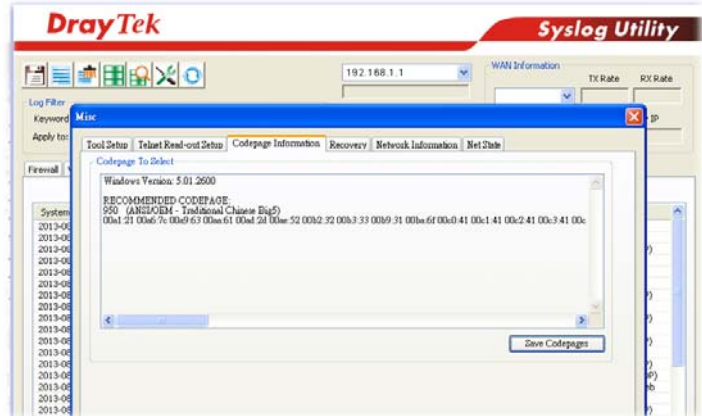
Note:

This will not backup the detail setting of Quality of Service and Schedule.

Available settings are explained as follows:

Item	Description
Filter	Select Pass or Block for the packets that do not match with the filter rules.
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.
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	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) 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.
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 style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>Advance Setting</p> <p>Codepage: <input type="text" value="ANSI(1252)-Latin I"/></p> <p>Window size: <input type="text" value="65535"/></p> <p>Session timeout: <input type="text" value="1440"/> Minute</p> </div> <p style="text-align: center;"> <input type="button" value="OK"/> <input type="button" value="Close"/> </p> <p>Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtain 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>



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.

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

VI-1-2 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 filter rule.

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1
 Comments :

Rule	Active	Comments	Direction	Src IP	Dst IP	Service Type	Action	CSM	Move Up	Move Down
1	<input checked="" type="checkbox"/>	Block NetBios	LAN/RT/VPN -> WAN	Any	Any	TCP/UDP, Port: from 137~139 to any	Block Immediately			Down
2	<input type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
3	<input type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
4	<input type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
5	<input type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
6	<input type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
7	<input type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	

Filter Set [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) Next Filter Set

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

Available settings are explained as follows:

Item	Description
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.
Direction	Display the direction of packet flow
Src IP Dst IP	Display the source IP address and destination IP address of the rule.

Service Type	Display the protocol setting with source port and destination port value.
Action	Display the action taken when packets match the rule.
CSM	Display the CSM profile name used by such rule.
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.
Wizard Mode	Allow to configure frequently used settings of filter rule via three setting pages
Advance Mode	Allow to configure detailed settings of filter rule in one page.

To use Wizard Mode, simple do the following steps:

1. Click the Wizard Mode radio button.
2. Click one of the index number links (e.g., Index 2) to access into the following page.

Firewall >> Edit Filter Set >> Edit Filter Rule Wizard

Filter Set 1 Rule 2

Firewall Rule applies to packets that meet the following criteria

Comments:

Direction: LAN/RT/VPN -> WAN

Source IP: Any Address

Start IP Address:

End IP Address:

Subnet Mask:

Destination IP: Any Address

Start IP Address:

End IP Address:

Subnet Mask:

Protocol: Any

Source Port: = ~

Destination Port: = ~

Available settings are explained as follows:

Item	Description
Comments	Enter filter set comments/description. Maximum length is 14- character long.
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 style="border: 1px solid black; padding: 5px; margin: 5px 0;"> LAN/RT/VPN -> WAN <input type="button" value="v"/> LAN/RT/VPN -> WAN WAN -> LAN/RT/VPN LAN/RT/VPN -> LAN/RT/VPN </div> Note: RT means routing domain for 2nd subnet or other

	LAN.
Source/Destination IP	To set the IP address manually, please choose Any Address/Single Address/Range Address/Subnet Address as the Address Type and Enter them in this dialog.
Protocol	Specify the protocol(s) which this filter rule will apply to.
Source Port / Destination Port	<p>(=) - when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type.</p> <p>(!=) - when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.</p> <p>(>) - the port number greater than this value is available.</p> <p>(<) - the port number less than this value is available for this profile.</p>

3. Click Next to get the following page.

Firewall >> Edit Filter Set >> Edit Filter Rule Wizard

Filter Set 1 Rule 2

Based on the settings in the previous pages, we guess you want to have: **Pass**
The current setting is :

Pass Immediately

APP Enforcement:

URL Content Filter:

Web Content Filter:

DNS Filter:

Block Immediately

4. After configuring the above settings, click Next to get the summary page for reference.

Filter Set 1 Rule 2 Configuration Summary

Comments :	test
Direction	
LAN/RT/VPN -> WAN	
Criteria	
Source IP	0.0.0.0
Destination IP	Any
Protocol	Any
More options	
Pass Immediately	
APP Enforcement :	None
URL Content Filter :	None
Web Content Filter :	None
DNS Filter :	None

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

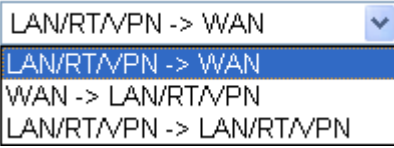
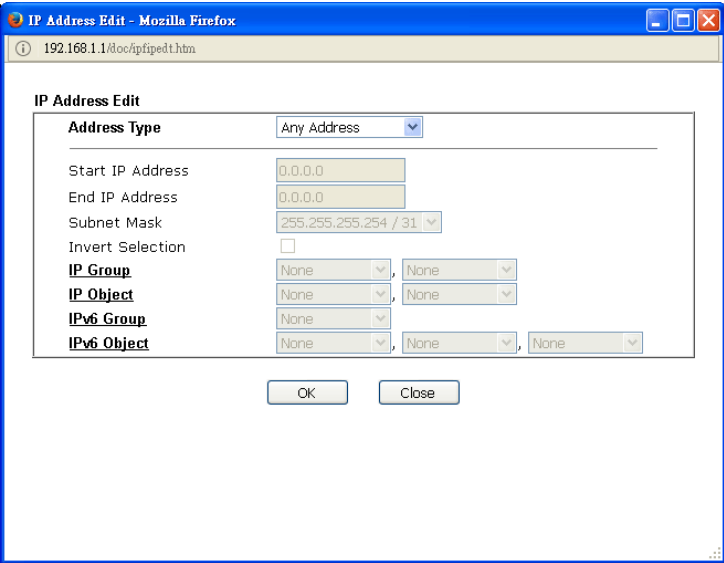
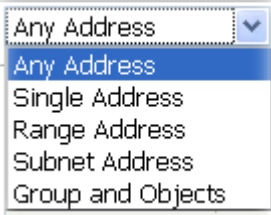
To use Advance Mode, do the following steps:

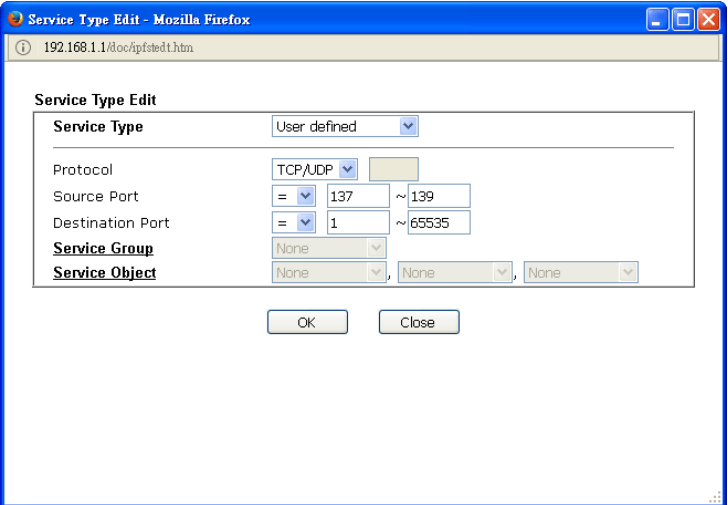
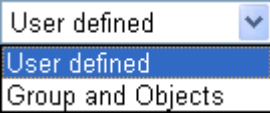
1. Click the Advance Mode radio button.
2. Click one of the index number linke (e.g., Index 2) to access into the following page.

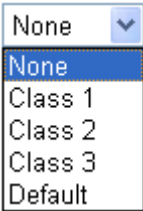
Filter Set 1 Rule 1

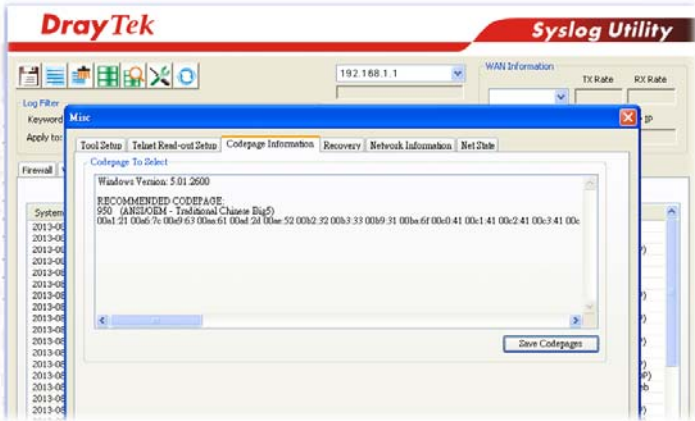
<input checked="" type="checkbox"/> Enable		
Comments	Block NetBios	
Schedule Profile	None	None
	None	None
	<input type="checkbox"/> Clear sessions when schedule is ON	
Direction		
	LAN/RT/VPN -> WAN	<input type="button" value="Advanced"/>
Source IP	Any	<input type="button" value="Edit"/>
Destination IP	Any	<input type="button" value="Edit"/>
Service Type	TCP/UDP, Port: from 137~139 to any	<input type="button" value="Edit"/>
Fragments	Don't Care	
Application	Action/Profile	Syslog
Filter	Block Immediately	<input type="checkbox"/>
Branch to Other Filter Set	None	
Sessions Control	0 / 50000	<input type="checkbox"/>
MAC Bind IP	Non-Strict	<input type="checkbox"/>
Quality of Service	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	<input type="button" value="Edit"/>	

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable the filter rule.
Comments	Enter filter set comments/description. Maximum length is 14-character long.
Schedule Profile	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	<p>Set the direction of packet flow. It is for Data Filter only. For the Call Filter, this setting is not available since Call Filter is only applied to outgoing traffic.</p>  <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>  <p>To set the IP address manually, please choose Any Address/Single Address/Range Address/Subnet Address/Group and Objects as the Address Type and Enter them in this dialog. For example, if you want to use the IP range from defined groups or objects, please choose Group and Objects as the Address Type.</p>  <p>From the IP Group drop down list, choose the one that you</p>

	<p>want to apply. Or use the IP Object drop down list to choose the object that you want.</p>
<p>Service Type</p>	<p>Click Edit to access into the following dialog to choose a suitable service type.</p>  <p>To set the service type manually, please choose User defined as the Service Type and Enter 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.</p>  <p>Protocol - Specify the protocol(s) which this filter rule will apply to.</p> <p>Source/Destination Port -</p> <p>(=) - when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type.</p> <p>(!=) - when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.</p> <p>(>) - the port number greater than this value is available.</p> <p>(<) - the port number less than this value is available for this profile.</p> <p>Service Group/Object - Use the drop down list to choose the one that you want.</p>
<p>Fragments</p>	<p>Specify the action for fragmented packets. And it is used for Data Filter only.</p> <ul style="list-style-type: none"> ● 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	<p>Specifies the action to be taken when packets match the rule.</p> <p>Block Immediately - Packets matching the rule will be dropped immediately.</p> <p>Pass Immediately - Packets matching the rule will be passed immediately.</p> <p>Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped.</p> <p>Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through.</p>
Branch to other Filter Set	<p>If the packet matches the filter rule, the next filter rule will branch to the specified filter set. Select next filter rule to branch from the drop-down menu. Be aware that the router will apply the specified filter rule for ever and will not return to previous filter rule any more.</p>
Sessions Control	<p>The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.</p>
MAC Bind IP	<p>Strict - Make the MAC address and IP address settings configured in IP Object for Source IP and Destination IP are 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> 
APP Enforcement	<p>Select an APP Enforcement profile for global IM/P2P application blocking. If there is no profile for you to select, please choose [Create New] from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the APP Enforcement profile selected here. For detailed information, refer to the section of APP Enforcement profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p>
URL Content Filter	<p>Select one of the URL Content Filter profile settings (created in CSM>> URL Content Filter) for applying with this router. Please set at least one profile for choosing in CSM>> URL Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for URL Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p>
Web Content Filter	<p>Select one of the Web Content Filter profile settings (created in CSM>> Web Content Filter) for applying with this router. Please set at least one profile for anti-virus in</p>

	<p>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) 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.</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 >> Edit Filter Set >> Edit Filter Rule</p> <hr/> <p>Filter Set 1 Rule 1</p> <p>Advance Setting</p> <p>Codepage: ANSI(1252)-Latin I</p> <p>Window size: 65535</p> <p>Session timeout: 1440 Minute</p> <p>DrayTek Banner: <input checked="" type="checkbox"/></p> <p>Strict Security Checking</p> <p><input type="checkbox"/> APP Enforcement</p> <p>OK Close</p> <p>Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage.</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>  <p>Window size - It determines the size of TCP protocol (0-65535). The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper.</p> <p>Session timeout-Setting timeout for sessions can make the best utilization of network resources. However, Queue</p>

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.

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.

VI-1-3 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.

V-1-3-1 DoS Defense

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

Firewall >> Defense Setup

DoS Defense
Spoofing Defense

DoS defense

Enable DoS Defense
 Select All
White/Black List Option
Log: Enable

<input type="checkbox"/> Enable SYN flood defense	Threshold	<input style="width: 50px;" type="text" value="2000"/>	packets / sec
	Timeout	<input style="width: 50px;" type="text" value="10"/>	sec
<input type="checkbox"/> Enable UDP flood defense	Threshold	<input style="width: 50px;" type="text" value="2000"/>	packets / sec
	Timeout	<input style="width: 50px;" type="text" value="10"/>	sec
<input type="checkbox"/> Enable ICMP flood defense	Threshold	<input style="width: 50px;" type="text" value="250"/>	packets / sec
	Timeout	<input style="width: 50px;" type="text" value="10"/>	sec
<input type="checkbox"/> Enable Port Scan detection	Threshold	<input style="width: 50px;" type="text" value="2000"/>	packets / sec

Block IP options
 Block Land
 Block Smurf
 Block trace route
 Block SYN fragment
 Block Fraggle Attack

Block TCP flag scan
 Block Tear Drop
 Block Ping of Death
 Block ICMP fragment
 Block Unassigned Numbers

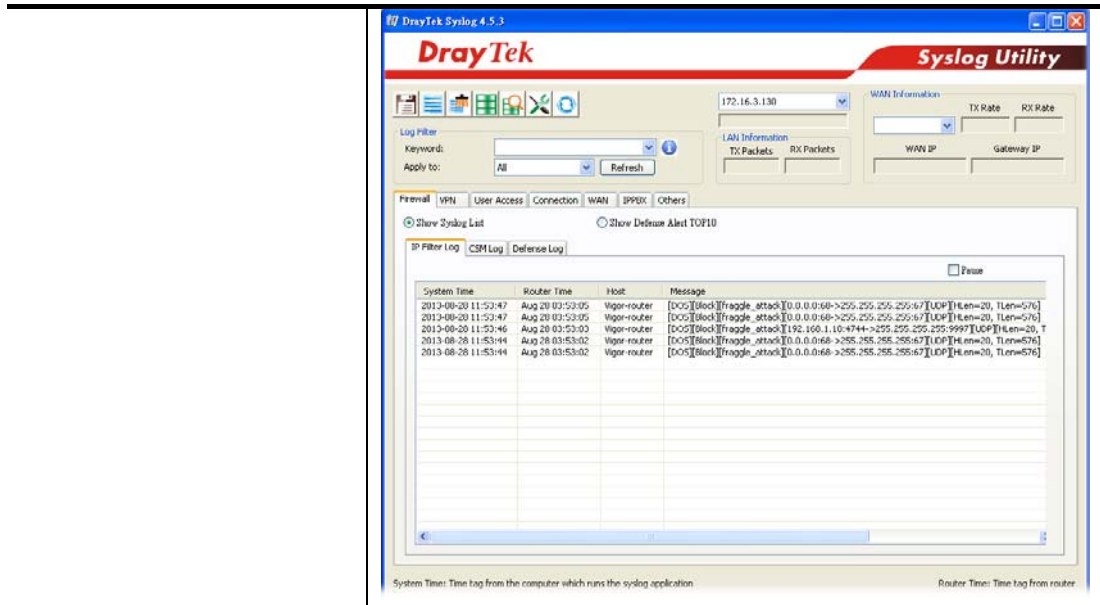
OK
Clear All
Cancel

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 means, when 2000 packets per second received, they will be regarded as “attack event” and the session will be paused for 10 seconds.</p>
Enable ICMP flood defense	<p>Check the box to activate the ICMP flood defense function. Similar to the UDP flood defense function, once if the Threshold of ICMP packets from Internet has exceeded the defined value, the router will discard the ICMP echo requests coming from the Internet.</p> <p>The default setting for threshold and timeout are 250 packets per second and 10 seconds, respectively. That means, when 250 packets per second received, they will be regarded as “attack event” and the session will be paused for 10 seconds.</p>
Enable PortScan detection	<p>Port Scan attacks the Vigor router by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the port-scanning Threshold rate, the Vigor router will send out a warning.</p> <p>By default, the Vigor router sets the threshold as 2000 packets per second. That means, when 2000 packets per second received, they will be regarded as “attack event”.</p>
Block IP options	<p>Check the box to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messages...etc. An eavesdropper outside might learn the details of your private networks.</p>
Block Land	<p>Check the box to enforce the Vigor router to defend 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 route	<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 coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.</p>		
Block TCP flag scan	<p>Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include <i>no flag scan</i>, <i>FIN without ACK scan</i>, <i>SYN FINscan</i>, <i>Xmas scan</i> and <i>full Xmas scan</i>.</p>		
Block Tear Drop	<p>Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.</p>		
Block Ping of Death	<p>Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.</p>		
Block ICMP Fragment	<p>Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.</p>		
Block Unassigned Numbers	<p>Check the box to activate the 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.</p>		
Warning Messages	<p>We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client.</p> <p>All the warning messages related to DoS Defense will be sent to user and user can review it through Syslog daemon. Look for the keyword DoS in the message, followed by a name to indicate what kind of attacks is detected.</p> <p>System Maintenance >> SysLog / Mail Alert Setup</p> <div style="border: 1px solid black; padding: 5px;"> <p>SysLog / Mail Alert Setup</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; vertical-align: top;"> <p>SysLog Access Setup</p> <p><input checked="" type="checkbox"/> Enable</p> <p>Syslog Save to:</p> <p><input checked="" type="checkbox"/> Syslog Server</p> <p><input type="checkbox"/> USB Disk</p> <p>Router Name <input type="text" value="DrayTek"/></p> <p>Server IP/Hostname <input type="text"/></p> <p>Destination Port <input type="text" value="514"/></p> <p>Mail Syslog <input type="checkbox"/> Enable</p> <p>Enable syslog message:</p> <p><input checked="" type="checkbox"/> Firewall Log</p> <p><input checked="" type="checkbox"/> VPN Log</p> <p><input checked="" type="checkbox"/> User Access Log</p> <p><input checked="" type="checkbox"/> Call Log</p> <p><input checked="" type="checkbox"/> WAN Log</p> <p><input checked="" type="checkbox"/> Router/DSL information</p> <p><input checked="" type="checkbox"/> WLAN Log</p> </td> <td style="width: 50%; vertical-align: top;"> <p>Mail Alert Setup</p> <p><input checked="" type="checkbox"/> Enable <input type="button" value="Send a test e-mail"/></p> <p>SMTP Server <input type="text"/></p> <p>SMTP Port <input type="text" value="25"/></p> <p>Mail To <input type="text"/></p> <p>Return-Path <input type="text"/></p> <p><input type="checkbox"/> Use SSL</p> <p><input type="checkbox"/> Authentication</p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>Enable E-Mail Alert:</p> <p><input checked="" type="checkbox"/> DoS Attack</p> <p><input checked="" type="checkbox"/> APPE</p> <p><input checked="" type="checkbox"/> VPN LOG</p> <p><input type="checkbox"/> APPE Signature</p> <p><input type="checkbox"/> Debug Log</p> </td> </tr> </table> <p>Note:</p> <ol style="list-style-type: none"> 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. <p style="text-align: right;"><input type="button" value="OK"/> <input type="button" value="Clear"/></p> </div>	<p>SysLog Access Setup</p> <p><input checked="" type="checkbox"/> Enable</p> <p>Syslog Save to:</p> <p><input checked="" type="checkbox"/> Syslog Server</p> <p><input type="checkbox"/> USB Disk</p> <p>Router Name <input type="text" value="DrayTek"/></p> <p>Server IP/Hostname <input type="text"/></p> <p>Destination Port <input type="text" value="514"/></p> <p>Mail Syslog <input type="checkbox"/> Enable</p> <p>Enable syslog message:</p> <p><input checked="" type="checkbox"/> Firewall Log</p> <p><input checked="" type="checkbox"/> VPN Log</p> <p><input checked="" type="checkbox"/> User Access Log</p> <p><input checked="" type="checkbox"/> Call Log</p> <p><input checked="" type="checkbox"/> WAN Log</p> <p><input checked="" type="checkbox"/> Router/DSL information</p> <p><input checked="" type="checkbox"/> WLAN Log</p>	<p>Mail Alert Setup</p> <p><input checked="" type="checkbox"/> Enable <input type="button" value="Send a test e-mail"/></p> <p>SMTP Server <input type="text"/></p> <p>SMTP Port <input type="text" value="25"/></p> <p>Mail To <input type="text"/></p> <p>Return-Path <input type="text"/></p> <p><input type="checkbox"/> Use SSL</p> <p><input type="checkbox"/> Authentication</p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>Enable E-Mail Alert:</p> <p><input checked="" type="checkbox"/> DoS Attack</p> <p><input checked="" type="checkbox"/> APPE</p> <p><input checked="" type="checkbox"/> VPN LOG</p> <p><input type="checkbox"/> APPE Signature</p> <p><input type="checkbox"/> Debug Log</p>
<p>SysLog Access Setup</p> <p><input checked="" type="checkbox"/> Enable</p> <p>Syslog Save to:</p> <p><input checked="" type="checkbox"/> Syslog Server</p> <p><input type="checkbox"/> USB Disk</p> <p>Router Name <input type="text" value="DrayTek"/></p> <p>Server IP/Hostname <input type="text"/></p> <p>Destination Port <input type="text" value="514"/></p> <p>Mail Syslog <input type="checkbox"/> Enable</p> <p>Enable syslog message:</p> <p><input checked="" type="checkbox"/> Firewall Log</p> <p><input checked="" type="checkbox"/> VPN Log</p> <p><input checked="" type="checkbox"/> User Access Log</p> <p><input checked="" type="checkbox"/> Call Log</p> <p><input checked="" type="checkbox"/> WAN Log</p> <p><input checked="" type="checkbox"/> Router/DSL information</p> <p><input checked="" type="checkbox"/> WLAN Log</p>	<p>Mail Alert Setup</p> <p><input checked="" type="checkbox"/> Enable <input type="button" value="Send a test e-mail"/></p> <p>SMTP Server <input type="text"/></p> <p>SMTP Port <input type="text" value="25"/></p> <p>Mail To <input type="text"/></p> <p>Return-Path <input type="text"/></p> <p><input type="checkbox"/> Use SSL</p> <p><input type="checkbox"/> Authentication</p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>Enable E-Mail Alert:</p> <p><input checked="" type="checkbox"/> DoS Attack</p> <p><input checked="" type="checkbox"/> APPE</p> <p><input checked="" type="checkbox"/> VPN LOG</p> <p><input type="checkbox"/> APPE Signature</p> <p><input type="checkbox"/> Debug Log</p>		



V-1-3-2 Spoofing Defense

Open Firewall >> Defense Setup and click Spoofing Defense to open the setup page.

Firewall >> Defense Setup

DoS Defense Spoofing Defense

ARP Spoofing Defense

- Block ARP replies with inconsistent source MAC addresses.
- Block ARP replies with inconsistent destination MAC addresses.
- Decline VRRP MAC into ARP table.

IP Spoofing Defense

- Block IP packet from WAN with inconsistent source IP addresses.
- Block IP packet from LAN with inconsistent source IP addresses.

OK Cancel

VI-1-4 Diagnose

The purpose of this function is to test when the router receiving incoming packet, which firewall rule will be applied to that packet. The test result, including firewall rule profile, IP address translation in packet transmission, state of the firewall functions and etc., also will be shown on this page.



Info

The result obtained by using Diagnose is offered for RD debug. It will be different according to actual state such as network connection, LAN/WAN settings and so on.

Firewall >> Diagnose

Mode

ICMP UDP TCP IPv4

Direction

From LAN

Test View



Packet & Payload

Packet	Enable	Direction	Protocol
1	<input checked="" type="checkbox"/>	A->B	UDP:Customize
2	<input checked="" type="checkbox"/>	B->A	UDP:Customize

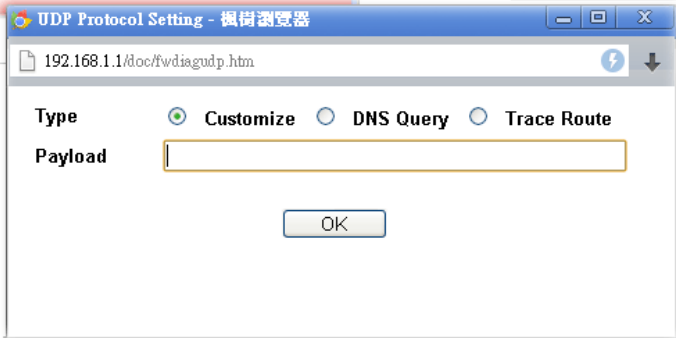
Note:

This is firewall live test which need setup WAN and plug cable in.

Analyze

Available settings are explained as follows:

Item	Description
Mode	To have a firewall rule test, specify the service type (ICMP, UDP, TCP) of the packet and type of the IP address (IPv4/IPv6).
Direction	Set the way (from WAN or from LAN) that Vigor router receives the first packet for test. Different way means the firewall will process the connection initiated from LAN or from WAN.
Test View	This is a dynamic display page. According to the direction specified, test view will display the figure to guide you typing IP address, port number, and MAC address. Later, after clicking the Analyze button, the information for the firewall rule profile and address translation will be shown on this page.
Src IP	Enter the IPv4/IPv6 address of the packet's source.
Src Port	Enter the port number of the packet's source.
Src MAC	Enter the MAC address of the packet's source.

Dst IP	Enter the IPv4/IPv6 address of the packet's destination.
Dst Port	Enter the port number of the packet's destination.
Packet & Payload	<p>In firewall diagnose, two packets belong to one connection. In general, two packets are enough for Vigor router to perform this test.</p> <p>Enable - Check the box to send out the test packet.</p> <p>Direction - The first packet of the firewall test will follow the direction specified above. However, the direction for the second packet might be different. Simply choose the direction (from Computer A to B or from the B to A) for the second packet.</p> <p>Protocol - It displays the mode selected above and the sate. If required, click the mode link to configure advanced setting. The common service type (Customize, Ping, Trace Route / Customize, DNS, Trace Route / Customize, Http(GET) related to that mode (ICMP / UDP / TCP) will be shown on the following dialog box.</p>  <ul style="list-style-type: none"> ● Type - Choose Customize, DNS Query and Trace Route. ● Payload - It is available when Customzie is selected. Simply type 16 HEX characters which represent certain packet (e.g., DNS packet) if you want to set the data transfered with protocol (ICMP/UDP/TCP) which is different to Type setting.
Analyze	Execute the test and analyze the result.

The following figure shows the test result after clicking Analyze. Processing state for the functions (MAC Filter, QoS, User management, etc.) related to the firewall will be displayed by green or red LED.

Firewall >> Diagnose

Mode
 ICMP UDP TCP

Direction

Test View

A

192.168.1.111:22222
->7.7.7.51348

ORIGIN» LAN Firewall WAN1 «REPLY

7.7.7.51348
172.16.2.234:62094<-

B

Status	Packet	Set	Rule	UCF/WCF
Pass	2	default	default	n/a

Packet & Payload

Packet	Enable	Direction	Protocol			
1	<input checked="" type="checkbox"/>	A->B ▼	UDP:Customize			
Acceleration						
2	<input checked="" type="checkbox"/>	B->A ▼	UDP:Customize			
Acceleration						
<input checked="" type="checkbox"/> SESS_CTL	<input checked="" type="checkbox"/> MAC FILTER	<input checked="" type="checkbox"/> PCAP	<input checked="" type="checkbox"/> USER MGT	<input checked="" type="checkbox"/> APPE	<input checked="" type="checkbox"/> UCF	<input checked="" type="checkbox"/> WCF
<input checked="" type="checkbox"/> DNSF	<input checked="" type="checkbox"/> SESS_LMT	<input checked="" type="checkbox"/> BW_LMT	<input checked="" type="checkbox"/> QOS	<input checked="" type="checkbox"/> APP_QOS	<input checked="" type="checkbox"/> HW_ACC	

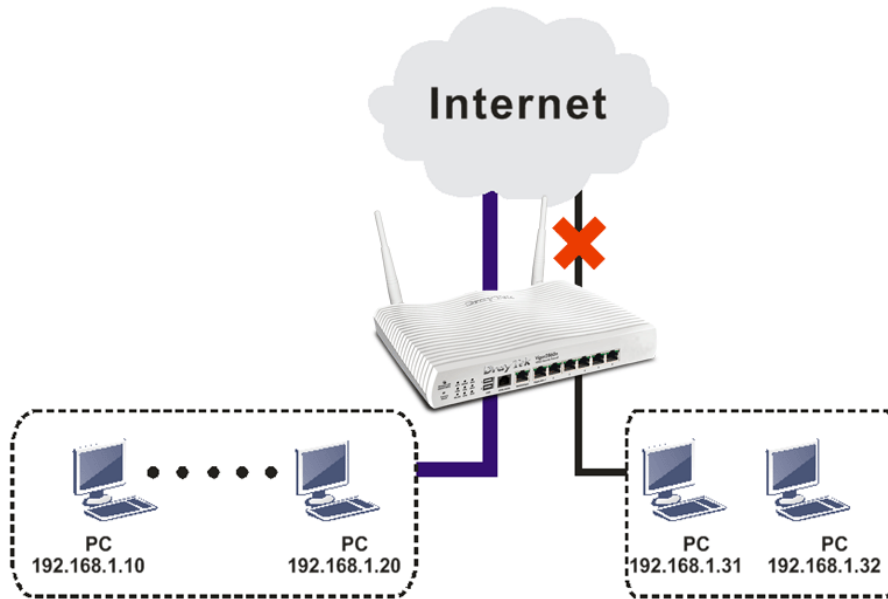
APP: The APP need to check. : The APP is completed.
 APP: The APP doesn't need to check. : The APP is processing.

Note:
 PCAP is "ip pcap" in telnet command.

Application Notes

A-1 How to Configure Certain Computers Accessing to Internet

We can specify certain computers (e.g., 192.168.1.10 ~ 192.168.1.20) accessing to Internet through Vigor router. Others (e.g., 192.168.1.31 and 192.168.1.32) outside the range can get the source from LAN only.



The way we can use is to set two rules under Firewall. For Rule 1 of Set 2 under Firewall>>Filter Setup is used as the default setting, we have to create a new rule starting from Filter Rule 2 of Set 2.

1. Access into the web user interface of Vigor router.
2. Open Firewall>>Filter Setup. Click the Set 2 link and choose the Filter Rule 2 button.

Firewall >> Filter Setup

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

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 2

Comments: Default Data Filter

Rule	Active	Comments	Direction	Src IP	Dst IP	Service Type	Action	CSM	Move Up	Move Down
1	<input checked="" type="checkbox"/>	xNetBios -> DNS	LAN/RT/VPN -> WAN	Any	Any	TCP/UDP, Port: from 137~139 to 53	Block Immediately			Down
2	<input type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
3	<input type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down

3. Check the box of Check to enable the Filter Rule. Enter the comments (e.g., block_all). Choose Block If No Further Match for the Filter setting. Then, click OK.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 2

Check to enable the Filter Rule

Comments: block_all

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

Clear sessions when schedule ON: Enable

Direction: LAN/RT/VPN -> WAN

Source IP: Any [Edit]

Destination IP: Any [Edit]

Service Type: Any [Edit]

Fragments: Don't Care

Application

Filter: Action/Profile: Pass If No Further Match [Syslog:

Branch to Other Filter Set: None

Sessions Control: 0 / 50000



Info

In default, the router will check the packets starting with Set 2, Filter Rule 2 to Filter Rule 7. If Block If No Further Match for is selected for Filter, the firewall of the router would check the packets with the rules starting from Rule 3 to Rule 7. The packets not matching with the rules will be processed according to Rule 2.

4. Next, set another rule. Just open Firewall>>Filter Setup. Click the Set 2 link and choose the Filter Rule 3 button.
5. Check the box of Check to enable the Filter Rule. Enter the comments (e.g., open_ip). Click the Edit button for Source IP.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 3

Check to enable the Filter Rule

Comments: open_ip

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

Clear sessions when schedule ON: Enable

Direction: LAN/RT/VPN -> WAN

Source IP: Any [Edit]

Destination IP: Any [Edit]

Service Type: Any [Edit]

Fragments: Don't Care

Application

Filter: Action/Profile: Block Immediately [Syslog:

- A dialog box will be popped up. Choose Range Address as Address Type by using the drop down list. Type 192.168.1.10 in the field of Start IP, and type 192.168.1.20 in the field of End IP. Then, click OK to save the settings. The computers within the range can access into the Internet.

IP Address Edit

Address Type	Range Address
Start IP Address	192.168.1.10
End IP Address	192.168.1.20
Subnet Mask	0.0.0.0
Invert Selection	<input type="checkbox"/>
IP Group	None
or IP Object	None
or IP Object	None
or IP Object	None
IPv6 Group	None
or IPv6 Object	None
or IPv6 Object	None
or IPv6 Object	None

OK Close

- Now, check the content of Source IP is correct or not. The action for Filter shall be set with Pass Immediately. Then, click OK to save the settings.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 3

<input checked="" type="checkbox"/> Check to enable the Filter Rule	
Comments:	open_ip
Index(1-15) in Schedule Setup:	
Clear sessions when schedule ON:	<input type="checkbox"/> Enable
Direction:	LAN/RT/VPN -> WAN
Source IP:	192.168.1.10~192.168.1.20
Destination IP:	Any
Service Type:	Any
Fragments:	Don't Care
Application	Action/Profile
Filter:	Pass Immediately
Branch to Other Filter Set:	None
	Syslog <input type="checkbox"/>

- Both filter rules have been created. Click OK.

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 2

Comments :

Rule	Active	Comments	Direction	Src IP	Dst IP	Service Type
1	<input checked="" type="checkbox"/>	xNetBios -> DNS	LAN/RT/VPN -> WAN	Any	Any	TCP/UDP, Port: from 137~139 to 53
2	<input checked="" type="checkbox"/>	block_all	LAN/RT/VPN -> WAN	Any	Any	Any
3	<input checked="" type="checkbox"/>	open_ip	LAN/RT/VPN -> WAN	192.168.1.10 ~ 192.168.1.20	Any	Any
4	<input type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any

Now, all the settings are configured well. Only the computers with the IP addresses within 192.168.1.10 ~ 192.168.1.20 can access to Internet.

A-2 How to backup and restore firewall rule and object settings?

Firewall of Vigor router is object-oriented, such as IP object, service type object and keyword object. Since firmware version 3.8.5, Vigor router supports Firewall backup/restore feature. Users can backup firewall settings including object and CSM, then restore it to other routers to make the process of configuration more user-friendly.

After firewall setting is configured on one Vigor router, go to Firewall>>General Setting and click Backup in the end of the page to backup firewall configuration.

Firewall >> General Setup

General Setup

General Setup **Default Rule**

Call Filter Enable Start Filter Set: Set#1

Disable

Data Filter Enable Start Filter Set: Set#2

Disable

Always pass inbound fragmented large packets (required for certain games and streaming)

Enable Strict Security Firewall

Block routing connections initiated from WAN IPv4 IPv6

Backup Firewall : **Backup** **Restore Firewall:** Choose File No file chosen **Restore**

Note:

Packets are filtered by firewall functions in the following order:

- 1.Data Filter Sets and Rules
- 2.Block routing connections initiated from WAN
- 3.Default Rule

OK Cancel

Backup Firewall : **Backup** **Restore Firewall:** Choose File No file chosen **Restore**

Then we can restore these settings on another router on the same page. Also, we can choose what settings to be restored.

Firewall >> Restore

Please choose the items that you want to restore:

Firewall rules User management

Objects Setting

IP Object/Group Service Type Object/Group

IPv6 Object/Group Keyword Object/Group

File Extension Object

CSM

APP Enforcement URL Content Filter

Web Content Filter DNS Filter

Note:

1. Only the selected items will be restored.
2. The detail setting of Quality of Service and Schedule will not be restored.

Select All Clear All OK Close

Backup Firewall : **Backup** **Restore Firewall:** Choose File firewallback...0180828.cfg **Restore**

Note:

This will not backup the detail setting of Quality of Service and Schedule.

The router will show a success message after firewall restoration finishes.

Firewall >> Restore

Congratulation

Firewall rules has been restored successfully.
Please click to return.

Restore Status

Name	Status
Firewall Rule	v
User Management	v
IP Object/Group	v
Service Type Object/Group	v
IPv6 Object/Group	v
File Extension Object	v
Keyword Object/Group	v
URL Content Filter	v
APP Enforcement	v
Web Content Filter	v
DNS Filter	v

VI-2 CSM (Central Security Management)

CSM is an abbreviation of Central 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 reserved 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.



Info

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

Web User Interface

- Object Setting
- CSM**
- APP Enforcement Profile
- APPE Signature Upgrade
- URL Content Filter Profile
- Web Content Filter Profile
- DNS Filter Profile
- APPE Support List
- Bandwidth Management

VI-2-1 APP Enforcement Profile

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

CSM >> APP Enforcement Profile

APP Enforcement Profile Table: [Set to Factory Default](#)

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

Note:

To make APP Enforcement profile effective, please go to [Firewall >> Filter Setup](#) page to create a firewall rule and select the desired profile.

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.

Profile Index : 1

Profile Name:

Category	Application		
Instant Message	<input type="checkbox"/> AIM	<input type="checkbox"/> AIM Login	<input type="checkbox"/> AliWW
<input type="button" value="Select All"/>	<input type="checkbox"/> Ares	<input type="checkbox"/> BaiduHi	<input type="checkbox"/> Facebook
<input type="button" value="Clear All"/>	<input type="checkbox"/> Fetion	<input type="checkbox"/> GaduGadu Protocol	<input type="checkbox"/> Google Hangouts
	<input type="checkbox"/> ICQ	<input type="checkbox"/> iMessage	<input type="checkbox"/> iSpQ
	<input type="checkbox"/> KC	<input type="checkbox"/> LINE	<input type="checkbox"/> Paltalk
	<input type="checkbox"/> PocoCall	<input type="checkbox"/> Qnext	<input type="checkbox"/> Tencent QQ
	<input type="checkbox"/> UC	<input type="checkbox"/> WebIM URLs	<input type="checkbox"/> WhatsApp
	<input type="checkbox"/> Yahoo! Messenger		
VoIP	<input type="checkbox"/> RC Voice	<input type="checkbox"/> Skype	<input type="checkbox"/> TeamSpeak
<input type="button" value="Select All"/>	<input type="checkbox"/> TelTel		
<input type="button" value="Clear All"/>			
P2P	<input type="checkbox"/> BitTorrent	<input type="checkbox"/> eDonkey	<input type="checkbox"/> FastTrack
<input type="button" value="Select All"/>	<input type="checkbox"/> Gnutella	<input type="checkbox"/> OpenFT	<input type="checkbox"/> OpenNap
<input type="button" value="Clear All"/>	<input type="checkbox"/> SoulSeek	<input type="checkbox"/> Ares	<input type="checkbox"/> ClubBox
	<input type="checkbox"/> Huntmine	<input type="checkbox"/> Kuwo	<input type="checkbox"/> Pando
	<input type="checkbox"/> Spotify	<input type="checkbox"/> Vagaa	<input type="checkbox"/> Xunlei(Thunder)
Protocol	<input type="checkbox"/> DNS	<input type="checkbox"/> FTP	<input type="checkbox"/> HTTP
<input type="button" value="Select All"/>	<input type="checkbox"/> IBM DB2	<input type="checkbox"/> IBM Informix	<input type="checkbox"/> IMAP

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
Select All	Click it to choose all of the items in this page.
Clear All	Uncheck all the selected boxes.
Enable	Check the box to select the APP to be blocked by Vigor router.

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.

VI-2-2 APPE Signature Upgrade

The APPE Enforcement Profile adopted by Vigor router will be treated as the APPE signature. DrayTek will periodically upgrade versions for all of the APPs supported by Vigor router. However, it might be inconvenient for users to upgrade the APP version one by one. This feature is specially designed to offer a quick method to execute APP version upgrade. Users can perform the APPE signature upgrade manually or configure the settings on this page to make Vigor router performing the APPE signature automatically.

CSM >> APPE Signature Upgrade

APP Enforcement License [Activate](#)
 [Status: **Inactivated**]

Upgrade Setting

APPE Module Version: **10.14** New version from the Internet: -- [Download](#)
 Upgrade via interface: auto-selected ▾ (Waiting for WAN connection...)

Setup Download Server	<input type="text" value="auto-selected"/>	Find more
Signature authentication / download message <div style="border: 1px solid gray; padding: 5px; font-family: monospace; font-size: small;"> [2000-01-01 00:00:00] Load APPE signature failed. System will use APPE default signature. </div>		

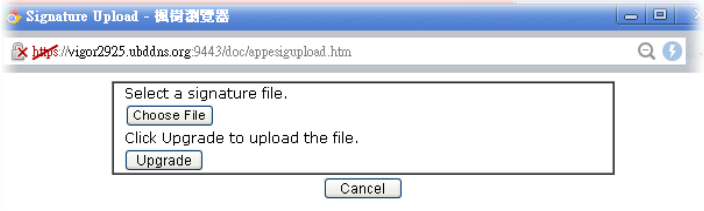
Upgrade Manually	Import
-------------------------	------------------------

Upgrade Automatically			
<input type="checkbox"/> Scheduled Update			
<input checked="" type="radio"/> Every:	<input type="text" value="1"/> (hour)	<input type="text" value="00"/> (minutes after the hour)	
<input type="radio"/> Daily:	<input type="text" value="0"/> (hour)	<input type="text" value="00"/> (minute)	
<input type="radio"/> Weekly:	<input type="text" value="Sunday"/> (day)	<input type="text" value="0"/> (hour)	<input type="text" value="00"/> (minute)

[OK](#)

Available settings are explained as follows:

Item	Description
Upgrade Setting	<p>APPE Module Version - Display current version status of APPE signature.</p> <p>New version from the Internet - Download button is available only when Vigor router detects new APPE version. After clicking it, a dialog will appear with information added to such new version. Click OK to exit the dialog and start the signature upgrade.</p> <p>Upgrade via interface - Choose one of the WAN interfaces as a channel for APPE signature upgrade.</p>
Setup Download Server	<p>Specify the download server by typing the URL of the server located. Or you can click Find more link to search the one you want.</p> <p>Signature authentication/download message - Display the status of APPE Signature Upgrade.</p>
Upgrade Manually	<p>Import - Click this button to open the following page. Press Choose File to locate the signature file which downloaded from MyVigor portal or FTP server previously. Then, click</p>

	<p>Upgrade and wait for the system completing the process.</p> 
Upgrade Automatically	<p>Scheduled Update - Check the box to make Vigor router upgrading the APPE signature based on the schedule configured here.</p>

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

VI-2-3 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.



URL Content Filter Profile Table:

[Set to Factory Default](#)

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

Note:

To make URL Content Filter profile effective, please go to **Firewall >> Filter Setup** page to create a firewall rule and select the desired profile.

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	You can Enter the message manually for your necessity. Default Message - You can Enter the message manually for your necessity or click this button to get the default message which will be displayed on the field of Administration Message.

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

CSM >> URL Content Filter Profile

Profile Index: 1

Profile Name:

Priority: Log:

1.URL Access Control

Enable URL Access Control Prevent web access from IP address

Action:

Exception List

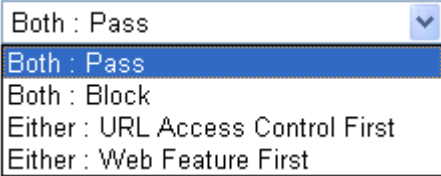
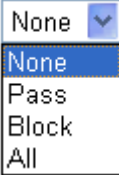
2.Web Feature

Enable Web Feature Restriction

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

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
Priority	<p>It determines the action that this router will apply.</p> <p>Both: Pass - The router will let all the packages that match with the conditions specified in URL Access Control and Web Feature below passing through. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.</p> <p>Both: Block -The router will block all the packages that match with the conditions specified in URL Access Control and Web Feature below. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.</p> <p>Either: URL Access Control First - When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for URL first, then Web feature second.</p> <p>Either: Web Feature First -When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router 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.</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> 
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</p>

properly on a web page that you visited before.

Action - This setting is available only when Either : URL Access Control First or Either : Web Feature First is selected.

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

Exception List - Specify the object profile(s) as the exception list which will be processed in an opposite manner to the action selected above.

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

Object/Group Edit

<u>Keyword Object</u>	None ▾
or Keyword Object	None ▾
or Keyword Object	None ▾
or Keyword Object	None ▾
or Keyword Object	None ▾
or Keyword Object	None ▾
or Keyword Object	None ▾
or Keyword Object	None ▾
or <u>Keyword Group</u>	None ▾
or Keyword Group	None ▾
or Keyword Group	None ▾
or Keyword Group	None ▾
or Keyword Group	None ▾
or Keyword Group	None ▾
or Keyword Group	None ▾
or Keyword Group	None ▾

OK Close

Web Feature

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

Action - This setting is available only when Either: URL Access Control First or Either: Web Feature First is selected.

- *Pass* - Allow accessing into the corresponding webpage with the keywords listed on the box below.
- *Block* - Restrict accessing into the corresponding webpage with the keywords listed on the box below. If the web pages do not match with the 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.



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.

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

VI-2-4 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.

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.



Info 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.

Info 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: **Activated**] [Provider: Cyren] [Start Date: 2019-02-01 Expire Date: 2019-03-03]

Setup Query Server	<input type="text" value="auto-selected"/>	Find more
Setup Test Server	<input type="text" value="auto-selected"/>	Find more
Look up category by URL, or report inappropriate categorization.		

Web Content Filter Profile Table:

Cache : | [Set to Factory Default](#)

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

Note:

To make Web Content Filter profile effective, please go to [Firewall >> Filter Setup](#) page to create a firewall rule and select the desired profile.

Administration Message (Max 255 characters)

[Default Message](#)

```
<body><center><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:

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

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.
Cache	<p>None - the router will check the URL that the user wants to access via WCF precisely, however, the processing rate is normal. Such item can provide the most accurate URL matching.</p> <p>L1 - the router will check the URL that the user wants to access via WCF. If the URL has been accessed previously, it will be stored in the router to be accessed quickly if required. Such item can provide accurate URL matching with faster rate.</p> <p>L2 - the router will check the URL that the user wants to access via WCF. If the data has been accessed previously, the IP addresses of source and destination IDs will be memorized for a short time (about 1 second) in the router. When the</p>

	<p>user tries to access the same destination ID, the router will check it by comparing the record stored. If it matches, the page will be retrieved quickly. Such item can provide URL matching with the fastest rate.</p> <p>L1+L2 Cache - the router will check the URL with fast processing rate combining the feature of L1 and L2.</p>
Set to Factory Default	Click this link to retrieve the factory settings.
Default Message	You can Enter 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.

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:

Action:

<p>Groups</p> <p>Child Protection</p> <p><input type="button" value="Select All"/></p> <p><input type="button" value="Clear All"/></p>	<p>Categories</p> <p><input checked="" type="checkbox"/> Alcohol & Tobacco</p> <p><input checked="" type="checkbox"/> Hate & Intolerance</p> <p><input checked="" type="checkbox"/> Porn & Sexually</p> <p><input checked="" type="checkbox"/> School Cheating</p> <p><input type="checkbox"/> Finance</p> <p><input type="checkbox"/> News</p> <p><input type="checkbox"/> Politics</p> <p><input type="checkbox"/> Restaurants & Dining</p> <p><input type="checkbox"/> General</p> <p><input type="checkbox"/> Image Sharing</p> <p><input type="checkbox"/> Private IP Addresses</p>	<p><input checked="" type="checkbox"/> Criminal Activity</p> <p><input checked="" type="checkbox"/> Illegal Drug</p> <p><input checked="" type="checkbox"/> Violence</p> <p><input checked="" type="checkbox"/> Sex Education</p> <p><input type="checkbox"/> Government</p> <p><input type="checkbox"/> Non-profits & NGOs</p> <p><input type="checkbox"/> Real Estate</p> <p><input type="checkbox"/> Shopping</p> <p><input type="checkbox"/> Cults</p> <p><input type="checkbox"/> Network Errors</p> <p><input type="checkbox"/> Uncategorized Sites</p>	<p><input checked="" type="checkbox"/> Gambling</p> <p><input checked="" type="checkbox"/> Nudity</p> <p><input checked="" type="checkbox"/> Weapons</p> <p><input checked="" type="checkbox"/> Tasteless</p> <p><input type="checkbox"/> Health & Medicine</p> <p><input type="checkbox"/> Personal Sites</p> <p><input type="checkbox"/> Religion</p> <p><input type="checkbox"/> Translators</p> <p><input type="checkbox"/> Greeting cards</p> <p><input type="checkbox"/> Parked Domains</p>
---	---	---	---

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
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>

	<div style="border: 1px solid black; padding: 2px;"> Block ▾ None Pass Block All </div>
Black/White List	<p>Enable - Activate white/black list function for such profile. Group/Object Selections - Click Edit to choose the group or object profile as the content of white/black list.</p> <p>Pass - allow accessing into the corresponding webpage with the characters listed on Group/Object Selections. If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below.</p> <p>Block - restrict accessing into the corresponding webpage with the characters listed on Group/Object Selections. If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below.</p>
Action	<p>Pass - allow accessing into the corresponding webpage with the categories listed on the box below.</p> <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>

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

VI-2-5 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.



Info

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.	

Note:

To make DNS Filter profile effective, please go to [Firewall >> Filter Setup](#) page to create a firewall rule and select the desired profile.

DNS Filter Local Setting

DNS Filter	<input type="checkbox"/> Enable	
Web Content Filter	None	▼
URL Content Filter	None	▼
Syslog	None	▼
Black/White List	<input type="checkbox"/> Enable	Blacklist ▼
	Address Type	Any Address ▼
	Start IP Address	0.0.0.0
	End IP Address	0.0.0.0
	Subnet Mask	0.0.0.0
	IP Group	None ▼
	or IP Group	None ▼
	or IP Object	None ▼
	or IP Object	None ▼

Administration Message (Max 255 characters)

Default Message

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

Legend:

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

OK

Cancel

Available settings are explained as follows:

Item	Description
DNS Filter 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, Enter the name of the profile and specify WCF/UCF based on your requirement.</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>Web Content Filter- Set the filtering conditions.</p> <p>URL Content Filter - Set the filtering conditions.</p> <p>Black/White List - Specify IP address, subnet mask, IP object, or IP group as a black list or white list for DNS packets passing through or blocked by Vigor router.</p>
Administration Message	<p>Enter the words or sentences which will be displayed when a web page is blocked by Vigor router.</p>

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

VI-2-6 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 2017-3-15

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.	
AliWWW	2008		
Ares	2.0.9		
BaiduHi	37378		
Facebook	97.0.0.18.69	To block Facebook for PC and mobile phone(97.0.0.18.69).	
Fetion	2010		
GaduGadu Protocol			
Google Hangouts	18.0	Block PC user's login and Android user's chat/phone service.	
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.	
KC	2008		

Application Notes

A-1 How to Create 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.

Create 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 **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: Cache : | [Set to Factory Default](#) |

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

Note:
To make Web Content Filter profile effective, please go to [Firewall >> Filter Setup](#) page to create a firewall rule and select the desired profile.

Administration Message (Max 255 characters) Default Message

Or

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

System Maintenance >> Activation Activate via interface :

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

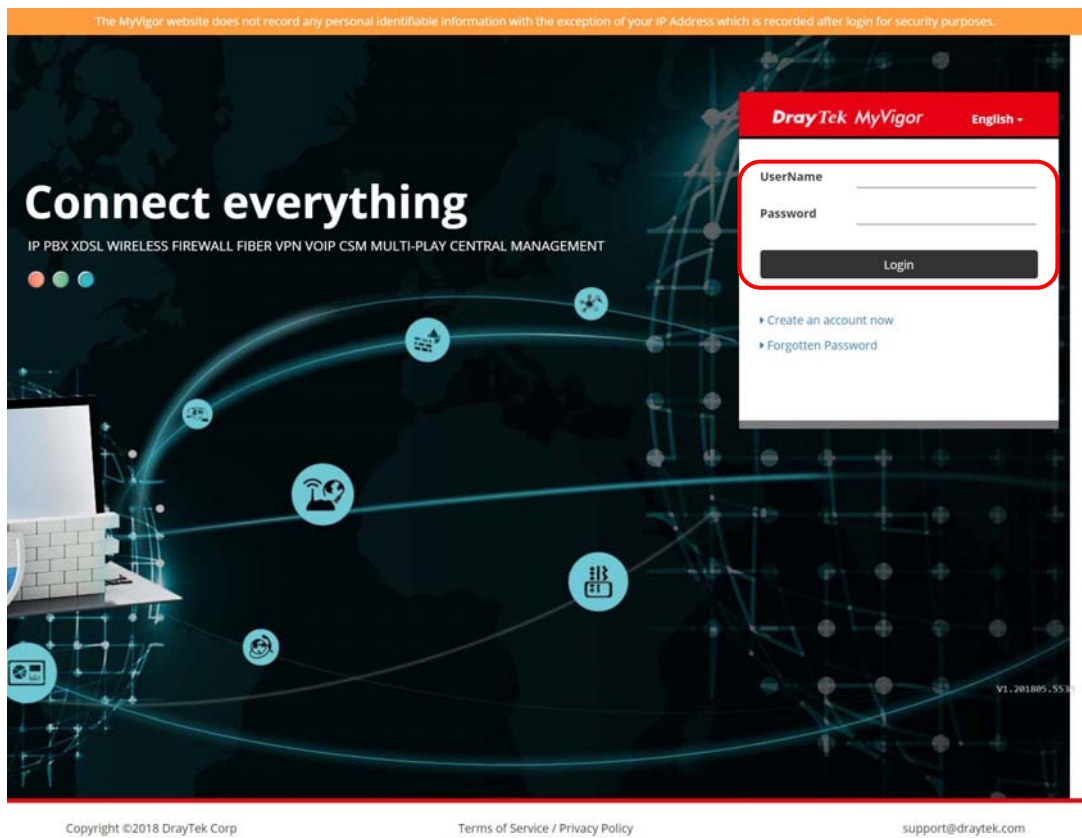
Authentication Message

Note: If you want to use email alert or syslog, please configure the [SysLog/Mail Alert Setup](#) page.

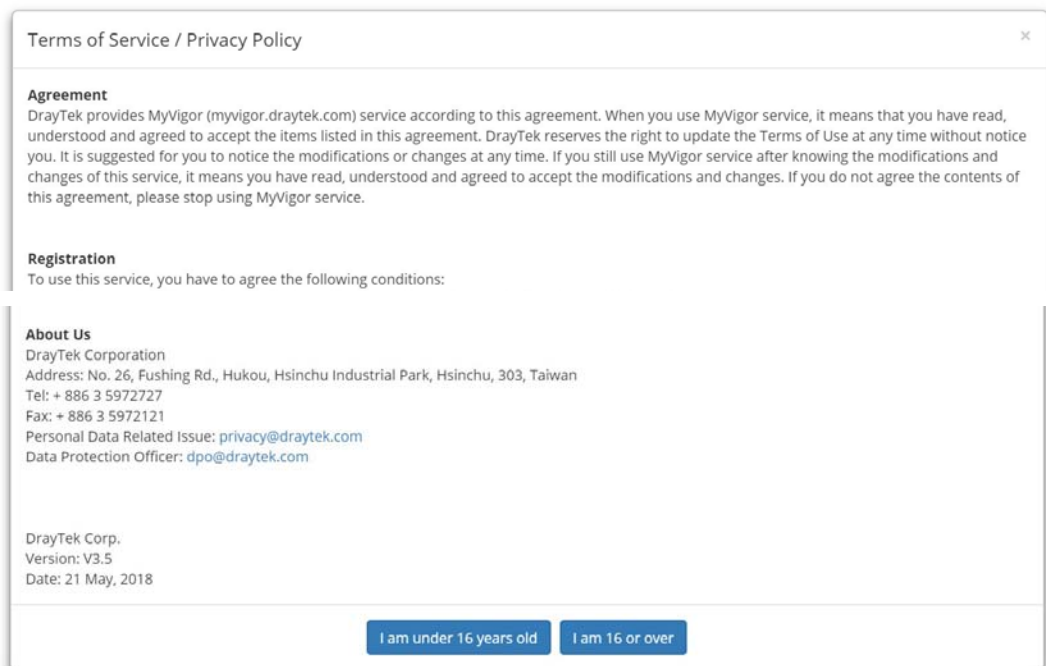
Or,

Access into <http://myvigor.draytek.com> directly.

2. A login page for MyVigor web site will pop up automatically.



3. Click the link of Create an account now.
4. The system will ask if you are 16 years old or over.
 - If yes, click I am 16 or over.



- If not, click I am under 16 years old to get the following page. Then, click I and my legal guardian agree.

this section 8.

About Us
 DrayTek Corporation
 Address: No. 26, Fushing Rd., Hukou, Hsinchu Industrial Park, Hsinchu, 303, Taiwan
 Tel: + 886 3 5972727
 Fax: + 886 3 5972121
 Personal Data Related Issue: privacy@draytek.com
 Data Protection Officer: dpo@draytek.com

DrayTek Corp.
 Version: V3.5
 Date: 21 May, 2018

5. After reading the terms of service/privacy policy, click Agree.

this section 8.

About Us
 DrayTek Corporation
 Address: No. 26, Fushing Rd., Hukou, Hsinchu Industrial Park, Hsinchu, 303, Taiwan
 Tel: + 886 3 5972727
 Fax: + 886 3 5972121
 Personal Data Related Issue: privacy@draytek.com
 Data Protection Officer: dpo@draytek.com

DrayTek Corp.
 Version: V3.5
 Date: 21 May, 2018

6. In the following page, enter your personal information in this page and then click Continue.


DrayTek MyVigor English ▾

Create an account - Please enter personal profile.

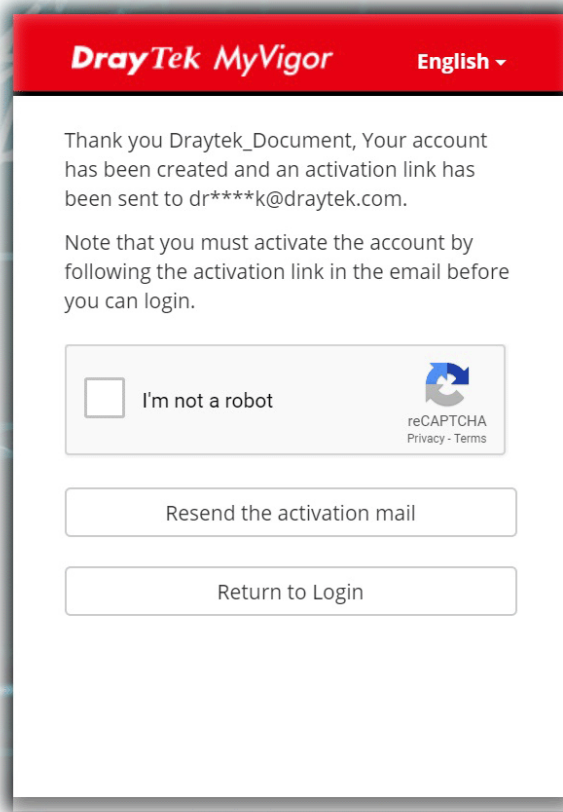
UserName Draytek_Document	Email Address draytek@draytek.com
<input type="text"/>	<input type="text"/>
<p>The user account (Draytek_Document)is available. Please complete registration to register this account.</p>	Country TAIWAN ▾
Password	Industry Other ▾
<input type="text"/>	<input type="text"/>
Confirm Password	
<input type="text"/>	

Do you agree to share your information to DrayTek office, regional distributor, local dealer and third party, in order to receive the newsletter or information from us?

Do you agree that MyVigor website can record your IP Address for security purposes?
 Your IP Address record will only be used for the purposes of detecting and preventing malicious login attempts.
 You can change the setting or clear the record at anytime.

I'm not a robot 

7. Choose proper selection for your computer and click Continue.



8. Now you have created an account successfully. Click START.
9. Check to see the confirmation *email* with the title of New Account Confirmation Letter from myvigor.draytek.com.

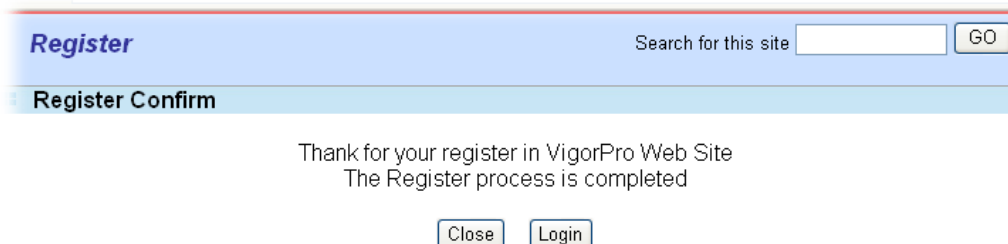
***** This is an automated message from myvigor.draytek.com.*****

Thank you (**Mary**) for creating an account.

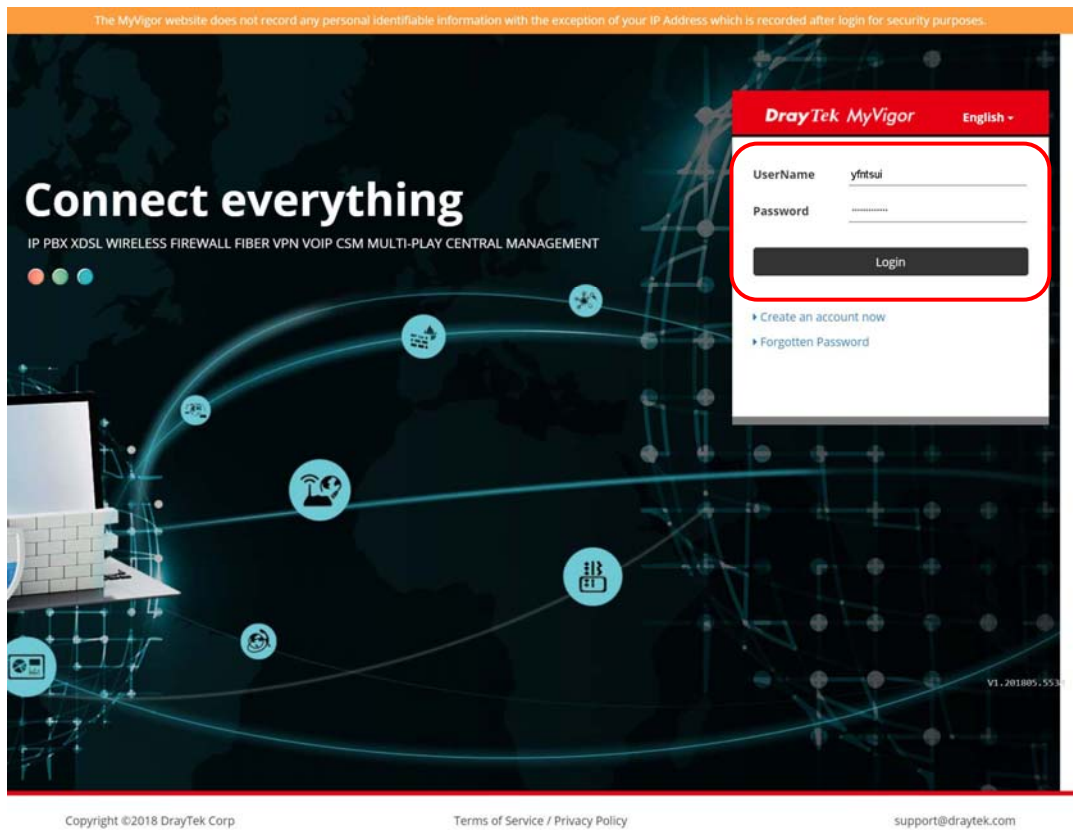
Please click on the activation link below to activate your account

Link : [Activate my Account](#)

10. 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.



11. When you see the following page, please type in the account and password (that you just created) in the fields of UserName and Password.



12. Now, click Login. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

A-2 How to Block Facebook Service Accessed by the Users via Web Content Filter / URL Content Filter

There are two ways to block the facebook service, Web Content Filter and URL Content Filter.

Web Content Filter,

Benefits: Easily and quickly implement the category/website that you want to block.

Note: License is required.

URL Content Filter,

Benefits: Free, flexible for customize webpage.

Note: Manual setting (e.g., one keyword for one website.)

I. Via Web Content Filter

1. Make sure the Web Content Filter (powered by Commtouch) license is valid.

CSM >> Web Content Filter Profile ?

Web-Filter License [Activate](#)
 [Status: **Commtouch**] [Start Date: 2012-12-31 Expire Date: 2013-01-08]

Setup Query Server	auto-selected	Find more
Setup Test Server	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.	

Cache : L1 + L2 Cache ▼

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% Web Content Filter.
<p>Please contact your system administrator for further information.</center></body>
```

Legend:
 %SIP% - Source IP , %DIP% - Destination IP , %URL% - URL
 %CL% - Category , %RNAME% - Router Name

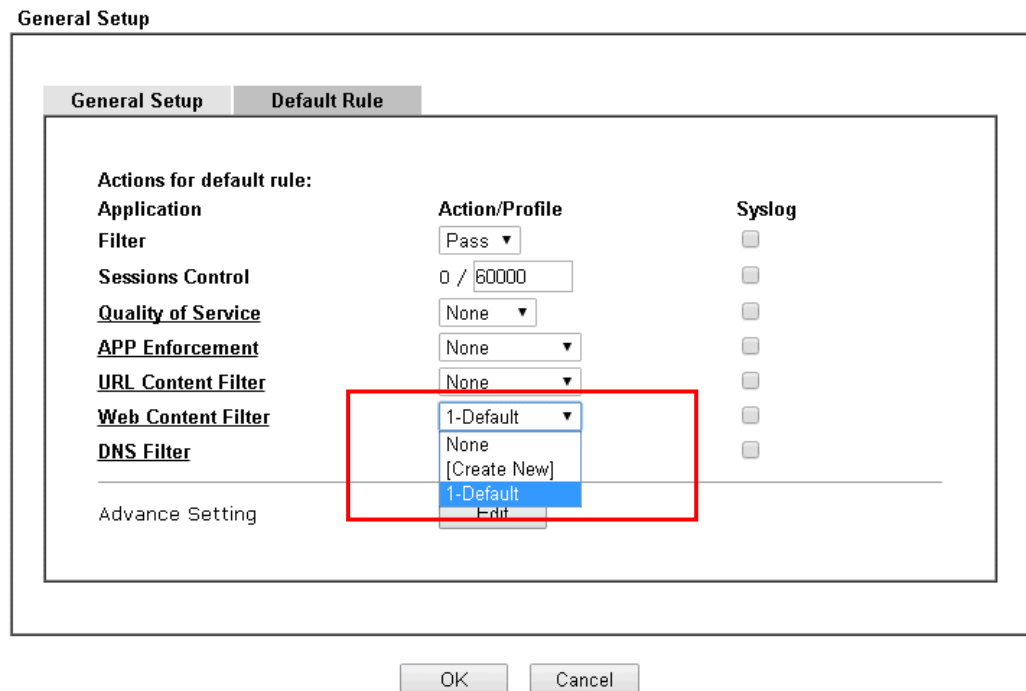
[OK](#)

2. Open CSM >> Web Content Filter Profile to create a WCF profile. Check Social Networking with Action, Block.

Select All	<input checked="" type="checkbox"/> Hate & Intolerance	<input checked="" type="checkbox"/> Illegal Drug	<input checked="" type="checkbox"/> Nudity
Clear All	<input checked="" type="checkbox"/> Porn & Sexually	<input checked="" type="checkbox"/> Violence	<input checked="" type="checkbox"/> Weapons
	<input checked="" type="checkbox"/> School Cheating	<input checked="" type="checkbox"/> Sex Education	<input checked="" type="checkbox"/> Tasteless
	<input checked="" type="checkbox"/> Child Abuse Images		
Leisure			
Select All	<input type="checkbox"/> Entertainment	<input type="checkbox"/> Games	<input type="checkbox"/> Sports
Clear All	<input type="checkbox"/> Travel	<input type="checkbox"/> Leisure & Recreation	<input type="checkbox"/> Fashion & Beauty
Business			
Select All	<input type="checkbox"/> Business	<input type="checkbox"/> Job Search	<input type="checkbox"/> Web-based Mail
Clear All			
Chatting			
Select All	<input type="checkbox"/> Chat	<input type="checkbox"/> Instant Messaging	
Clear All			
Computer-Internet			
Select All	<input type="checkbox"/> Anonymizers	<input type="checkbox"/> Forums & Newsgroups	<input type="checkbox"/> Computers
Clear All	<input type="checkbox"/> Download Sites	<input type="checkbox"/> Streaming Downloads	<input type="checkbox"/> Phishing & Fraud
	<input type="checkbox"/> Search Engine, Portals	<input checked="" type="checkbox"/> Social Networking	<input type="checkbox"/> Spam Sites
	<input type="checkbox"/> Malware	<input type="checkbox"/> Botnets	<input type="checkbox"/> Hacking
	<input type="checkbox"/> Illegal Software	<input type="checkbox"/> Information Security	<input type="checkbox"/> Peer-to-Peer
Other			
Select All	<input type="checkbox"/> Adv & Pop-Ups	<input type="checkbox"/> Arts	<input type="checkbox"/> Transportation
Clear All	<input type="checkbox"/> Compromised	<input type="checkbox"/> Dating & Personals	<input type="checkbox"/> Education
	<input type="checkbox"/> Finance	<input type="checkbox"/> Government	<input type="checkbox"/> Health & Medicine
	<input type="checkbox"/> News	<input type="checkbox"/> Non-profits & NGOs	<input type="checkbox"/> Personal Sites
	<input type="checkbox"/> Politics	<input type="checkbox"/> Real Estate	<input type="checkbox"/> Religion
	<input type="checkbox"/> Restaurants & Dining	<input type="checkbox"/> Shopping	<input type="checkbox"/> Translators

3. Enable this profile in Firewall>>General Setup>>Default Rule.

Firewall >> General Setup



4. Next time when someone accesses facebook via this router, the web page would be blocked and the following message would be displayed instead.

The requested Web page
from 192.168.2.114
to www.facebook.com/
that is categorized with [Social Networking]
has been blocked by Web Content Filter.

Please contact your system administrator for further information.

[Powered by DrayTek]

II. Via URL Content Filter

A. Block the web page containing the word of “Facebook”

1. Open Object Settings>>Keyword Object. Click an index number to open the setting page.
2. In the field of Contents, please type *facebook*. Configure the settings as the following figure.

Objects Setting >> Keyword Object Setup

Profile Index : 1

Name	Facebook
Contents	facebook

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

3. Open CSM>>URL Content Filter Profile. Click an index number to open the setting page.
4. Configure the settings as the following figure.

CSM >> URL Content Filter Profile

Profile Index: 1

Profile Name: Facebook

Priority: Either : URL Access Control First Log: None

1.URL Access Control

Enable URL Access Control Prevent web access from IP address

Action: Block Group/Object Selections: Facebook Edit

2.Web Feature

Enable Restrict Web Feature

Action: Pass Cookie Proxy Upload File Extension Profile: None

OK Clear Cancel

5. When you finished the above steps, click OK. Then, open Firewall>>General Setup.

- Click the Default Rule tab. Choose the profile just configured from the drop down list in the field of URL Content Filter. Now, users cannot open any web page with the word “facebook” inside.

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 / 50000	<input type="checkbox"/>
Quality of Service	None	<input type="checkbox"/>
APP Enforcement	None	<input type="checkbox"/>
URL Content Filter	1-Facebook	<input type="checkbox"/>
Web Content Filter	None	<input type="checkbox"/>
DNS Filter	None	<input type="checkbox"/>

Advance Setting Edit

B. Disallow users to play games on Facebook

- Open Object Settings>>Keyword Object. Click an index number to open the setting page.
- In the field of Contents, please type *apps.facebook*. Configure the settings as the following figure.

Objects Setting >> Keyword Object Setup

Profile Index : 2

Name facebook-apps

Contents apps.facebook

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

- Open CSM>>URL Content Filter Profile. Click an index number to open the setting page.
- Configure the settings as the following figure.

CSM >> URL Content Filter Profile

Profile Index: 2

Profile Name:

Priority: Log:

1.URL Access Control

Enable URL Access Control Prevent web access from IP address

Action: Group/Object Selections:

2.Web Feature

Enable Restrict Web Feature

Action: Cookie Proxy Upload File Extension Profile:

- When you finished the above steps, please open Firewall>>General Setup.
- Click the Default Rule tab. Choose the profile just configured from the drop down list in the field of URL Content Filter. Now, users cannot open any web page with the word “facebook” inside.

Firewall >> General Setup

General Setup

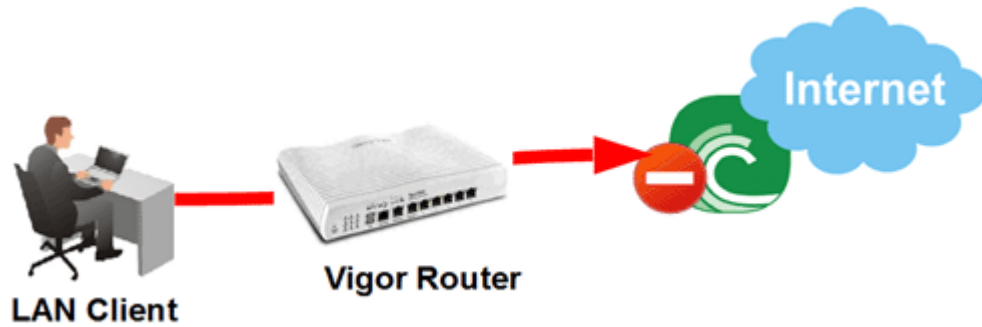
General Setup Default Rule

Actions for default rule:	Action/Profile	Syslog
Application		
Filter	<input type="text" value="Pass"/>	<input type="checkbox"/>
Sessions Control	<input type="text" value="0 / 50000"/>	<input type="checkbox"/>
Quality of Service	<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="2-face.apps"/>	<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		<input type="button" value="Edit"/>

A-3 How to use APP Enforcement to block application like Facebook, YouTube or TeamViewer?

APP Enforcement helps network administrator to block applications on LAN network. Draytek routers provide a few categories to set up the profiles e.g., IM, P2P, Protocol, Stream, Remote control.

This section is going to demonstrate how to use APP Enforcement to block Facebook, Skype, YouTube and TeamViewer.



1. Create an APP Enforcement Profile: Click on an Index number to create a new profile at CSM >> APP Enforcement Profile.

CSM >> APP Enforcement Profile

APP Enforcement Profile Table:

[Set to Factory Default](#)

Profile	Name	Profile	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	

- Set up the details in the profile.

Profile Index : 1
 Profile Name:

Category	Application		
Instant Message <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> AIM	<input type="checkbox"/> AIM Login	<input type="checkbox"/> AliWW
	<input type="checkbox"/> Ares	<input type="checkbox"/> BaiduHi	<input checked="" type="checkbox"/> Facebook b
	<input type="checkbox"/> Fetion	<input type="checkbox"/> GaduGadu Protocol	<input type="checkbox"/> Google Hangouts
	<input type="checkbox"/> ICQ	<input type="checkbox"/> iMessage	<input type="checkbox"/> iSpQ
	<input type="checkbox"/> KC	<input type="checkbox"/> LINE	<input type="checkbox"/> Paltalk
	<input type="checkbox"/> PocoCall	<input type="checkbox"/> Qnext	<input type="checkbox"/> Tencent QQ
	<input type="checkbox"/> UC	<input type="checkbox"/> WebIM URLs	<input type="checkbox"/> WhatsApp
	<input type="checkbox"/> Yahoo! Messenger		
VoIP <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> RC Voice	<input checked="" type="checkbox"/> Skype c	<input type="checkbox"/> TeamSpeak
	<input type="checkbox"/> TelTel		
?			
Stream <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> FlashVideo	<input type="checkbox"/> MMS protocol	<input type="checkbox"/> MySee
	<input type="checkbox"/> PPStream	<input type="checkbox"/> PPTV	<input type="checkbox"/> QQLive
	<input type="checkbox"/> QvodPlayer	<input type="checkbox"/> RTSP protocol	<input type="checkbox"/> SilverLight
	<input type="checkbox"/> Slingbox	<input type="checkbox"/> SopCast	<input type="checkbox"/> TVUPlayer
	<input type="checkbox"/> UUSEE 2008	<input checked="" type="checkbox"/> YouTube d	
Remote Control <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> Ammy Admin	<input type="checkbox"/> LogMeIn Pro2	<input type="checkbox"/> Radmin
	<input type="checkbox"/> ShowMyPC	<input type="checkbox"/> SpyAnywhere	<input checked="" type="checkbox"/> TeamViewer e
	<input type="checkbox"/> Timbuku	<input type="checkbox"/> VNC protocol	<input type="checkbox"/> Windows Live Sync
	<input type="checkbox"/> WindowsRDP		
Web HD <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> ADrive	<input type="checkbox"/> Box	<input type="checkbox"/> Dropbox
	<input type="checkbox"/> Google Service	<input type="checkbox"/> HTTP Upload	<input type="checkbox"/> iCloud
	<input type="checkbox"/> Microsoft Office Live	<input type="checkbox"/> Microsoft OneDrive	<input type="checkbox"/> Mozy
f <input type="button" value="OK"/> <input type="button" value="Cancel"/>			

- Enter Profile Name.
- Choose the Facebook in Instant Message.
- Choose Skype in VoIP.
- Choose YouTube in Stream.
- Choose TeamViewer in Remote control.
- Click OK to save.

- Apply the APP Enforcement Profile to a Firewall Filter Rule. Go to Firewall >> Filter Setup, and click an available set.

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.	

- Click on a Filter Rule index to set up a filter.

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 2
Comments : Default Data Filter

Rule	Enable	Comments	Direction	Src IP	Dst IP	Service Type	Action	CSM	Move Up	Move Down
1	<input checked="" type="checkbox"/>	xNetBios -> DNS	LAN/DMZ/RT/VPN -> WAN	Any	Any	TCP/UDP, Port: from 137~139 to 53	Block Immediately			Down
2	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
3	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
4	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
5	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
6	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
7	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	

Filter Set 1 2 3 4 5 6 7 8 9 10 11 12 Next Filter Set None

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

- Set up the details in the profile.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 2

Enable **a**

Comments: Block_by_APPE **b**

Schedule Profile: None, None, None, None

Clear sessions when schedule is ON

Direction: LAN/DMZ/RT/VPN -> WAN **c** Advanced

Source IP/Country: Any Edit **d**

Destination IP/Country: Any Edit

Service Type: Any Edit

Fragments: Don't Care

Application Filter	Action/Profile	Syslog
Filter	Pass Immediately	<input type="checkbox"/>
Branch to Other Filter Set	None	<input type="checkbox"/>
Sessions Control	0 / 50000	<input type="checkbox"/>
MAC Bind IP	Non-Strict	<input type="checkbox"/>
Quality of Service	None	<input type="checkbox"/>
User Management	None	<input type="checkbox"/>
APP Enforcement	1-Block f	<input checked="" type="checkbox"/> g
URL Content Filter	None	<input type="checkbox"/>
Web Content Filter	None	<input type="checkbox"/>
DNS Filter	None	<input type="checkbox"/>

Advance Setting Edit

h OK Clear Cancel

- Enable the Filter Rule.
- Put the comments of this rule.
- Select the Direction as LAN/DMZ/RT/VPN -> WAN.
- Edit the Source IP which should be blocked from the APP.
- Select Filter as Pass Immediately.
- Select APP Enforcement as the profile we created in Step 2.
- You may also check the Syslog if needed.

- (h) Click OK to save.
6. With the above configuration, LAN clients cannot be able to use the APP and website.



This site can't provide a secure connection

www.facebook.com sent an invalid response.

[Try running Windows Network Diagnostics.](#)

ERR_SSL_PROTOCOL_ERROR

Part VII Management



System
Maintenance



Bandwidth
Management

There are several items offered for the Vigor router system setup: System Status, TR-069, Administrator Password, User Password, Login Page Greeting, Configuration Backup, Syslog /Mail Alert, Time and Date, Management, Reboot System, Firmware Upgrade and Activation.

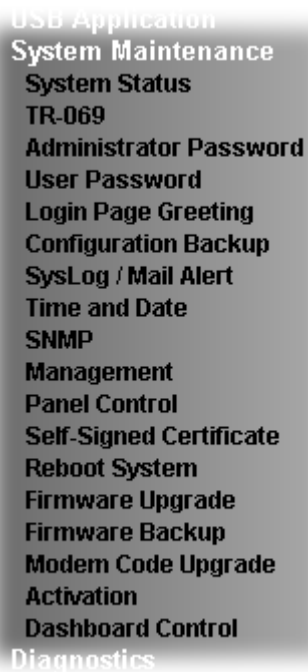
It is used to control the bandwidth of data transmission through configuration of Sessions Limit, Bandwidth Limit, and Quality of Service (QoS).

VII-1 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: System Status, TR-069, Administrator Password, User Password, Login Page Greeting, Configuration Backup, Syslog /Mail Alert, Time and Date, SNMP, Management, Self-Signed Certificate, Reboot System, Firmware Upgrade, Modem Code Upgrade and Activation.

Below shows the menu items for System Maintenance.

Web User Interface



- USB Application
- System Maintenance**
- System Status
- TR-069
- Administrator Password
- User Password
- Login Page Greeting
- Configuration Backup
- SysLog / Mail Alert
- Time and Date
- SNMP
- Management
- Panel Control
- Self-Signed Certificate
- Reboot System
- Firmware Upgrade
- Firmware Backup
- Modem Code Upgrade
- Activation
- Dashboard Control
- Diagnostics

VII-1-1 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 : Vigor2762Vac
Firmware Version : 3.9.0 STD
Build Date/Time : Dec 26 2018 18:40:38

LAN					
	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-1D-AA-08-F5-20	192.168.1.1	255.255.255.0	ON	8.8.8.8
LAN2	00-1D-AA-08-F5-20	192.168.2.1	255.255.255.0	ON	8.8.8.8
IP Routed Subnet	00-1D-AA-08-F5-20	192.168.0.1	255.255.255.0	ON	8.8.8.8

Wireless LAN(2.4GHz)			
MAC Address	Frequency Domain	Firmware Version	SSID
00-1D-AA-08-F5-20	Europe	4.0.1.0rev2.P1	DrayTek

Wireless LAN(5G)			
MAC Address	Frequency Domain	Firmware Version	SSID
00-1D-AA-08-F5-22	Europe	10.2-00082-4	DrayTek_5G

WAN					
	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Disconnected	00-1D-AA-08-F5-21	---	---	---
WAN2	Disconnected	00-1D-AA-08-F5-22	---	---	---
WAN3	Disconnected	00-1D-AA-08-F5-23	---	---	---

IPv6		
Address	Scope	Internet Access Mode
LAN FE80::21D:AAFF:FE08:F520/64	Link	---

VoIP			
Port	Profile	Reg.	In/Out
Phone1		No	0/0
Phone2		No	0/0

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.
WAN	Link Status - Display current connection status. MAC Address - Display the MAC address of the WAN Interface. Connection

	<p>- Display the connection type.</p> <p>IP Address</p> <p>- Display the IP address of the WAN interface.</p> <p>Default Gateway</p> <p>- Display the assigned IP address of the default gateway.</p>
IPv6	<p>Address - Display the IPv6 address for LAN.</p> <p>Scope - Display the scope of IPv6 address. For example, IPv6 Link Local could only be used for direct IPv6 link. It can't be used for IPv6 internet.</p> <p>Internet Access Mode - Display the connection mode chosen for accessing into Internet.</p>

VII-1-2 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
Export Parameters

TR-069 Disable Enable

ACS Server On

ACS Server

URL Wizard

Acquire URL from DHCP option 43

Username

Password

Event Code

Last Inform Response Time :(NA) ●

CPE Client

Protocol HTTP HTTPS

URL

Port

Username

Password

Note: Please enable TR-069 server to allow access from Internet on [System Maintenance >> Management](#) page.

Periodic Inform Settings

Enable Disable

Time Interval second(s)

STUN Settings

Enable Disable

Server Address

Server **STUN** Port

Minimum Keep Alive Period second(s)

Maximum Keep Alive Period second(s)

Apply Settings to APs

Enable Disable

AP Password

Specify STUN Settings for APs

Bandwidth Utilisation Notification Settings

Enable Disable

Time Period

WAN	Threshold Level	Line Speed
<input type="checkbox"/> WAN1	Medium <input type="text" value="0"/> % High <input type="text" value="0"/> %	of TX: <input type="text" value="N/A"/> Mbps RX: <input type="text" value="N/A"/> Mbps
<input type="checkbox"/> WAN2	Medium <input type="text" value="0"/> % High <input type="text" value="0"/> %	of TX: <input type="text" value="0"/> Mbps RX: <input type="text" value="0"/> Mbps
<input type="checkbox"/> WAN3	Medium <input type="text" value="0"/> % High <input type="text" value="0"/> %	of TX: <input type="text" value="0"/> Mbps RX: <input type="text" value="0"/> Mbps

Note: Please turn off [Hardware Acceleration](#) in the router to receive Alerts Notifications, and accuracy of Bandwidth data.

Available settings are explained as follows:

Item	Description
TR-069	Click Enable to activate the settings on this page.
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.</p> <ul style="list-style-type: none"> ● Wizard - Click it to enter the IP address of VigorACS server, port number and the handler. ● Acquire URL form DHCP option 43 - Check the box to get the URL from DHCP option 43. <p>Username/Password - Such data must be typed according to the ACS (Auto Configuration Server) you want to link.</p> <ul style="list-style-type: none"> ● 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. ● Event Code - Use the drop down menu to specify an event to perform the test. <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>Protocol - Select HTTP or HTTPS.</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 - Enter the username and password that VigorACS can use to access into such CPE.</p>
Periodic Inform Settings	<p>Enable - It is the default setting.</p> <ul style="list-style-type: none"> ● Time Interval - Please set interval time or schedule time for the router to send notification to CPE. <p>Disable - Click it to close the mechanism of notification.</p>
STUN Settings	<p>Disable - The default is Disable.</p> <p>Enable - Please Enter the relational settings listed below:</p> <ul style="list-style-type: none"> ● Server Address - Enter the IP address of the STUN server. ● Server STUN Port - Enter the port number of the STUN server. ● Minimum Keep Alive Period - If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds". ● Maximum Keep Alive Period - If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.
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 Vigor2762 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</p>

	<p>enabled, you have to Enter the password for accessing VigorAP.</p> <ul style="list-style-type: none"> ● AP Password - Enter the password of the VigorAP that you want to apply Vigor2762's TR-069 settings. <p>Specify STUN Settings to APs - If you want to apply specific STUN settings (not the STUN Settings configured for Vigor2952) to VigorAPs to meet specific requirements, simply check this box. Then, enter the server IP address, server port, minimum keep alive period and maximum keep alive period respectively.</p>
<p>Bandwidth Utilisation Notification Settings</p>	<p>To administrator, this feature is useful to monitor the bandwidth utilization of CPE(s). When the bandwidth used is over the threshold level (percentage defined in medium and high fields), a notification will be sent to VigorACS. After a long time observation, the administrator can determine if it is necessary to increase the bandwidth setting for that CPE or not.</p> <p>Disable - The default is Disable.</p> <p>Enable - Click it to enable such feature.</p> <ul style="list-style-type: none"> ● Time Period - Choose the time interval (15 mins, 30 mins, 1hour, 3 hours, or 6 hours) for CPE to send a notification of bandwidth utilization to VigorACS. ● WAN - Choose the WAN interface for applying the bandwidth utilization notification mechanism. ● Threshold Level - Set the percentage of bandwidth in transmission and receiving data as threshold values for CPE to detect bandwidth utilization. ● Line Speed - Set the transmission rate and receiving rate for specified WAN interface.

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

VII-1-3 Administrator Password

This page allows you to set new password for administrator.

System Maintenance >> Administrator Password Setup

Administrator Password

Old Password	<input type="text"/>	Max: 83 characters
New Password	<input type="text"/>	Max: 83 characters
Confirm Password	<input type="text"/>	Max: 83 characters
<input checked="" type="checkbox"/> Enable 'admin' account login to Web UI from the Internet		
<input type="checkbox"/> Use only advanced authentication method for Admin "WAN" login		
<input checked="" type="radio"/> Mobile one-Time Passwords(mOTP)		
PIN Code	<input type="text"/>	Secret <input type="text"/>
<input type="radio"/> 2-Step Authentication		
Send Auth code via		
<input type="checkbox"/> SMS Profile	<input type="text"/>	To : <input type="text"/>
<input type="checkbox"/> Mail Profile	<input type="text"/>	<input type="text"/>

Note:

Password can contain only a-z A-Z 0-9 , ; : . " < > * + = | ? @ # ^ ! ()

Administrator Local User

<input type="checkbox"/> Enable Local User			
<input type="checkbox"/> Use only advanced authentication method for Admin "WAN" login			
Local User List			
Index	User Name	Type	Destination
<div style="border: 1px solid gray; height: 100px;"></div>			
Specific User			
User Name:	<input type="text"/>	Max: 15 characters	
Authentication method:			
Basic -			
<input checked="" type="radio"/> Local Password			
Password:	<input type="text"/>	Confirm Password:	<input type="text"/>
Max: 15 characters			
Advanced -			
<input type="radio"/> Mobile one-Time Passwords(mOTP)			
PIN Code	<input type="text"/>	Secret	<input type="text"/>
<input type="radio"/> 2-Step Authentication			
Password:	<input type="text"/>	Confirm Password:	<input type="text"/>
Max: 19 characters			
Send Auth code via			
<input type="checkbox"/> SMS Profile	<input type="text"/>	To :	<input type="text"/>
<input type="checkbox"/> Mail Profile	<input type="text"/>		<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			

Available settings are explained as follows:

Item	Description
Administrator Password	<p>Old Password - Type in the old password. The factory default setting for password is "admin".</p> <p>New Password -Type in new password in this field. The length of the password is limited to 23 characters.</p> <p>Confirm Password -Type in the new password again.</p> <p>Enable 'admin' account login to Web UI from the Internet - 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 Password	<p>The administrator can login web user interface of Vigor router to modify all of the settings to fit the requirements.</p> <p>Old Password - Type in the old password. The factory default setting for password is "admin".</p> <p>New Password - Define the basic password. The length of the password is limited to 23 characters.</p> <p>Confirm Password - Enter the basic password again for confirmation.</p> <p>Enable 'admin' account login to Web UI from the Internet - It is configurable only when Administrator Local User is enabled. The default setting is enabled. It can ensure that any user is able to successfully accesses into web user interface of Vigor router through Internet by username/password of "admin/admin". However, if you want to prevent the admin account from password attacks by hackers, disable this function and let local user account access into the WUI instead.</p> <p>Use only advanced authentication method for Admin "WAN" login - Advanced authentication method can offer a more secure network connection. In general, the above basic password setting will be used for authentication if such option is disabled. Simply check the box to enable the following settings.</p> <ul style="list-style-type: none"> ● Mobile one-Time Password (mOTP) - Click it to use mOTP as the advanced authentication method. Enter the PIN code and secret settings for one-time usage. ● 2-Step Auth code via <u>SMS Profile</u> and/or <u>Mail Profile</u> - Click it to use authentication code as the advanced authentication method. The authentication code will be sent out based on the selected SMS profile and Mail profile.
Administrator Local User	<p>Usually, the system administrator has the highest privilege to modify the settings on the web user interface of the Vigor router. However, in some cases, it might be necessary to have other users in LAN to access into the web user interface of Vigor router.</p> <p>This feature is used to define other users in LAN who can access into the web user interface with the same privilege as the administrator.</p> <p>Enable Local User - Check the box to enable Administrator Local User setting and define the local user account and password.</p> <p>Use only advanced authentication method for Admin "WAN" login - Advanced authentication method can offer a</p>

more secure network connection. In general, the following basic password setting will be used for authentication if such option is disabled. Simply check the box to enable the following settings.

- Local User List - Display the username, authentication method of the local user.
- Specific User - Create the new user account as the local user. Then specify the authentication method (dividing into Basic and Advanced) for the user account.
 - User Name - Enter a user name.
 - Authentication method (Basic) - Vigor router will authenticate the specific user via the local password.
Local Password - Enter the password for the local user.
 - Authentication method (Advanced) - Vigor router will authenticate the specific user via the mOTP or 2-Step Auth code.
Mobile one-Time Password (mOTP) - Click it to use mOTP as the advanced authentication method. Enter the PIN code and secret settings for one-time usage.
2-Step Authentication via SMS Profile and/or Mail Profile - Click it to use authentication code as the advanced authentication method. The authentication code will be sent out based on the selected SMS profile and Mail profile.
- 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.
- 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.
- Delete - If the local user listed on the box above is not satisfied, simply click the username and click Delete to remove it.
-

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

VII-1-4 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	Max: 23 characters
Confirm Password	Max: 23 characters
Password Strength:	Weak Medium Strong
Strong password requirements:	
1. Have at least one upper-case letter and one lower-case letter.	
2. Including non-alphanumeric characters is a plus.	

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.

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. The length of the password is limited to 31 characters.
Confirm Password	Type in the new password again.
Password Strength	Display the security strength of the password specified above.
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"/>
Password Strength:	<input type="button" value="Weak"/> <input checked="" type="button" value="Medium"/> <input type="button" value="Strong"/>
Strong password requirements:	
1. Have at least one upper-case letter and one lower-case letter.	
2. Including non-alphanumeric characters is a plus.	

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. The following screen will appear. Simply click OK.

System Maintenance >> User Password

Active Configuration

Password	: *****
----------	---------

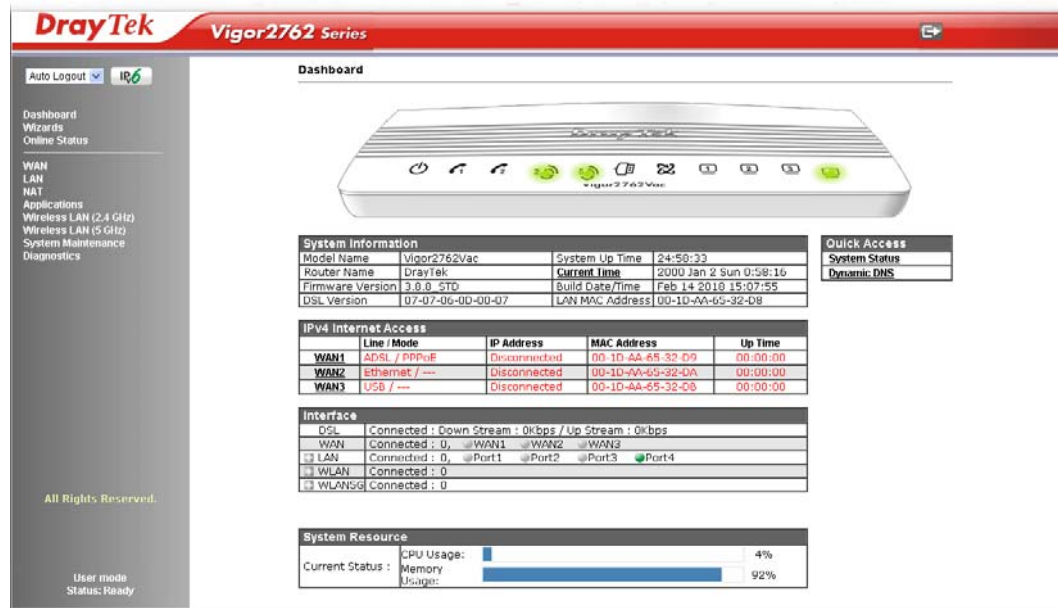
4. Log out Vigor router web user interface by clicking the Logout button.



5. The following window will be open to ask for username and password. Enter the new user password in the field of Password and click Login.

A login window for the DrayTek Vigor2762 Series. The header features the DrayTek logo and "Vigor2762 Series". Below the header is a "Login" section with two input fields: "Username" and "Password". The "Password" field contains five dots. A "Login" button is positioned below the fields. At the bottom, there is a copyright notice: "Copyright © 2000-2017 DrayTek Corp. All Rights Reserved."

- The main screen with User Mode will be shown as follows.



Settings to be configured in User Mode will be less than settings in Admin Mode. Only basic configuration settings will be available in User Mode.



Info

Setting in User Mode can be configured as same as in Admin Mode.

VII-1-5 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 login URL 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

Username

Password

Login

Copyright © 2000-2017 DrayTek Corp. All Rights Reserved.

Welcome Message

This welcome message is displayed in the Login page of the router. Replace this text with your own message.

1. The welcome message can be written in HTML so lists such as this one can be created
2. Other markup tags such as p, font or img can be used

VII-1-6 Configuration Backup

Such function can be used to apply the router settings configured by Vigor2760 to Vigor2762.

Backup the Configuration

Follow the steps below to backup your configuration.


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

System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restore
Restore settings from a configuration file.

選擇檔案 未選擇任何檔案

USB Storage 

Restore configuration except the login password.

Note:
This will work only if the selected configuration file was created from this device.


Backup
Back up the current settings into a configuration file.

Protect with password

Note:
The router's certificates are not part of the configuration file. Please use [Certificate Management >> Certificate Backup](#) for backup.

Auto Backup to USB storage

Enable

Backup folder 

Periodic backup
Cycle duration: days and hours

Backup after change configuration

Note:

1. 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.
2. Auto backup to USB: if settings do not change, configuration doesn't backup.
3. Auto backup to USB: if configuration backup multiple times in one hour, the old file will be overwritten with the same filename.

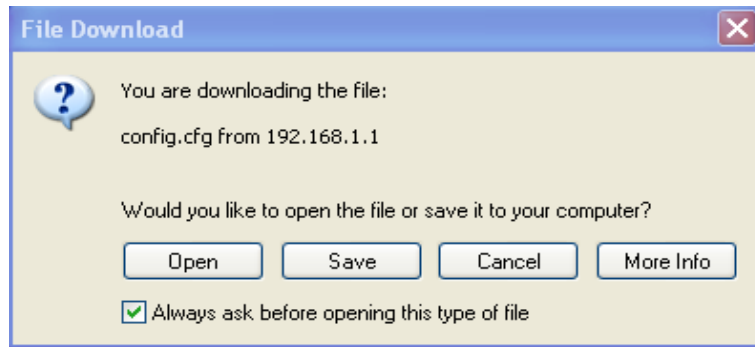
Supported Model List

Model	Firmware Version
Vigor2760	3.8.2.2, or later

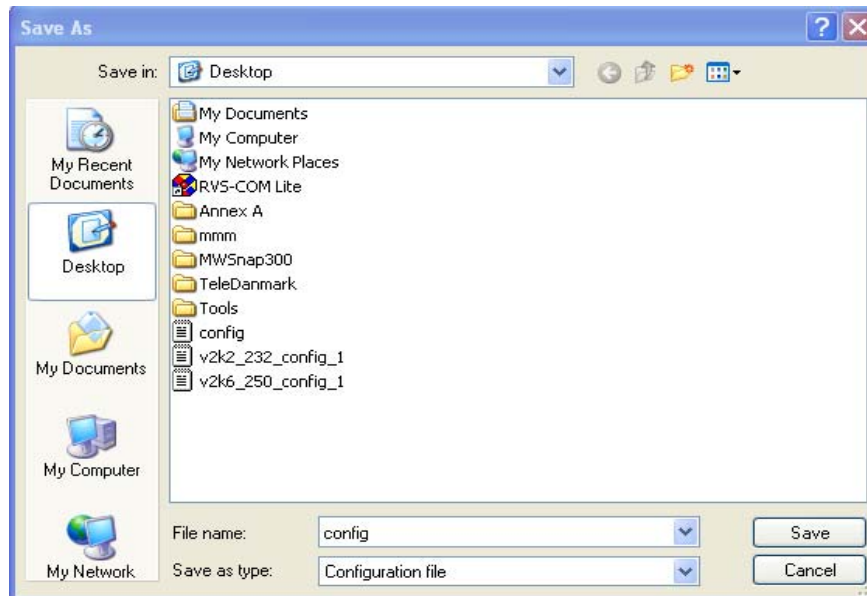
Available settings are explained as follows:

Item	Description
Restore	Choose File - Click it to specify a file to be restored. Click Restore to restore the configuration.
Backup	Click it to perform the configuration backup of this router.

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.



Info


Backup for Certification must be done independently. The Configuration Backup does not include information of Certificate.

Restore Configuration

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


System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restore
Restore settings from a configuration file.
 選擇檔案 未選擇任何檔案
 USB Storage 
 Restore configuration except the login password.
Note:
This will work only if the selected configuration file was created from this device.

Backup
Back up the current settings into a configuration file.
 Protect with password

Note:
The router's certificates are not part of the configuration file. Please use [Certificate Management >> Certificate Backup](#) for backup.

Auto Backup to USB storage
 Enable
Backup folder 
 Periodic backup
Cycle duration: days and hours
 Backup after change configuration

Note:

1. 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.
2. Auto backup to USB: if settings do not change, configuration doesn't backup.
3. Auto backup to USB: if configuration backup multiple times in one hour, the old file will be overwritten with the same filename.

Supported Model List

Model	Firmware Version
Vigor2760	3.8.2.2, or later

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

VII-1-7 SysLog/Mail Alert

SysLog function is provided for users to monitor router.

System Maintenance >> SysLog / Mail Alert Setup

SysLog / Mail Alert Setup

<p>SysLog Access Setup</p> <p><input checked="" type="checkbox"/> Enable</p> <p>Syslog Save to:</p> <p><input checked="" type="checkbox"/> Syslog Server</p> <p><input type="checkbox"/> USB Disk</p> <p>Router Name <input type="text" value="DrayTek"/></p> <p>Server IP Address <input type="text"/></p> <p>Destination Port <input type="text" value="514"/></p> <p>Mail Syslog <input type="checkbox"/> Enable</p> <p>Enable syslog message:</p> <p><input checked="" type="checkbox"/> Firewall Log</p> <p><input checked="" type="checkbox"/> VPN Log</p> <p><input checked="" type="checkbox"/> User Access Log</p> <p><input checked="" type="checkbox"/> Call Log</p> <p><input checked="" type="checkbox"/> WAN Log</p> <p><input checked="" type="checkbox"/> Router/DSL information</p> <p><input checked="" type="checkbox"/> WLAN Log</p>	<p>Mail Alert Setup</p> <p><input checked="" type="checkbox"/> Enable <input type="button" value="Send a test e-mail"/></p> <p>SMTP Server <input type="text"/></p> <p>SMTP Port <input type="text" value="25"/></p> <p>Mail To <input type="text"/></p> <p>Return-Path <input type="text"/></p> <p><input type="checkbox"/> Use SSL</p> <p><input type="checkbox"/> Authentication</p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>Enable E-Mail Alert:</p> <p><input checked="" type="checkbox"/> DoS Attack</p> <p><input checked="" type="checkbox"/> APPE</p> <p><input checked="" type="checkbox"/> VPN LOG</p> <p><input type="checkbox"/> APPE Signature</p> <p><input type="checkbox"/> Debug Log</p>
--	--

Note:

1. Mail Syslog cannot be activated unless USB Disk is ticked for "Syslog Save to".
2. Mail Syslog feature sends a Syslog file when its size reaches 1M Bytes.
3. We only support secured SMTP connection on port 465.

Available settings are explained as follows:

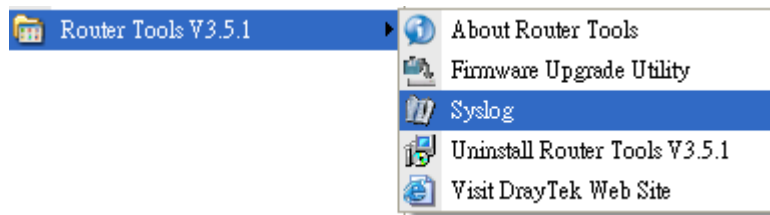
Item	Description
SysLog Access Setup	<p>Enable - Check Enable to activate function of syslog.</p> <p>Syslog Save to - Check Syslog Server to save the log to Syslog server.</p> <p>Check USB Disk to save the log to the attached USB storage disk.</p>
Router Name	<p>Display the name for such router configured in System Maintenance>>Management.</p> <p>If there is no name here, simply lick the link to access into System Maintenance>>Management to set the router name.</p> <p>Server IP Address -The IP address of the Syslog server.</p> <p>Destination Port - Assign a port for the Syslog protocol.</p> <p>Mail Syslog - Check the box to recode the mail event on Syslog.</p> <p>Enable syslog message - Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to Syslog.</p>
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</p>

	<p>address is available or not.</p> <p>SMTP Server/SMTP Port - The IP address/Port number of the SMTP server.</p> <p>Mail To - Assign a mail address for sending mails out.</p> <p>Return-Path - Assign a path for receiving the mail from outside.</p> <p>Use SSL - Check this box to use port 465 for SMTP server for some e-mail server uses https as the transmission method.</p> <p>Authentication - Check this box to activate this function while using e-mail application.</p> <p>User Name - Enter the user name for authentication.</p> <p>Password - Enter 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>
--	--

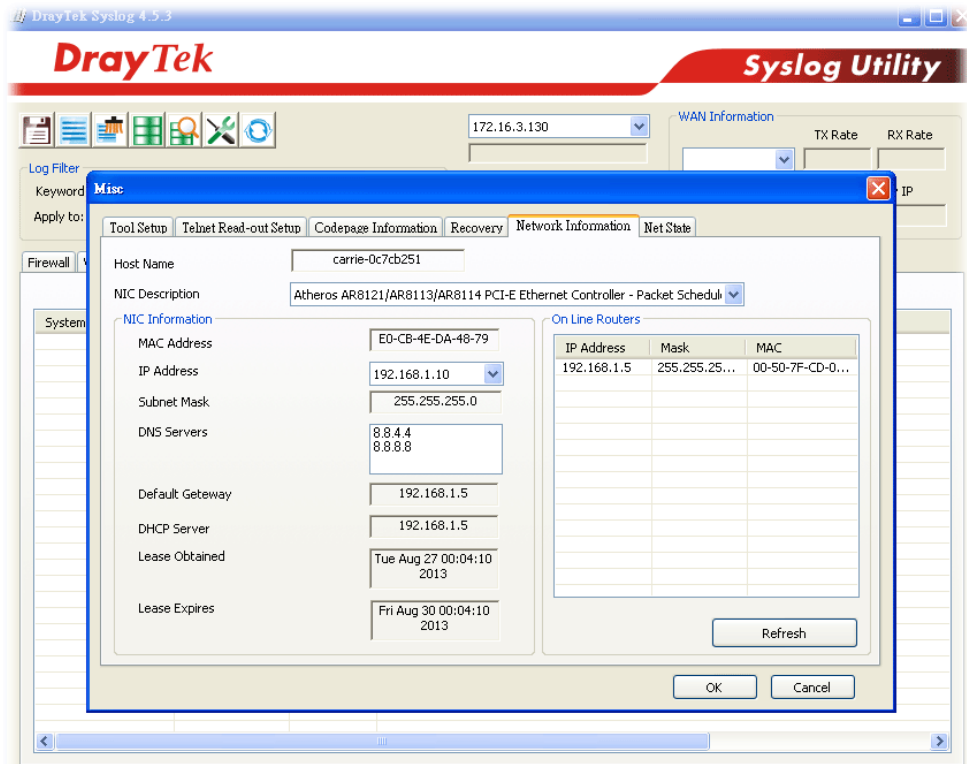
Click OK to save these settings.

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.



- 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.



System Time: Time taken from the computer which runs the custom application

Router Time: Time taken from router

VII-1-8 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 2 Sun 19 : 14 : 53 Inquire Time

Time Setup

Use Browser Time
 Use Internet Time

Time Server:

Priority:

Time Zone:

Enable Daylight Saving: Advanced

Automatically Update Interval:

Send NTP Request Through:

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	Enter the web site of the time server.
Priority	Choose Auto or IPv6 First as the priority.
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 style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <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 <input type="text" value=""/> Month <input type="text" value=""/> Day <input type="text" value=""/> 00 : 00 End: Year <input type="text" value=""/> Month <input type="text" value=""/> Day <input type="text" value=""/> 00 : 00 </p> <p> <input type="radio"/> Yearly Start: Yearly On <input type="text" value="Januai"/> <input type="text" value="First"/> <input type="text" value="Sunda"/> 00 : 00 End: Yearly On <input type="text" value="Januai"/> <input type="text" value="First"/> <input type="text" value="Sunda"/> 00 : 00 </p> <p style="text-align: center;"> <input type="button" value="OK"/> <input type="button" value="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.

Send NTP Request Through	Specify a WAN interface to send NTP request for time synchronization.
--------------------------	---

Click OK to save these settings.

VII-1-9 SNMP

This page allows you to configure settings for SNMP and SNMPV3 services.

The SNMPv3 is more secure than SNMP through the encryption method (support AES and DES) and authentication method (support MD5 and SHA) for the management needs.

System Maintenance >> SNMP

SNMP Setup

<input type="checkbox"/> Enable SNMP Agent													
<input checked="" type="checkbox"/> Enable SNMPV1 Agent													
<input checked="" type="checkbox"/> Enable SNMPV2C Agent													
Get Community	public												
Set Community	private												
Manager Host IP(IPv4)	<table border="1"> <thead> <tr> <th>Index</th> <th>IP</th> <th>Subnet Mask</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>2</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>3</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table>	Index	IP	Subnet Mask	1	<input type="text"/>	<input type="text"/>	2	<input type="text"/>	<input type="text"/>	3	<input type="text"/>	<input type="text"/>
Index	IP	Subnet Mask											
1	<input type="text"/>	<input type="text"/>											
2	<input type="text"/>	<input type="text"/>											
3	<input type="text"/>	<input type="text"/>											
Manager Host IP(IPv6)	<table border="1"> <thead> <tr> <th>Index</th> <th>IPv6 Address</th> <th>/ Prefix Length</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>2</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>3</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table>	Index	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"/>
Index	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"/>											
Trap Community	public												
Notification Host IP(IPv4)	<table border="1"> <thead> <tr> <th>Index</th> <th>IP</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="text"/></td> </tr> <tr> <td>2</td> <td><input type="text"/></td> </tr> </tbody> </table>	Index	IP	1	<input type="text"/>	2	<input type="text"/>						
Index	IP												
1	<input type="text"/>												
2	<input type="text"/>												
Notification Host IP(IPv6)	<table border="1"> <thead> <tr> <th>Index</th> <th>IPv6 Address</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="text"/></td> </tr> <tr> <td>2</td> <td><input type="text"/></td> </tr> </tbody> </table>	Index	IPv6 Address	1	<input type="text"/>	2	<input type="text"/>						
Index	IPv6 Address												
1	<input type="text"/>												
2	<input type="text"/>												
Trap Timeout	10												
<input type="checkbox"/> Enable SNMPV3 Agent													
USM User	<input type="text"/>												
Auth Algorithm	No Auth												
Auth Password	<input type="text"/>												
Privacy Algorithm	No Priv												
Privacy Password	<input type="text"/>												

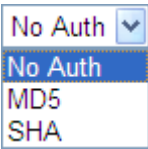
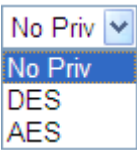
Note:

SNMP service also shall be enabled for Internet access in [System Maintenance >> Management](#).

OK Cancel

Available settings are explained as follows:

Item	Description
Enable SNMP Agent	Check it to enable this function. Then, enable SNMPV1 agent/SNMPV2C agent.

Get Community	Set the name for getting community by typing a proper character. The default setting is public. The maximum length of the text is limited to 23 characters.
Set Community	Set community by typing a proper name. The default setting is private. The maximum length of the text is limited to 23 characters.
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. The maximum length of the text is limited to 23 characters.
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. The maximum length of the text is limited to 23 characters.
Auth Algorithm	Choose one of the encryption methods listed below as the authentication algorithm. 
Auth Password	Type a password for authentication. The maximum length of the text is limited to 23 characters.
Privacy Algorithm	Choose one of the methods listed below as the privacy algorithm. 
Privacy Password	Type a password for privacy. The maximum length of the text is limited to 23 characters.

Click OK to save these settings.

VII-1-10 Management

This page allows you to manage the settings for Internet/LAN Access Control, Access List from Internet, Management Port Setup, TLS/SSL Encryption Setup, and Device Management.

The management pages for IPv4 and IPv6 protocols are different.

VII-1-10-1 IPv4 Management Setup

System Maintenance >> Management





IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup																																	
Router Name <input type="text" value="DrayTek"/>																																			
<input type="checkbox"/> Default: Disable Auto-Logout <input type="checkbox"/> Enable Validation Code in Internet/LAN Access Internet Access Control <input type="checkbox"/> Allow management from the Internet Domain name allowed <input type="text"/> <input type="checkbox"/> FTP Server <input type="checkbox"/> HTTP Server <input type="checkbox"/> Enforce HTTPS Access <input checked="" type="checkbox"/> HTTPS Server <input type="checkbox"/> Telnet Server <input type="checkbox"/> TR069 Server <input type="checkbox"/> SSH Server <input type="checkbox"/> SNMP Server <input checked="" type="checkbox"/> Disable PING from the Internet Access List from the Internet <input type="checkbox"/> Apply Access List to PING <table border="1"> <thead> <tr> <th>List</th> <th>index in IP Object</th> <th>IP / Mask</th> </tr> </thead> <tbody> <tr><td>1</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>2</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>3</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>4</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>5</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>6</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>7</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>8</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>9</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>10</td><td><input type="text"/></td><td><input type="text"/></td></tr> </tbody> </table>	List	index in IP Object	IP / Mask	1	<input type="text"/>	<input type="text"/>	2	<input type="text"/>	<input type="text"/>	3	<input type="text"/>	<input type="text"/>	4	<input type="text"/>	<input type="text"/>	5	<input type="text"/>	<input type="text"/>	6	<input type="text"/>	<input type="text"/>	7	<input type="text"/>	<input type="text"/>	8	<input type="text"/>	<input type="text"/>	9	<input type="text"/>	<input type="text"/>	10	<input type="text"/>	<input type="text"/>	Management Port Setup <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports Telnet Port <input type="text" value="23"/> (Default: 23) HTTP Port <input type="text" value="80"/> (Default: 80) HTTPS Port <input type="text" value="443"/> (Default: 443) FTP Port <input type="text" value="21"/> (Default: 21) TR069 Port <input type="text" value="8069"/> (Default: 8069) SSH Port <input type="text" value="22"/> (Default: 22)	
List	index in IP Object	IP / Mask																																	
1	<input type="text"/>	<input type="text"/>																																	
2	<input type="text"/>	<input type="text"/>																																	
3	<input type="text"/>	<input type="text"/>																																	
4	<input type="text"/>	<input type="text"/>																																	
5	<input type="text"/>	<input type="text"/>																																	
6	<input type="text"/>	<input type="text"/>																																	
7	<input type="text"/>	<input type="text"/>																																	
8	<input type="text"/>	<input type="text"/>																																	
9	<input type="text"/>	<input type="text"/>																																	
10	<input type="text"/>	<input type="text"/>																																	
	Brute Force Protection <input type="checkbox"/> Enable brute force login protection <input type="checkbox"/> FTP Server <input type="checkbox"/> HTTP Server <input type="checkbox"/> HTTPS Server <input type="checkbox"/> Telnet Server <input type="checkbox"/> TR069 Server <input type="checkbox"/> SSH Server Maximum login failures <input type="text" value="0"/> times Penalty period <input type="text" value="0"/> seconds																																		
	Blocked IP List																																		
	TLS/SSL Encryption Setup <input checked="" type="checkbox"/> Enable TLS 1.2 <input checked="" type="checkbox"/> Enable TLS 1.1 <input checked="" type="checkbox"/> Enable TLS 1.0 <input type="checkbox"/> Enable SSL 3.0																																		
	AP Management <input checked="" type="checkbox"/> Enable AP Management																																		
	<input checked="" type="checkbox"/> Device Management <input type="checkbox"/> Respond to external device																																		

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> 
<p>Enable Validation Code in Internet/LAN Access</p>	<p>If it is enabled, the mechanism of validation code will be offered by Vigor router. That is, the client must type validation code while accessing into Internet or web user interface of Vigor router.</p>
<p>Internet Access Control</p>	<p>Allow management from the Internet - Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.</p> <p>Disable PING from the Internet - Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.</p>
<p>Access List from the Internet</p>	<p>You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.</p> <p>Apply Access List to PING - The behavior of this feature is related to the function of Disable PING from the Internet. When Disable PING from the Internet is disabled (unchecked) and Apply Access List to PING is enabled (checked), Vigor router will ping only the IPs list below (index in IP Object). When both Disable PING from the Internet and Apply Access List to PING are disabled (unchecked), Vigor router allows ping job of any IP.</p> <p>index in IP Object- Enter the index number of the IP object profile. Related IP with Subnet Mask will appear automatically.</p>
<p>Management Port Setup</p>	<p>User Define Ports - Check to specify user-defined port numbers for the Telnet, HTTP, HTTPS, FTP, TR-069 and SSH servers.</p> <p>Default Ports - Check to use standard port numbers for the Telnet and HTTP servers.</p>
<p>Brute Force Protection</p>	<p>Any client trying to access into Internet via Vigor router will be asked for passing through user authentication. Such feature can prevent Vigor router from attacks when a hacker tries every possible combination of letters, numbers and symbols until find out the correct combination of password.</p> <p>Enable brute force login protection - Enable the protection mechanism.</p> <p>Maximum login failure - Specify the maximum number of wrong password that client can try for logging to Vigor router.</p> <p>Penalty period - Set a period of time to block the IP address</p>

	<p>which is used (by user or hacker) for passing through the user authentication again and again but failed always. When the time is up, Vigor system will unblock that IP and allow it to access into Vigor router again.</p> <p>Blocked IP List - Open another web page which displays current blocked IPs.</p>
TLS/SSL Encryption Setup	<p>Enable SSL 3.0 and TLS 1.0/1.1/1.2 - Check the box to enable the function of SSL 3.0 and TLS 1.0/1.1/1.2 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>
AP Management	<p>Enable AP Management - Check it to enable the function of Central Management>>AP. If unchecked, menu items related to Central Management>>AP will be hidden.</p>
Device Management	<p>Check the box to enable the device management function for Vigor2762.</p> <p>Respond to external device - If it is enabled, Vigor2762 will be regarded as slave device. When the external device (master device) sends request packet to Vigor2762, Vigor2762 would send back information to respond the request coming from the external device which is able to manage Vigor2762.</p>

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

VII-1-10-2 IPv6 Management Setup

System Maintenance >> Management



IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup																																	
<p>Management Access Control</p> <p><input type="checkbox"/> Allow management from the Internet</p> <ul style="list-style-type: none"> <input type="checkbox"/> Telnet Server (Port : 23) <input type="checkbox"/> HTTP Server (Port : 80) <input type="checkbox"/> Enforce HTTPS Access <input type="checkbox"/> HTTPS Server (Port : 443) <input type="checkbox"/> SSH Server (Port : 22) <input type="checkbox"/> SNMP Server (Port : 161) <p><input checked="" type="checkbox"/> Disable PING from the Internet</p> <hr/> <p>Access List from the Internet</p> <p><input type="checkbox"/> Apply Access List to PING</p> <table border="1"> <thead> <tr> <th>List</th> <th>index in IPv6 Object</th> <th>IPv6 / Prefix</th> </tr> </thead> <tbody> <tr><td>1</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>2</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>3</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>4</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>5</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>6</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>7</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>8</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>9</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>10</td><td><input type="text"/></td><td><input type="text"/></td></tr> </tbody> </table> <p>Note: Telnet / Http server port is the same as IPv4.</p>			List	index in IPv6 Object	IPv6 / Prefix	1	<input type="text"/>	<input type="text"/>	2	<input type="text"/>	<input type="text"/>	3	<input type="text"/>	<input type="text"/>	4	<input type="text"/>	<input type="text"/>	5	<input type="text"/>	<input type="text"/>	6	<input type="text"/>	<input type="text"/>	7	<input type="text"/>	<input type="text"/>	8	<input type="text"/>	<input type="text"/>	9	<input type="text"/>	<input type="text"/>	10	<input type="text"/>	<input type="text"/>
List	index in IPv6 Object	IPv6 / Prefix																																	
1	<input type="text"/>	<input type="text"/>																																	
2	<input type="text"/>	<input type="text"/>																																	
3	<input type="text"/>	<input type="text"/>																																	
4	<input type="text"/>	<input type="text"/>																																	
5	<input type="text"/>	<input type="text"/>																																	
6	<input type="text"/>	<input type="text"/>																																	
7	<input type="text"/>	<input type="text"/>																																	
8	<input type="text"/>	<input type="text"/>																																	
9	<input type="text"/>	<input type="text"/>																																	
10	<input type="text"/>	<input type="text"/>																																	
<input type="button" value="OK"/>																																			

Available settings are explained as follows:

Item	Description
Management 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>Enable PING from the Internet - Check the checkbox to enable all PING packets from the Internet. For security issue, this function is disabled by default.</p>
Access List 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>Index in <u>IP Object</u>- Enter the index number of the IP object profile. Related IP address will appear automatically.</p>

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

VII-1-10-3 LAN Access Control

System Maintenance >> Management



IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup
<input checked="" type="checkbox"/> Allow management from LAN		
<input checked="" type="checkbox"/> FTP Server		
<input checked="" type="checkbox"/> HTTP Server <input type="checkbox"/> Enforce HTTPS Access		
<input checked="" type="checkbox"/> HTTPS Server		
<input checked="" type="checkbox"/> Telnet Server		
<input checked="" type="checkbox"/> TR069 Server		
<input checked="" type="checkbox"/> SSH Server		
Apply To Subnet		Index in <u>IP Object</u>
<input checked="" type="checkbox"/> LAN1		<input type="checkbox"/> <input type="text"/>
<input checked="" type="checkbox"/> LAN2		<input type="checkbox"/> <input type="text"/>
<input checked="" type="checkbox"/> IP Routed Subnet		<input type="checkbox"/> <input type="text"/>

Note:

If an IP Object is specified in a LAN Subnet, the setting will be applied to the selected IP only.

OK

Available settings are explained as follows:

Item	Description
Allow management from LAN	Enable the checkbox to allow system administrators to login from LAN interface. There are several servers provided by the system which allow you to manage the router from LAN interface. Check the box(es) to specify.
Apply To Subnet	Check the LAN interface for the administrator to use for accessing into web user interface of Vigor router. Index in <u>IP Object</u> - Enter the index number of the IP object profile. Related IP address will appear automatically.

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

VII-1-11 Panel Control

The behavior of the LEDs, buttons, USB ports and LAN ports on the front panel of the Vigor router can be customized as desired.

For LED

By default, the LEDs are enabled, and will illuminate or blink continuously to show the status of the various functions in the router. However, they can be configured to remain off at all times, or remain off until a button is pressed to wake them up.

System Maintenance >> Panel Control

LED	Button	USB	LAN Port	Refresh
<input checked="" type="checkbox"/> Enable LED <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Enable Sleep Mode Turn off LED after <u> 1 </u> minutes (Default: 1 minute) Status : Sleep <input type="button" value="Wake up LED"/>				

Note:

Enable the Sleep Mode will make the functions of "Wireless Button" and "Factory Reset Button" on the front panel as below:

LED Status	LED On	LED Off
Wireless Button	Wireless On/Off/WPS	Turn LED On*
Factory Reset Button	Press 1 second: Turn LED off immediately* Press till the ACT light flashing: Reset router	

*Still functional even the buttons are disabled.

Available settings are explained as follows:

Item	Description
Refresh	Click to refresh the page to display the latest information.
Enable LED	Select to enable front panel LEDs. <ul style="list-style-type: none"> ● Enable Sleep Mode/Turn off LED after _ minutes - Available when Enable LED is selected. Select this option to turn off the LEDs after the specified number of minutes. ● When sleep mode is enabled, LEDs can be woken up by pressing either the Wireless LAN ON/OFF/WPS button or the Factory Reset button on the front panel, or by clicking the Wake up LED button on this page. When LEDs are lit, they can be put to sleep by briefly pressing the Factory Reset button, or by clicking the LED sleep immediately button on this page.



<p>Status</p>	<p>Shows the status of the LEDs:</p> <p>Status : Sleep Wake up LED – LEDs are in sleep mode. To wake them up, do one of the following:</p> <ul style="list-style-type: none"> ● press the Wake up LED button on this page ● press the Wireless On/Off/WPS button on the front panel ● press the Factory Reset button on the front panel. <p>Status : Awake, sleep after 1 minutes LED sleep immediately</p> <p>– LEDs are awake. To put them to sleep immediately</p> <ul style="list-style-type: none"> ● press the LED sleep immediately button on this page ● press the Factory Reset button on the front panel for 1 second.
---------------	---

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

For Button

The Factory Reset and Wireless ON/OFF/WPS buttons on the front panel are enabled by default and can be enabled or disabled if required. Disabling the Factory Reset button will prevent tampering by unauthorized parties, or to avoid accidental triggering of a router reset when being used wake up LEDs. Disabling the wireless button will prevent changing the wireless setting when LED Sleep Mode is enabled, and the buttons are primarily used to turn the LEDs on and off.

Click the Button tab to get the following page.

System Maintenance >> Panel Control

LED	Button	USB	LAN Port	Refresh						
<table border="1"> <thead> <tr> <th>Enable</th> <th>Button</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>Factory Reset</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>Wireless</td> </tr> </tbody> </table>					Enable	Button	<input checked="" type="checkbox"/>	Factory Reset	<input checked="" type="checkbox"/>	Wireless
Enable	Button									
<input checked="" type="checkbox"/>	Factory Reset									
<input checked="" type="checkbox"/>	Wireless									

Available settings are explained as follows:

Item	Description
Refresh	Click to refresh the page to display the latest information.
Enable Factory Reset Button	The default value is Enabled. Deselect to disable the reset function of the factory reset button. Disabling the Factory Reset button only prevents it from

	being used to reboot Vigor router with default settings. It can still be used to wake up the LEDs when LED sleep mode is enabled.
Enable Wireless Button	The default value is Enabled. Deselect to disable the ability of the Wireless button to control WLAN and WPS functions. Disabling the wireless button only prevents it from being used to control WLAN functions. It can still be used to wake up the LEDs when LED sleep mode is enabled.

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

For USB

The USB ports can be individually enabled or disabled. When a USB port is disabled, attached devices will not be recognized by the router.

System Maintenance >> Panel Control

LED	Button	USB	LAN Port	Refresh									
<table border="1"> <thead> <tr> <th>Port</th> <th>Enable</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input checked="" type="checkbox"/></td> <td>No Device</td> </tr> <tr> <td>2</td> <td><input type="checkbox"/></td> <td>---</td> </tr> </tbody> </table>					Port	Enable	Status	1	<input checked="" type="checkbox"/>	No Device	2	<input type="checkbox"/>	---
Port	Enable	Status											
1	<input checked="" type="checkbox"/>	No Device											
2	<input type="checkbox"/>	---											

OK

Available settings are explained as follows:

Item	Description
Refresh	Click to refresh the page to display the latest information.
Port	The number corresponds to the USB port number shown on the front panel.
Enable	Deselect to disable the USB port. The default value is enabled.
Status	Shows the status of the USB port. No device - no USB device is connected to the port. Connected - a USB device is connected to the port. --- - the USB port is disabled.

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

For LAN Port

The 4 LAN ports can be individually enabled or disabled. When a LAN port is disabled, attached devices will not be recognized by the router.

System Maintenance >> Panel Control

LED	Button	USB	LAN Port	Refresh																				
<table border="1"> <thead> <tr> <th>Port</th> <th>Enable</th> <th>Status</th> <th>Speed</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input checked="" type="checkbox"/></td> <td>Link Up</td> <td>100Mbps</td> </tr> <tr> <td>2</td> <td><input checked="" type="checkbox"/></td> <td>Link Down</td> <td>---</td> </tr> <tr> <td>3</td> <td><input checked="" type="checkbox"/></td> <td>Link Down</td> <td>---</td> </tr> <tr> <td>4</td> <td><input type="checkbox"/></td> <td>---</td> <td>---</td> </tr> </tbody> </table>					Port	Enable	Status	Speed	1	<input checked="" type="checkbox"/>	Link Up	100Mbps	2	<input checked="" type="checkbox"/>	Link Down	---	3	<input checked="" type="checkbox"/>	Link Down	---	4	<input type="checkbox"/>	---	---
Port	Enable	Status	Speed																					
1	<input checked="" type="checkbox"/>	Link Up	100Mbps																					
2	<input checked="" type="checkbox"/>	Link Down	---																					
3	<input checked="" type="checkbox"/>	Link Down	---																					
4	<input type="checkbox"/>	---	---																					

Available settings are explained as follows:

Item	Description
Refresh	Click to refresh the page to display the latest information.
Port	The number corresponds to the LAN port number shown on the front panel.
Enable	Deselect to disable the LAN port. The default value is enabled.
Status	Shows the status of the USB port. Link Up - An active Ethernet device is connected to the port. Link Down - No active Ethernet device is detected. --- - The LAN port is disabled.
Speed	Shows the negotiated speed of the LAN port. 1000Mbps - Negotiated speed of the LAN port is 1000 Mbps. 100Mbps - Negotiated speed of the LAN port is 100 Mbps. 10Mbps - Negotiated speed of the LAN port is 10 Mbps. --- - The LAN port is disabled or there is no active device connected.

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

VII-1-12 Self-Signed Certificate

A self-signed certificate is a *unique* identification for the device (e.g., Vigor router) which generates the certificate by itself to ensure the router security. Such self-signed certificate is signed with its own private key.

The self-signed certificate will be applied in SSL VPN, HTTPS, and so on. In addition, it can be created for free by using a wide variety of tools.

System Maintenance >> Self-Signed Certificate

Self-Signed Certificate Information

Certificate Name :	self-signed
Issuer :	C=TW, ST=HsinChu, L=HuKou, O=DrayTek Corp., OU=DrayTek Support, CN=Vigor Router
Subject :	C=TW, ST=HsinChu, L=HuKou, O=DrayTek Corp., OU=DrayTek Support, CN=Vigor Router
Subject Alternative Name :	
Valid From :	Jun 2 13:05:46 2016 GMT
Valid To :	Jun 2 13:05:46 2046 GMT
PEM Format Content :	<pre> -----BEGIN CERTIFICATE----- MIIDcTCCAlmgAwIBAgIJAP67J8my6NLIMAOGCSqGSIb3DQEBCwUAMHgx CzA JBgNV BAYTA1RXMRAsDgYDVQQIEwdIc2luQ2h1MQ4wDAYDVQQHEwVIdUtvdTEWMBQGA1UE ChMNRHJheVRlayBDb3JwLjEYMBYGA1UECzMFRHJheVRlayBTdXBwb3JOMRUwEwYD VQQDEwWaWdvczB3V0ZlIwHhcNMTYwNjAyMTMwNTQ2WbcNNDYwNjAyMTMwNTQ2 WjB4MQswCQYDVQQGEwJUVzEQMA4GA1UECBMHSHNpbkNodTEOMAAGALUEBxMFSHV Lb3Ux FjAUBgNVBAoTDURyYXlUZWsgQ29ycC4xGDAWBgNVBAsTD0RyYXlUZWsgU3Vw cG9ydEVMBMGA1UEAxMMVmlnb3IgdG9yMIIBIjANBgkqhkiG9w0BAQEFAAOC AQ8AMIIBCGKCAQEAyy8jGcJhUfPcMBODHvg/jtSemVlMXJxPBd0mv780PyPvQ3QH mWLRNFLTeu9Y7Y7Yp8AdK8y0p1vxUW30hjQI6WbuKcndYzddqTx6aV6gtT09XriRU zjFcXxhLNNidtS1GYt6GiysFJR219BSudCeaAlMoeHWiVq34/juLuEcV8XqVlheX cJGvpVBAAAjDM3sWnsYCuLk51FuCRZpPcXajaS5fx9Hz0TbMy2T1oE0zudD219eX lbkqdkjX56VQlZ9G6/wQKYNBw9B015MFMik3/moLkjm8E5HbaESSJozhyFMQF9TJ bvqN1DNQH8f0Wic5tqZkIXE0gm0vyKdYAccstwIDAQABMAOGCSqGSIb3DQEBCwUA A4IBAQBZ+Jb8UxgMmipmSuSYai0JPrboigtDt3fE3SULkGGgkd04jtW1Jq0+KtUZ Ma0uU4zxEGl3tmYY5nqPTs/EGnzJI/vWxxtG1cB0vcC3EcjbTj+g0Y9WnB8Y0vJE B8QiJgIW+coPjsFCbZkzf+Rb16LAABTw7718S/qkHgFmydaqsa5L94SgKwNaijk jg6J+piagGhx6t/LY2WB3Tezb/UH5iD8SfII1C1F/yiz3w4Sg2godJsocklqZxcB LbRGK1+x0TzM5gd7W8gSZeRc0z3u0+iRfKqi0bJ0YNZDz4Kyx1WoprNG4iF7cLcR /HAPsHeloqs0Ttlx3M2yLICmrzzi -----END CERTIFICATE----- </pre>

Note:

1. Please setup the **System Maintenance >> Time and Date** correctly before you try to regenerate a self-signed certificate!!
2. The Time Zone MUST be setup correctly!!

[Regenerate](#)

Click Regeneration to open Regenerate Self-Signed Certificate 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.

Regenerate Self-Signed Certificate

Certificate Name	self-signed
Subject Alternative Name	
Type	IP Address ▾
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 ▾
Key Size	2048 Bit ▾

VII-1-13 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

Auto Reboot Time Schedule

Schedule Profile :

Note: Action and Idle Timeout settings will be ignored.

Schedule Profile - You can type in four sets of time schedule for performing system reboot. All the schedules can be set previously in **Applications >> Schedule** web page and you can use the number that you have set in that web page.

If you want to reboot the router using the current configuration, check **Using current configuration** and click **Reboot Now**. To reset the router settings to default values, check **Using factory default configuration** and click **Reboot Now**. The router will take 5 seconds to reboot the system.



Info

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.

VII-1-14 Firmware Upgrade

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://ftp.DrayTek.com).

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

System Maintenance >> Firmware Upgrade



Firmware Version Status

Current Firmware Version: 3.9.0_STD

Web Firmware Upgrade

Select a firmware file.

未選擇任何檔案

Click Upgrade to upload the file.

Note:

Upgrade using the ALL file will retain existing router configuration, whereas using the RST file will reset the configuration to factory defaults.

Choose the right firmware by clicking Select. Then, click Upgrade. The system will upgrade the firmware of the router automatically.

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

VII-1-15 Firmware Backup

The firmware for Vigor router can be saved on the host as a backup firmware. After that, if the router crashes due to the firmware error, the backup firmware will be applied to make the router run normally.

System Maintenance >> Firmware Backup

Automatic Firmware Recovery

- Enable automatic firmware recovery
If the router unexpectedly reboots three times in a row then the backup firmware will be restored to the unit on the third reboot.

Backup Setting

- Backup after reboot
 Backup after system uptime of day hour (max. 7 days)
 Backup manually

Backup Firmware: 3.9.0_RC4_STD
Last backup: 2000/01/01 23:59:59

OK

Cancel

Simply specify the condition to run the firmware backup and click OK to save the settings.

VII-1-16 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

VII-1-17 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

Note:

1. If you want to use email alert or syslog, please configure the [SysLog/Mail Alert Setup](#) page.
2. 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.
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:

Web-Filter License

[Activate](#)

[Status: **Commtouch**] [Start Date: **2011-03-28** Expire Date: **2011-04-27**]

Authentication Message

```
WebFilter, Activation authenticate fail, contact with support@draytek.com, 2011-03-28 01:00:24
```

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.

VII-1-18 Dashboard Control

There are nine groups of setting information which can be displayed on Dashboard as a reference for administrator/user. Except for Front Panel and System Information, the settings information regarding to the groups listed on this page can be hidden if required.

System Maintenance >> Dashboard Control

<input checked="" type="checkbox"/> Front Panel
<input checked="" type="checkbox"/> System Information
<input checked="" type="checkbox"/> IPv4 LAN Information
<input checked="" type="checkbox"/> IPv4 Internet Access
<input checked="" type="checkbox"/> IPv6 Internet Access
<input checked="" type="checkbox"/> Interface
<input checked="" type="checkbox"/> Security
<input checked="" type="checkbox"/> VoIP
<input checked="" type="checkbox"/> System Resource
<input checked="" type="checkbox"/> Quick Access

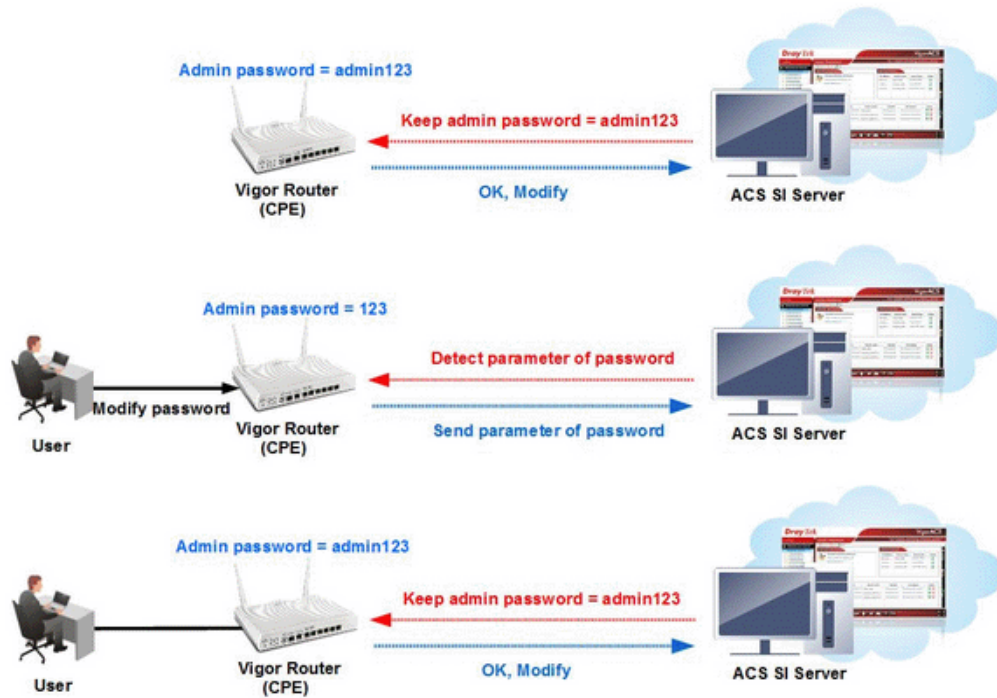
OK

Cancel

Application Notes

A-1 How to prevent CPE's settings from being changed by the end-users?

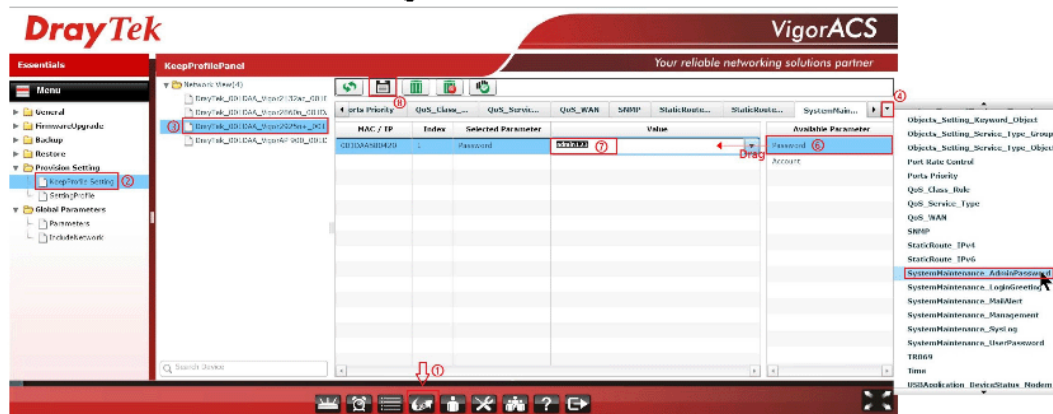
Sometimes network administrator does not wish end-users to change the configuration of CPE device. VigorACS (the administrator) server could use the KeepProfile Setting in the Provision page to always keep the parameter as original.



This document will demonstrate how to keep the admin123 as admin password via ACS SI.

Keep Profile Setup on VigorACS SI

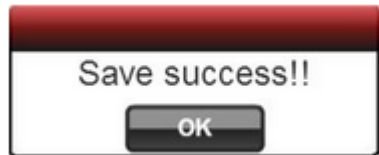
1. Setup the parameter in KeepProfile Setting



- Go to Provision page
- Click Provision Setting >> KeepProfile Setting
- From Network View, select the device which network administrator want to keep the setting

- Click on drop menu to select on the setting menu, and choose SystemMaintenance _AdminPassword
- Click Password parameter then drag it to left block
- Type admin123 in Value field
- Click Save button to save the setting

2. ACS server will pops up “Save Success” window.



3. Check ACS log: Go to Log page, select Device Action >> SetParameterLog, and we could see there's one log says that parameter has been applied.

Log ID	Device ID	Device Name	MAC Address	Device IP	User	ParameterKey	Create Time	Finish Time	Status
16	2	DrayTek_001DAA_Vigor2925r	001DAA	192.168.1.1	root	KeepSettingProfile_1456212f	2016/02/23 03:36	2016/02/23 03:36	Parameter changes have been validated and applied.
15	2	DrayTek_001DAA_Vigor2925r	001DAA	192.168.1.1	root	KeepSettingProfile_14561998	2016/02/23 11:38	2016/02/23 11:38	Parameter changes have been validated and applied.
14	2	DrayTek_001DAA_Vigor2925r	001DAA	192.168.1.1	root	KeepSettingProfile_1456128f	2016/02/22 04:05	2016/02/22 04:05	Parameter changes have been validated and applied.
13	2	DrayTek_001DAA_Vigor2925r	001DAA	192.168.1.1	root	WDSSetting_client_1456128f	2016/02/22 04:03		Parameter initiate.
12	2	DrayTek_001DAA_Vigor2925r	001DAA	192.168.1.1	root	KeepSettingProfile_1456128f	2016/02/22 04:02	2016/02/22 04:02	Parameter changes have been validated and applied.
11	3	DrayTek_001DAA_Vigor2132r	001DAA	192.168.1.11	root	WDSSetting_server_145612f	2016/02/22 04:02		Parameter initiate.
10	2	DrayTek_001DAA_Vigor2925r	001DAA	192.168.1.1	root	VPNSetting_client_14561280	2016/02/22 04:01		Parameter initiate.
9	3	DrayTek_001DAA_Vigor2132r	001DAA	192.168.1.11	root	VPNSetting_server_1456128f	2016/02/22 04:00		Parameter initiate.
8	2	DrayTek_001DAA_Vigor2925r	001DAA	192.168.1.1	root	KeepSettingProfile_1456126f	2016/02/22 03:42	2016/02/22 03:42	Parameter changes have been validated and applied.
7	2	DrayTek_001DAA_Vigor2925r	001DAA	192.168.1.1	root	KeepSettingProfile_1456121f	2016/02/22 02:05	2016/02/22 02:05	Parameter changes have been validated and applied.
6	2	DrayTek_001DAA_Vigor2925r	001DAA	192.168.1.1	root	KeepSettingProfile_1456111f	2016/02/22 11:32	2016/02/22 11:32	Parameter changes have been validated and applied.
2	2	DrayTek_001DAA_Vigor2925r	001DAA	192.168.1.1	root	GlobalParameter	2016/02/19 03:51	2016/02/19 03:51	Parameter changes fail.
1	2	DrayTek_001DAA_Vigor2925r	001DAA	192.168.1.1	root	GlobalParameter	2016/02/19 03:46	2016/02/19 03:46	Parameter changes fail.

Verifying

1. Go to the CPE router, login with the password (admin123) set in KeepProfile Setting, and it could login successfully.

2. Try to modify the admin password to 123, then check whether ACS server will detect the changes and keep the original setting.

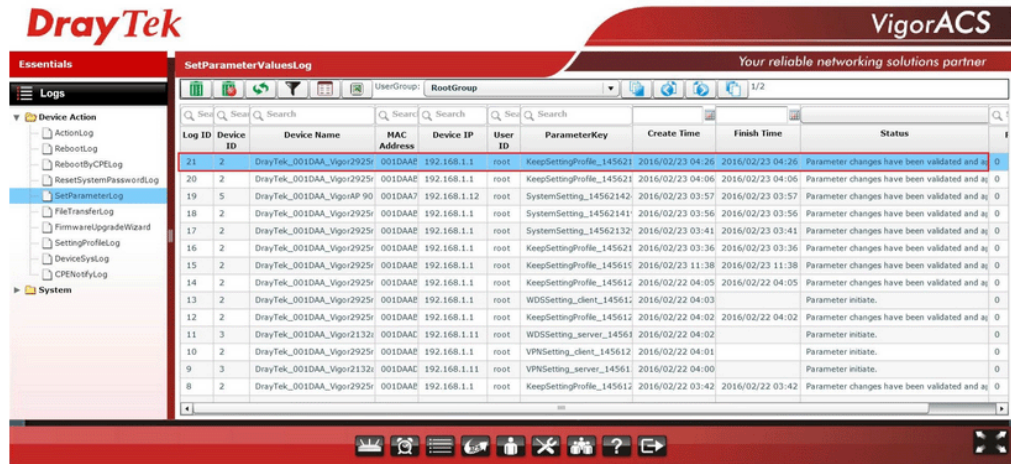
System Maintenance >> Administrator Password Setup

Administrator Password

Old Password	*****	
New Password	***	(Max. 23 characters allowed)
Confirm Password	***	(Max. 23 characters allowed)

Note: Password can contain only a-z A-Z 0-9 , ; : . " < > * + = \ | ? @ # ^ ! ()

3. Wait a period of time for CPE inform. Then from the ACS log, we will find ACS has detected the parameter difference but assigned the original value again.



4. Go back to login the router, type 123 as password, we will find the password is incorrect, which means ACS has kept the password as admin123.



VII-2 Bandwidth Management

Sessions Limit

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

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.

Quality of Service (QoS)

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?

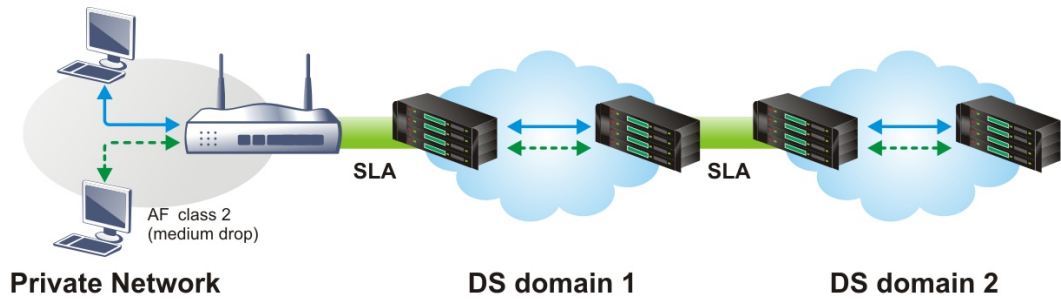
There are two components within Primary configuration of QoS deployment:

- 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, 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.

Web User Interface

Below shows the menu items for Bandwidth Management.



VII-2-1 Sessions Limit

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

Bandwidth Management >> Sessions Limit

IPv4
IPv6

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 255 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

Schedule Profile : , , ,

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	Enable - Click this button to activate the function of limit session. Disable - Click this button to close the function of limit

	<p>session.</p> <p>Default Max Sessions - Defines the default session number used for each computer in LAN.</p>
Limitation List	<p>Displays a list of specific limitations that you set on this web page.</p>
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>Enter the words which will be displayed when reaches the maximum number of Internet sessions permitted.</p> <p>Default Message - Click this button to apply the default message offered by the router.</p>
Time Schedule	<p>Schedule Profile - 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>

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

VII-2-2 Bandwidth Limit

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

Bandwidth Management >> Bandwidth Limit

IPv4
IPv6

Enable
 Disable
 IP Routed Subnet

Default Limit (Per User)

TX Limit: Kbps
 RX Limit: Kbps

Limitation List

Index	Start IP/Group	End IP/Object	TX limit	RX limit	Share

Add Entry By: IP Range
 IP Object
 Start IP:
 End IP:

Each
 Shared
 TX Limit: Kbps
 RX Limit: Kbps

Auto-Adjustment

Allow user to use more bandwidth than the assigned limit when there are bandwidth available.

Smart Bandwidth Limit

Apply the below limit to users not in Limitation List and user more than sessions

TX Limit : Kbps
 RX Limit : Kbps

Time Schedule

Schedule Profile : , , ,

Note:

1. Use "0" for TX/RX Limit for unlimited bandwidth.
2. Available bandwidth is calculated according to the maximum bandwidth detected or the Line Speed defined in WAN >> **General Setup** when in "According to Line Speed" Load Balance mode.
3. The Action and Idle Timeout settings in the Schedule Profile will be ignored.

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	Enable - Click this button to activate the function of limit bandwidth. <ul style="list-style-type: none"> ● IP Routed Subnet - Check this box to apply the bandwidth limit to the second subnet specified in LAN>>General Setup. Disable - Click this button to close the function of limit bandwidth.
Default Limit (Per User)	TX Limit - Define the default speed of the upstream for each computer in LAN. RX Limit - Define the default speed of the downstream for each computer in LAN.

<p>Limitation List</p>	<p>Display a list of specific limitations that you set on this web page.</p> <p>Add Entry By - Specify an entry with an IP address (IP address range) and limit for data transmission.</p> <p>IP Range - All the IPs within the range defined will be restricted by bandwidth limit defined by TX Limit and RX Limit below.</p> <ul style="list-style-type: none"> ● Start IP - Define the start IP address for limit bandwidth. ● End IP - Define the end IP address for limit bandwidth. <p>IP Object - All the IPs specified by the selected IP object or IP group will be restricted by bandwidth limit defined by TX Limit and RX Limit below.</p> <ul style="list-style-type: none"> ● IP Group - Specify an IP group by using the drop down list. ● IP Object - Specify an IP object by using the drop down list. <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>Edit - Allow you to edit the settings for the selected limitation.</p> <p>Delete - Remove the selected settings existing on the limitation list.</p>
<p>Allow-Adjustment</p>	<p>Allow user to use more bandwidth... - Check this box to make the best utilization of available bandwidth.</p>
<p>Smart Bandwidth Limit</p>	<p>Apply the below limit to users not in Limitation List... - Check this box to apply the following limits to users not in Limitation List and apply to the user more than sessions defined.</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>Time Schedule</p>	<p>Schedule Profile - 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>

VII-2-3 Quality of Service

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

Bandwidth Management >> Quality of Service

[Set to Factory Default](#)

Index	Enable	Direction	Inbound/ Outbound Bandwidth		Class 1	Class 2	Class 3	Others	Status
WAN1	<input type="checkbox"/>	BOTH	--Kbps/	--Kbps	25 %	25 %	25 %	25 %	Status
WAN2	<input type="checkbox"/>	BOTH	100 Mbps /	100 Mbps	25 %	25 %	25 %	25 %	Status
WAN3	<input type="checkbox"/>	BOTH	100 Mbps /	100 Mbps	25 %	25 %	25 %	25 %	Status

Note:
QoS may not work properly if the bandwidth entered is not correct. Before enable QoS, you may run speed test (from e.g., <http://speedtest.net>) or contact your ISP for the accurate bandwidth.

Class Rule

Index	Enable	Qos Class	Local Address	Remote Address	DSCP	Service Type
<input type="button" value="Add"/>						

Note:
The packets that don't match any class rules above will be classified into 'Others'

VoIP Prioritization

Enable the First Priority for VoIP SIP/RTP:
SIP UDP Port: (Default: 5060)

Tag Outbound Traffic

Class 1	<input type="checkbox"/> Add DSCP or Precedence Value	Default
Class 2	<input type="checkbox"/> Add DSCP or Precedence Value	Default
Class 3	<input type="checkbox"/> Add DSCP or Precedence Value	Default

Available settings are explained as follows:

Item	Description
General Setup	<p>Index - Display the WAN interface number link that you can edit.</p> <p>Enable - Check the box to enable the QoS function for WAN interface. If it is enabled, you can configure general QoS setting for each WAN interface.</p> <ul style="list-style-type: none"> ● Direction - Define which traffic the QoS Control settings will apply to. <ul style="list-style-type: none"> ■ IN- apply to incoming traffic only. ■ OUT- apply to outgoing traffic only. ■ BOTH- apply to both incoming and outgoing traffic. ● Inbound/Outbound Bandwidth - Set the connecting rate of data input/output for other WAN. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 1000kbps for this box. The default value is 10000kbps. ● Class 1 ~ 3 / Others - Define the ratio of bandwidth to upstream speed and bandwidth to downstream speed. There are four queues allowed for QoS control. The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. In which, the "Others" field is used for the packets which are not suitable for the three class

Item	Description
	rules. Status - Display the online statistics of WAN interface.
Class Rule	Set detailed settings for the selected Class. Index - Display the class number that you can edit. Enable - QoS Class - Local Address - Remote Address - DSCP - Service Type - Display detailed settings for the service type. Add - Click it to create a class rule for QoS.
VoIP Prioritization	Enable the First Priority for VoIP SIP/RTP - When this feature is enabled, the VoIP SIP/UDP packets will be sent with highest priority. SIP UDP Port - Set a port number used for SIP.
Tag Outbound Traffic	Add DSCP or Precedence Value for Class 1 to Class 3 -

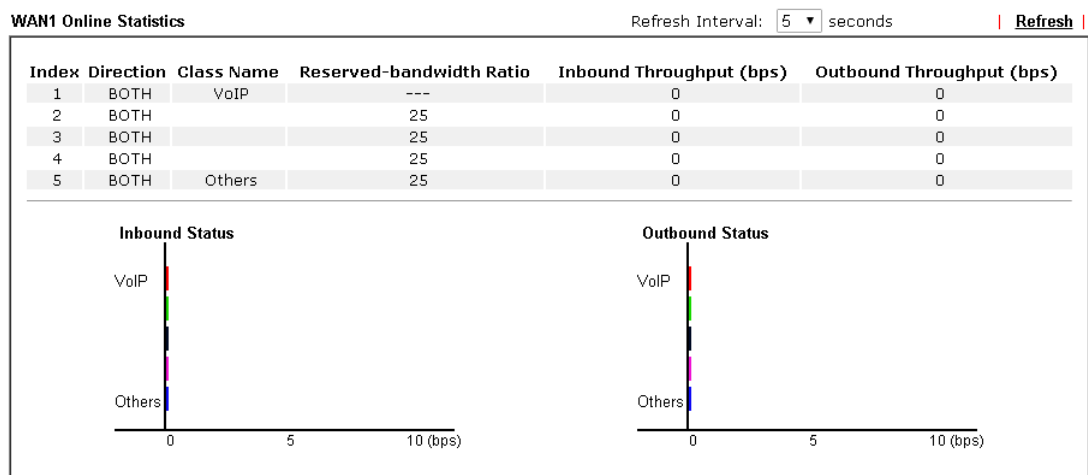
This page displays the QoS settings result of the WAN interface. Click the Setup link to access into next page for the general setup of WAN interface. As to class rule, simply click the Edit link to access into next for configuration.

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

Online Statistics

Display an online statistics for quality of service for your reference. This feature is available only when the Quality of Service for WAN interface is enabled.

Bandwidth Management >> Quality of Service



Cancel

General Setup for WAN Interface

Click WAN interface number link to configure the limited bandwidth ratio for QoS of the WAN interface.

Bandwidth Management >> Quality of Service >> WAN1

Enable UDP Bandwidth Control
Limited_bandwidth Ratio %

Outbound TCP ACK Prioritize

Available settings are explained as follows:

Item	Description
Enable UDP Bandwidth Control	Set the limited bandwidth ratio. This is a protection of TCP application traffic since UDP application traffic such as streaming video will exhaust lots of bandwidth. Limited_bandwidth Ratio - The ratio typed here is reserved for limited bandwidth of UDP application.
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.



Info

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.

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 Add / Edit button of that one.

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

Index	Enable	Direction	Inbound/ Outbound Bandwidth		Class 1	Class 2	Class 3	Others	Status
			--Kbps/	--Kbps	%	%	%	%	
WAN1	<input type="checkbox"/>	BOTH			25	25	25	25	Status
WAN2	<input type="checkbox"/>	BOTH	100	100	25	25	25	25	Status
WAN3	<input type="checkbox"/>	BOTH	100	100	25	25	25	25	Status


Note:
QoS may not work properly if the bandwidth entered is not correct. Before enable QoS, you may run speed test (from e.g., <http://speedtest.net>) or contact your ISP for the accurate bandwidth.

Class Rule

Index	Enable	Qos Class	Local Address	Remote Address	DSCP	Service Type
<input type="button" value="Add"/>						

Note:
The packets that don't match any class rules above will be classified into 'Others'

VoIP Prioritization

Enable the First Priority for VoIP SIP/RTP:
SIP UDP Port: (Default: 5060) 

Tag Outbound Traffic

Class 1	<input type="checkbox"/> Add DSCP or Precedence Value	Default
Class 2	<input type="checkbox"/> Add DSCP or Precedence Value	Default
Class 3	<input type="checkbox"/> Add DSCP or Precedence Value	Default

- For adding a new rule, click Add to open the following page.

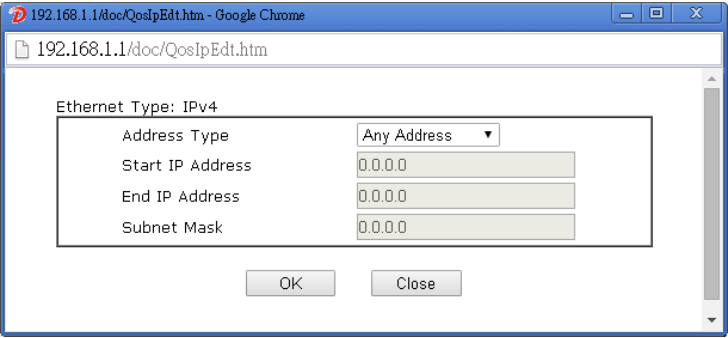
Bandwidth Management >> Quality of Service

Rule 1

<input type="checkbox"/> Enable	<input type="checkbox"/> Hardware Acceleration
IP Version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Local IP Address	Any <input type="button" value="Edit"/>
Remote IP Address	Any <input type="button" value="Edit"/>
DiffServ CodePoint	ANY
Service Type	DNS(TCP/UDP:53)
QoS Class	Class 1

Available settings are explained as follows:

Item	Description
Enable	Check this box to invoke these settings.
Hardware Acceleration	Check this box to enable the hardware acceleration when such rule is applied.
IP Version	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.

<p>Remote Address</p>	<p>Click the Edit button to set the remote IP address (on LAN/WAN) for the rule.</p>  <p>Address Type - Determine the address type for the source address. For Single Address, you have to fill in Start IP address. For Range Address, you have to fill in Start IP address and End IP address. For Subnet Address, you have to fill in Start IP address and Subnet Mask.</p>
<p>DiffServ CodePoint</p>	<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>
<p>Service Type</p>	<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>
<p>QoS Class</p>	<p>Specify the QoS class (1, 2 or 3) for this rule.</p>

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

Bandwidth Management >> Quality of Service

General Setup [Set to Factory Default](#)

Index	Enable	Direction	Inbound/ Outbound Bandwidth		Class 1	Class 2	Class 3	Others	Status
			--Kbps/	--Kbps					
WAN1	<input type="checkbox"/>	BOTH			25 %	25 %	25 %	25 %	Status
WAN2	<input type="checkbox"/>	BOTH	100 Mbps	100 Mbps	25 %	25 %	25 %	25 %	Status
WAN3	<input type="checkbox"/>	BOTH	100 Mbps	100 Mbps	25 %	25 %	25 %	25 %	Status

Note:

QoS may not work properly if the bandwidth entered is not correct. Before enable QoS, you may run speed test (from e.g., <http://speedtest.net>) or contact your ISP for the accurate bandwidth.

Class Rule

Index	Enable	Qos Class	Local Address	Remote Address	DSCP	Service Type
1	<input type="checkbox"/>	Class 1	Any	Any	ANY	DNS(TCP/UDP:53)

Note:

The packets that don't match any class rules above will be classified into 'Others'

VoIP Prioritization

Enable the First Priority for VoIP SIP/RTP:
SIP UDP Port: (Default: 5060) 

Tag Outbound Traffic

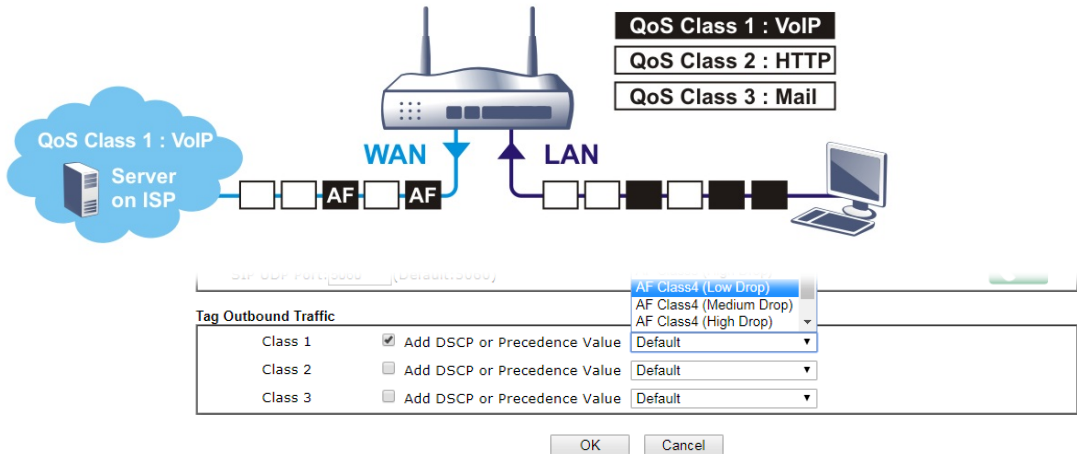
Class 1	<input type="checkbox"/>	Add DSCP or Precedence Value	Default
Class 2	<input type="checkbox"/>	Add DSCP or Precedence Value	Default
Class 3	<input type="checkbox"/>	Add DSCP or Precedence Value	Default

You can set up to 20 rules and 10 service types for a Class. If you want to edit an existed rule, please click index number of the rule to open the rule edit page for modification.

Retag the Packets for Identification

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

For example, in the following illustration, the VoIP packets in LAN go into Vigor router without any header. However, when they go forward to the Server on ISP through Vigor router, all of the packets are tagged with AF (configured in Bandwidth >>QoS>>Class) automatically.



VII-2-4 APP QoS

The QoS function is used to do bandwidth management for the services with certain IP or port number. However, there is no effect of bandwidth management on the service such as VNC or PPTV without fixed IP or port number.

APP QoS employs the function of APP Enforcement to detect the types of software in application layer. By combining the function of QoS (adjustment on Inbound/Outbound bandwidth and bandwidth ratio), Vigor router can perform the bandwidth management for the protocols, streaming, remote control, web HD and so on.

Click Bandwidth Management>>APP QoS to open the following page.

Bandwidth Management >> APP QoS

APP QoS

Enable Disable

Traceable Untraceable

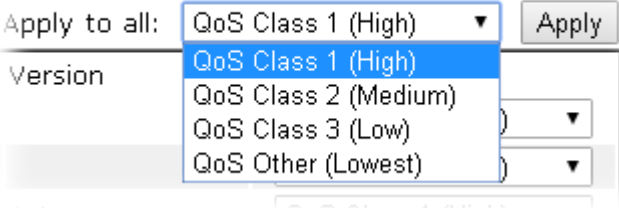
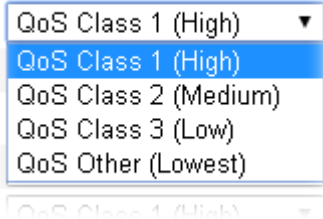
Apply to all: QoS Class 1 (High) ▼

Enable	Protocol	Version	Action
<input type="checkbox"/>	DNS		QoS Class 1 (High) ▼
<input type="checkbox"/>	FTP		QoS Class 1 (High) ▼
<input type="checkbox"/>	HTTP	1.1	QoS Class 1 (High) ▼
<input type="checkbox"/>	IMAP	4.1	QoS Class 1 (High) ▼
<input type="checkbox"/>	IMAP STARTTLS	4.1	QoS Class 1 (High) ▼
<input type="checkbox"/>	IRC	2.4.0	QoS Class 1 (High) ▼
<input type="checkbox"/>	NNTP		QoS Class 1 (High) ▼
<input type="checkbox"/>	POP3		QoS Class 1 (High) ▼
<input type="checkbox"/>	POP3 STARTTLS		QoS Class 1 (High) ▼
<input type="checkbox"/>	QUIC	Q025	QoS Class 1 (High) ▼
<input type="checkbox"/>	SMB	3.0	QoS Class 1 (High) ▼
<input type="checkbox"/>	SMTP		QoS Class 1 (High) ▼
<input type="checkbox"/>	SMTP STARTTLS		QoS Class 1 (High) ▼
<input type="checkbox"/>	SNMP	2C	QoS Class 1 (High) ▼
<input type="checkbox"/>	SSH	2	QoS Class 1 (High) ▼
<input type="checkbox"/>	SSL/TLS	3.0/1.2	QoS Class 1 (High) ▼
<input type="checkbox"/>	TELNET		QoS Class 1 (High) ▼

Note:
Please remember to adjust Inbound/Outbound bandwidth of your network in "Quality of Service". This will help QoS to work more efficient.

Available settings are explained as follows:

Item	Description
Enable/Disable	Click Enable to activate APP QoS function. Click Disable to deactivate APP QoS function.
Traceable	The protocol listed below is traceable by Vigor router. Each tab offers different types of protocols to fit your request.

Untraceable	<p>The protocol listed below is not easy to be traced by Vigor router.</p> <p>Each tab offers different types of protocols to fit your request.</p>
Select All	Click it to select all of the protocols.
Clear All	Click it to de-select all of the protocols.
Apply to all	<p>Choose one of the actions from the drop down list. It is prepared for applying to all protocols.</p>  <p>Apply - Click it to make the selected action be applied all of the selected protocols immediately.</p>
Action	<p>There are many protocols which can be specified with different QoS Class.</p> 

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

VII-3 Hotspot Web Portal

The Hotspot Web Portal feature allows you to set up profiles so that LAN users could either be redirected to specific URLs, or be shown messages when they first connect to the Internet through the router. Users could be required to read and agree to terms and conditions, or authenticate themselves, prior to gaining access to the Internet. Other potential uses include the serving of advertisements and promotional materials, and broadcast of public service announcements.

Web User Interface

LAN
Hotspot Web Portal
Profile Setup
Quota Management
Routing

VII-3-1 Profile Setup

Select Profile Setup to create or modify Portal profiles. Up to 4 profiles can be created to meet different requirements according to LAN subnets, WLAN SSIDs, origin and destination IP addresses, etc.

Hotspot Web Portal >> Profile Setup



Hotspot Web Portal Profile:

Index	Enable	Comments	Login Mode	Applied Interface	
1.	<input type="checkbox"/>		Click-through	None	Preview
2.	<input type="checkbox"/>		Click-through	None	Preview
3.	<input type="checkbox"/>		Click-through	None	Preview
4.	<input type="checkbox"/>		Click-through	None	Preview

Note:

1. The router must connect to the Internet before webpage redirection will work.
2. If the LAN clients are using another DNS server on LAN, please make sure the DNS query for domain name "portal.draytek.com" will be resolved by the router.

[OK](#)

Available settings are explained as follows:

Item	Description
Index	Click the index number link to view or update the profile settings.
Enable	Check the box to enable the profile.
Comments	Shows the description of the profile.
Login Mode	Shows the login mode used by the profile. See the section <i>Login Mode</i> for details.

Applied Interface	Shows the interfaces to which this profile applies.
Preview	Click this button to preview the Hotspot Web Portal page that will be displayed to users.

VII-3-1-1 Login Method

There are several login methods to choose from for authenticating network clients. Each login mode will present a different web page to users when they connect to the network.

(A) Skip Login, landing page only

This mode does not perform any authentication. The user will be redirected to the landing page. The user can then leave the landing page to visit other websites.

(B) Click-through

The following page will be shown to the users when they first attempt to access the Internet through the router. After clicking Accept on the page, users will be directed to the landing page (defined in Captive Portal URL) and be granted access to the Internet.

(C) Various Hotspot Login

An authentication page will appear when users attempt to access the Internet for the first time via the router. After authenticating themselves using a Facebook, Google account, PIN code, password for RADIUS sever, they will be directed to the landing page and be granted access to the Internet.

(D) External Portal Server

External RADIUS server will authenticate the users when they attempt to access the Internet for the first time via the router.

VII-3-1-2 Steps for Configuring a Web Portal Profile



1 Login Method

Click the index link (e.g., #1) of the selected profile to display the following page.



Enable this profile

Comments:

Portal Server

- Portal Method**
- Skip Login, landing page only
 - Click through
 - Various Hotspot Login
 - External Portal Server

Captive Portal URL

Login Methods

- Choose Login Method**
- Login with Facebook
Note : When Login with Facebook is selected, the protocol of the Captive Portal URL will be changed to HTTPS.
 - Login with Google
 - Receive PIN via SMS
 - Login with RADIUS

Available settings are explained as follows:

Item	Description
Enable this profile	Check to enable this profile.
Comments	Enter a brief description to identify this profile.
Portal Server	
Portal Method	There are four methods to be selected as for portal server. <input type="radio"/> Skip Login, landing page only <input type="radio"/> Click through <input checked="" type="radio"/> Various Hotspot Login <input type="radio"/> External Portal Server
Captive Portal URL	Enter certain URL as captive portal URL.
Redirection URL	It is available when External Portal Server is selected as portal method. Enter the URL to redirect the client.
RADIUS Server	It is available when External Portal Server is selected as portal method. Specify authentication method, enable RADIUS MAC authentication

	and choose MAC address format.
Login Methods	
Choose Login Method	<p>It is available when Various Hotspot Login is selected as portal method. Select and check desired login method(s)</p> <p><input type="checkbox"/> Login with Facebook</p> <p><input type="checkbox"/> Login with Google</p> <p><input type="checkbox"/> Receive PIN via SMS</p> <p><input type="checkbox"/> Login with RADIUS</p>
Facebook	<p>It appears when Login with Facebook is selected as login method.</p> <p>Facebook APP ID - Enter a valid Facebook developer app ID. If you do not already have an app ID, refer to section A-1 <i>How to create a Facebook App ID for Web Portal Authentication</i> for instructions on obtaining an APP ID.</p> <p>Facebook APP Secret - Enter the secret configured for the APP ID entered above. Refer to section A-1 <i>How to create a Facebook App ID for Web Portal Authentication</i> for details.</p>
Google	<p>It appears when Login with Google is selected as login method.</p> <p>Google App ID - Enter a valid Google app ID. If you do not already have an app ID, refer to section A-2 <i>How to create a Google App ID for Web Portal Authentication</i> for instructions on obtaining an APP ID.</p> <p>Google App Secret - Enter the secret configured for the APP ID entered above. Refer to section A-2 <i>How to create a Google APP ID for Web Portal Authentication</i> for details.</p>
SMS Provider	<p>It appears when Receive PIN via SMS is selected as login method.</p> <p>Receiving PIN via SMS Provider - Select the SMS Provider used to send PIN notifications SMS providers are configured in Objects Setting >> SMS / Mail Service Object.</p>
Radius Server	<p>It appears when Login with RADIUS is selected as login method.</p> <p>Authentication Method - Choose an external RADIUS server for authenticating web portal client.</p> <p>RADIUS MAC Authentication - Check Enable to activate user authentication by MAC address.</p> <p>MAC Address Format - Select a desirable format for MAC address.</p>
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to save the configuration on this page and proceed to the next page.

If you have chosen Skip Login, landing page only or External Portal Server as the portal method, skip to step 4 *Whitelisting* below.

Otherwise, proceed to configure the login page by following steps 2 and 3.

2 Background

If you have selected a Login Mode that requires authentication, select a background for the login page.

Hotspot Web Portal >> ProfileSetup

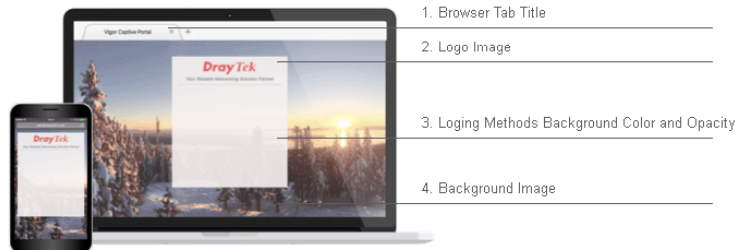


Choose Login Background

Color Background



Image Background



Browser Tab Title

Logo Image




Logo Background Color (format : FFFFFFFF)

Login Method Background Color (format : FFFFFFFF)

Available settings are explained as follows:

Item	Description
Choose Login Background	Select either Color Background or Image Background as the login page background scheme.
Browser Tab Title	Enter the text to be shown as the webpage title in the browser.

Logo Image	The DrayTek Logo will be displayed by default. However, you can enter HTML text or upload an image to replace the default logo.
Login Method Background Color	Select the background color of the login panel from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color. 
Opacity (10 ~ 100)	Available when Image Background is selected. Set the opacity of the background image.
Background Image	Available when Image Background is selected. Click Browse... to select an image file (.JPG or .PNG format), then click Upload to upload it to the router.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

If you have selected Skip Login, landing page only or External Portal Server as the portal method, proceed to Step 4 *Whitelist Setting*; otherwise, continue to Step 3 *Login Page Setup*.

3 Login Page Setup

In this step you can configure settings for the login page.

Click Through

This section describes the Login Page setup if you have selected Click Through as the Login Method.

Hotspot Web Portal >> Profile Setup



Configure Login Method and Details

Welcome!

We are pleased to provide free Wi-Fi to you!

By clicking the button below you agree to the [Terms and Conditions](#)

Accept

Welcome Message

Terms and Conditions Description and Content

Accept Button Description and Color

Welcome Message

Welcome!
Please log in to enjoy Wi-Fi.

(Max 1360 characters) Default

Terms and Conditions Description

By clicking the button below you agree to the Terms and Conditions.

(Max 170 characters) Default

Terms and Conditions Content

(Max 1360 characters)

Accept Button Description

Submit

(Max 170 characters) Default

Accept Button Color

Customize Color

A2A2A2

(format : FFFFFFFF)

Preview

Default

Save and Next

Cancel

Available settings are explained as follows:

Item	Description
Welcome Message	Enter the text to be displayed as the welcome message.
Terms and	Enter the text to be displayed as the Terms and Conditions

Conditions Description	hyperlink text.
Terms and Conditions Content	Enter the text to be displayed in the Terms and Conditions pop-up window.
Accept Button Description	Enter the text to be displayed on the accept button
Accept Button Color	Select the color of the accept button from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

Various Hotspot Login

This section describes the Login Page setup step if you have selected Various Hotspot Login the login method. You will see only settings that are relevant to the selected login method(s).

Hotspot Web Portal >> Profile Setup



Configure Login Method and Details

<p>Welcome! Please log in to enjoy Wi-Fi.</p> <p>By clicking the button below you agree to the Terms and Conditions</p> <p> Log in with Facebook</p> <p> Log in with Google</p> <p>Or log in with PIN code.</p> <p>Receive PIN via SMS</p> <p>Enter Existing PIN <input type="button" value="Submit"/></p> <p>Or log in with your account.</p> <p>Username <input type="text"/></p> <p>Password <input type="password"/></p> <p><input type="button" value="Login"/></p>	<p>Welcome Message</p> <hr/> <p>Terms and Conditions Description and Content</p> <p>Facebook Login</p> <hr/> <p>Google Login</p> <hr/> <p>Hint Message for PIN</p> <hr/> <p>Receive PIN via SMS Description</p> <hr/> <p>Enter PIN and Submit Button</p> <hr/> <p>Hint Message for RADIUS</p> <hr/> <p>RADIUS Login</p>
--	---

Welcome Message	<p>Welcome! Please log in to enjoy Wi-Fi.</p> <p>(Max 1360 characters) <input type="button" value="Default"/></p>
Terms and Conditions Description	<p>By clicking the button below you agree to the Terms and Conditions.</p> <p>(Max 170 characters) <input type="button" value="Default"/></p>
Terms and Conditions Content	<p>(Max 1360 characters)</p>

Settings that are common to Facebook, Google, PIN, and RADIUS authentication are:

Item	Description
Welcome Message	Enter the text to be displayed as the welcome message.
Terms and Conditions Description	Enter the text to be displayed as the Terms and Conditions hyperlink text.
Terms and Conditions Content	Enter the text to be displayed in the Terms and Conditions pop-up window.

If you have selected Facebook login, the setting will appear:

Facebook Login Description

(Max 170 characters)

Item	Description
Facebook Login Description	Enter the text to be displayed on the Facebook login button.

If you have selected Google login, the setting will appear:

Google Login Description

(Max 170 characters)

Item	Description
Google Login Description	Enter the text to be displayed on the Google login button.

If you have selected PIN login, these settings will appear:

Hint Message for PIN	<div style="border: 1px solid #ccc; padding: 5px; min-height: 40px;">Log in with PIN code.</div> <p>(Max 170 characters)</p> <p style="text-align: right;">Default</p>
Receiving PIN via SMS Description	<div style="border: 1px solid #ccc; padding: 5px; min-height: 30px;">Receive PIN via SMS</div> <p>(Max 170 characters)</p> <p style="text-align: right;">Default</p>
Receiving PIN via SMS Content	<div style="border: 1px solid #ccc; padding: 5px; min-height: 30px;">Welcome to DrayTek Hotspot! Your PIN is <PIN>. This PIN is valid for 10 min.</div> <p>(Max 150 characters)</p> <p style="text-align: right;">Default</p>
Enter PIN Description	<div style="border: 1px solid #ccc; padding: 5px; min-height: 30px;">Enter Existing PIN</div> <p>(Max 170 characters)</p> <p style="text-align: right;">Default</p>
Submit Button Description	<div style="border: 1px solid #ccc; padding: 5px; min-height: 30px;">Submit</div> <p>(Max 170 characters)</p> <p style="text-align: right;">Default</p>
Submit Button Color	<div style="border: 1px solid #ccc; padding: 5px; min-height: 30px;"> Customize Color </div> <div style="display: flex; align-items: center; margin-top: 5px;"> <div style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 5px;">A2A2A2</div> (format : FFFFFFFF) <div style="margin-left: 20px;">Preview</div> <div style="margin-left: 100px;">Default</div> </div>

Item	Description
Hint Message for PIN	Enter the text used to suggest users to choose SMS authentication.
Receiving PIN via SMS Description	Enter the text to be displayed on the button that the user clicks to receive an SMS PIN.
Receiving PIN via SMS Content	Enter the message to be sent by SMS to inform the user of the PIN. The PIN variable is specified by <PIN> within the message.
Enter PIN Description	Enter message to be displayed in the PIN textbox to prompt the user to enter the PIN.
Submit Button Description	Enter the text to be displayed on the submit PIN button
Submit Button Color	Select the color of the submit button from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.

If you have selected RADIUS account login, these settings will appear:

Hint Message for RADIUS	<input type="text" value="Log in with your account."/> (Max 170 characters) <input type="button" value="Default"/>
RADIUS Account Description	<input type="text" value="Username"/> (Max 170 characters) <input type="button" value="Default"/>
RADIUS Password Description	<input type="text" value="Password"/> (Max 170 characters) <input type="button" value="Default"/>
Login Button Description	<input type="text" value='Login'/> (Max 170 characters) <input type="button" value="Default"/>
Login Button Color	<input type="button" value="Customize Color"/> <input type="text" value="A2A2A2"/> (format : FFFFFFFF) <input type="button" value="Preview"/> <input type="button" value="Default"/>

Item	Description
Hint Message for RADIUS	Enter the text used to suggest users to choose RADIUS authentication.
RADIUS Account Description	Enter a brief description for reminding the user about the account.
RADIUS Password Description	Enter a brief description for reminding the user about the password.
Login Button Description	Enter the text to be displayed on the login button.
Login Button Color	Select the color of the login button from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.

And finally, the save and cancel buttons are always displayed.

Item	Description
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

2nd-stage Page for PIN Login

If you have selected PIN Login as the login method, you will also need to configure the page that is displayed to users when they request a PIN.

Hotspot Web Portal >> Profile Setup



Configure 2nd-stage Page for SMS Login

< Back

PIN Code will be sent over via SMS.

+ 886

Send PIN

Submit

Back Button

PIN Code Message

Default Country, Enter Mobile Number Description

Send Button Description and Color

Send Succeeded Message

Enter PIN and Submit Button

Back Button Description

Back

(Max 170 characters) Default

PIN Code Message

PIN code will be sent over via SMS.

(Max 170 characters) Default

Default Country Code + 93 Afghanistan

Enter Mobile Number Description

enter your mobile number

(Max 170 characters) Default

Send Button Description

Send PIN

(Max 170 characters) Default

Send Button Color

Customize Color
A2A2A2
(format : FFFFFFFF)
Preview
Default

Send Succeeded Message

PIN Code has been sent.Click Send PIN again if not receiving PIN in 3 minutes.

(Max 170 characters) Default

Save and Next
Cancel

Available settings are explained as follows:

Item	Description
Back Button Description	Enter text for the label of the hyperlink to return to the previous page.
PIN Code Message	Enter text to be displayed as the body text on the page.
Default Country	Select the default country code to be displayed using the dropdown

Code	menu.
Enter Mobile Number Description	Enter message to be displayed in the mobile number textbox to prompt the user to enter the mobile number.
Send Button Description	Enter the label text of the send button.
Send Button Color	Select the color of the send button from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.
Send Succeeded Message	Enter text to be displayed to notify the user after the PIN has been sent.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

4 Whitelist Setting

In this step you can configure the whitelist settings. Users are allowed to send and receive traffic that satisfies whitelist settings.

Hotspot Web Portal >> Profile Setup



NAT Rules	Dest Domain	Dest IP	Dest Port	Source IP
Always allow outbound connections from hosts in		<input type="checkbox"/> NAT >> Port Redirection <input type="checkbox"/> NAT >> Open Ports <input type="checkbox"/> NAT >> DMZ		

Save and Next

Cancel

Available settings are explained as follows:

Item	Description
NAT Rules	To prevent web portal settings from conflicting with NAT rules resulting in unexpected behavior, select the NAT rules that are allowed to bypass the web portal. Hosts listed in selected NAT rules can always access the Internet without being intercepted by the web portal.
Dest Domain	Enter up to 30 destination domains that are allowed to be accessed.
Dest IP	Enter up to 30 destination IP addresses that are allowed to be accessed.
Dest Port	Enter up to 30 destination protocols and ports that are allowed through the router.
Source IP	Enter up to 30 source IP addresses that are allowed through the router.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

5 More Options

In this step you can configure advanced options for the Hotspot Web Portal.

Hotspot Web Portal >> Profile Setup



Quota Management

Login Method	Quota Policy Profile	Valid Time	Device Allowed	Bandwidth Limit	Session Limit
RADIUS Login	1.Default	0d 5h 0m	Unlimited	Unlimited	Unlimited

Note:

To modify the quota settings, please go to [Hotspot Web Portal >> Quota Management](#)

Web Portal Options

HTTPS Redirection

Enable

When an unauthenticated client opening a HTTPS page, redirect will work but certificate errors may be shown. Disable this function to redirect only HTTP pages. HTTPS browsing will timeout without redirection and also no certificate errors.

Captive Portal Detection

Enable

Trigger the unauthenticated client to automatically pop-up the Web Portal page when connects to Wi-Fi. This function is not available when using **Social Login** because the page may not be shown correctly due to the limitation of the OS built-in Captive Portal Detection.

Landing Page After Authentication

- Fixed URL
- User Requested URL
- Bulletin Message

(Max 511 characters)

Default Message

Note:

Landing Page may not be shown correctly when using OS built-in Captive Portal Detection.

Applied Interfaces

Subnet		<input type="checkbox"/> LAN1 <input type="checkbox"/> LAN2
WLAN	2.4G	<input type="checkbox"/> SSID1 (DrayTek)
		<input type="checkbox"/> SSID2 (DrayTek_Guest)
		<input type="checkbox"/> SSID3
		<input type="checkbox"/> SSID4
	5G	<input type="checkbox"/> SSID1 (DrayTek_5G)
		<input type="checkbox"/> SSID2 (DrayTek_5G_Guest)
		<input type="checkbox"/> SSID3
		<input type="checkbox"/> SSID4

Available settings are explained as follows:

Item	Description
Quota Management	
Quota Policy Profile	Choose a policy profile to apply to web portal client.
Web Portal Options	
HTTPS Redirection	If this option is selected, unauthenticated clients accessing HTTPS

	websites will be redirected to the login page, but the browser may alert the user of certificate errors. If this option is not selected, attempts to access to HTTPS website will time out without redirection.
Captive Portal Detection	If this option is selected, the web portal page is triggered automatically when an unauthenticated client tries to access the Internet. This function is not available when the Login Mode is Social Login, as the web portal page may not be shown correctly due to the limitations of the operating system's built-in Captive Portal Detection.
Landing Page After Authentication	
Fixed URL	Specifies the webpage that will be displayed after the user has successfully authenticated. The user will be redirected to the specified URL. This could be used for displaying advertisements to users, such as guests requesting wireless Internet access in a hotel.
User Requested URL	The user will be redirected to the URL they initially requested.
Bulletin Message	The message configured here will be briefly shown for a few seconds to the user. Default Message - This button is enabled when Bulletin Message is selected. Click to load the default text into the bulletin message textbox.
Applied Interfaces	
Subnet	The current Hotspot Web Portal profile will be in effect for the selected subnets.
WLAN	The current Hotspot Web Portal profile will be in effect for the selected WLAN SSIDs.
Finish	Click to complete the configuration.
Cancel	Click to abort the configuration process and return to the profile summary page.

VII-3-2 Quota Management

The system administrator can specify bandwidth and sessions quota which is only applicable to the web portal clients.

Settings configured in Quota Management will override the policies set in Bandwidth Management>>Bandwidth Limit and Bandwidth Management>>Limit.

Hotspot Web Portal >> Quota Management

Web Portal Bandwidth and Session Limit

The settings here will apply only to the web portal clients and will override the policies set in Bandwidth Management.

Bandwidth Limit

Session Limit

Quota Policy Profile

Index	Name	Expired Time after First Login	Device Allowed per Account	Reconnection Time Restriction	Bandwidth Limit	Session Limit
1	Default	0d 5h 0m	Unlimited	Unlimited	Unlimited	Unlimited
<input type="button" value="Add"/> (up to 20)						

Available settings are explained as follows:

Item	Description
Bandwidth Limit	Check the box to override the policy configured in Bandwidth Management>>Bandwidth Limit.
Session Limit	Check the box to override the policy configured in Bandwidth Management>>Session Limit.
Quota Policy Profile	Add - Create up to 20 policy profiles in such page.

To create a new quotal policy profile, click Add to open the following page.

Hotspot Web Portal >> Management >> Quota Policy Profile 2

Profile Name

Account Validity

Expired Time After the First Login days hours min

Idle Timeout min

Device Control

Devices Allowed per account

Reconnection Time Restriction At : everyday

Block the same user from reconnecting before the set time

hours min

Block the same user from reconnecting for the set period

Bandwidth and Session Limit

Bandwidth Limit

Download Limit Kbps Mbps

Upload Limit Kbps Mbps

Session Limit sessions

Available settings are explained as follows:

Item	Description
Profile Name	Enter a name for a new profile.
Account Validity	Set a period of valid time for the client accessing Internet via web portal. Expired Time After the First Login - Set the days, hours, and minutes. After expired time, Vigor router will block the client to access into network/Internet. Idle Timeout - After checking the box, Vigor router will terminate the network connection if no activity for the user account after the time configured here.
Device Control	Set the number of devices that each account can control, and specify the time restriction for the client accessing Internet via web portal. Decices Allowed per account - Use the drop-down list to select a number. Each account allows the number of devices (defined here) for accessing into network. Reconnection Time Restriction - For each account, Vigor router can set a time for network connection <ul style="list-style-type: none"> ● At ... Everyday - Set the time to block the same client from reconnecting Vigor router before the time set here. ● Hours. . min - Set the time period to block the same client from reconnecting Vigor router.
Bandwidth and	Bandwidth Limit - Check the box to configure bandwidth limit for

Session Limit	web portal client. ● Download/Upload Limit - Set a value. Session Limit- Check the box to configure session limit for web portal client.
---------------	--

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

Application Notes

A-1 How to allow users login to Vigor’s Hotspot with their social media accounts (e.g., Facebook & Google)

Vigor Router supports Hotspot Web Portal function. The network administrator can set Vigor Router as a Hotspot provider with web authentication and allow users to log in with their social media accounts, such as Facebook and Google. We demonstrate how to set up the hotspot web portal with Facebook login in the following paragraphs.

Vigor Router Setup

1. Make sure the router is connected to the Internet.

Online Status

Physical Connection			System Uptime: 0day 0:11:28		
IPv4		IPv6			
LAN Status		Primary DNS: 168.95.1.1		Secondary DNS: 168.95.192.1	
IP Address	TX Packets	RX Packets			
192.168.60.1	5,950	6,130			
WAN 1 Status					>> Drop PPPoE
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:11:23	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
192.168.1.254	192.168.1.1	5,041	215	5,689	393

2. Go to Hotspot Web Portal >> Profile Setup, click on an available index.

Hotspot Web Portal >> Profile Setup

Hotspot Web Portal Profile:

Index	Enable	Comments	Login Mode	Applied Interface	
1.	<input type="checkbox"/>		Click-through	None	Preview
2.	<input type="checkbox"/>		Click-through	None	Preview
3.	<input type="checkbox"/>		Click-through	None	Preview
4.	<input type="checkbox"/>		Click-through	None	Preview

Note:

1. The router must connect to the Internet before webpage redirection will work.
2. If the LAN clients are using another DNS server on LAN, please make sure the DNS query for domain name "portal.draytek.com" will be resolved by the router.

OK

3. Enter the values as the following figure.

Enable this profile **a**

Comments: **b**

Portal Server

Portal Method Skip Login, landing page only
 Click through
 Various Hotspot Login **c**

Captive Portal URL **f**

Login Methods

Choose Login Method Login with Facebook **d**
 Login with Google
 Receive PIN via SMS

Facebook

Facebook APP ID **e**

Facebook APP Secret

Google

Google App ID

Google App Secret

- (a) Click Enable this profile.
- (b) Enter the comments.
- (c) Select Various Hotspot Login for Portal Method.
- (d) Choose Login with Facebook or Login with Google as Login Method.

If Login with Facebook is selected, the protocol of the Captive Portal URL need to be changed to HTTPS instead of HTTP because Facebook force to use HTTPS URL in their policy.

- (e) Enter the APP ID and secret.
- (f) Click Save and Next.

- Choose the Color Background, customize the information a logo color, and click Save and Next.

Hotspot Web Portal >> ProfileSetup



Choose Login Background

Color Background

Image Background

1. Browser Tab Title

2. Logo Image & Logo Background Color

3. Login Methods Background Color

1. Browser Tab Title

2. Logo Image

3. Login Methods Background Color and Opacity

4. Background Image

Login Page URL: portal.draytek.com

Browser Table Title: Draytek Hotspot

Logo Image: Default Draytek Logo Red

Logo Background Color: Vigor Red (F05B59) (format : FFFFFFFF) Preview

Login Method Background Color: Vigor Gold (F4E1D0) (format : FFFFFFFF) Preview

Save and Next Cancel

You can click the Step Icon on the top of the page to go to the step you want. The router will save your setting automatically.

Or choose the Image Background, customize the information and background image, and click Save and Next.

Hotspot Web Portal >> Profile Setup



Choose Login Background

Color Background



Image Background



Login Page URL	<input type="text" value="portal.draytek.com"/>
Browser Table Title	<input type="text" value="Draytek Hotspot"/>

Logo Image	<input type="text" value="Default Draytek Logo Red"/>

Login Method Background Color	<input type="text" value="Vigor Gold"/>
	<input type="text" value="F4E1D0"/> (format : FFFFFFFF) <input type="button" value="Preview"/>
Opacity(10 ~ 100)	<input type="text" value="80"/> %

Background Image	<input type="button" value="Choose File"/> No file chosen (max size: 1MB) <input type="button" value="Upload"/>
------------------	---

5. Customize the descriptions on the login page, then click Save and Next.

Configure Login Method and Details

Welcome!
Please log in to enjoy Wi-Fi.

By clicking the button below you agree to the
[Terms and Conditions](#)

Welcome Message _____

Terms and Conditions Description and Content _____

Facebook Login _____

Google Login _____

Welcome Message

Welcome to Draytek Video!
Please log in to enjoy Wi-Fi.

(Max 1360 characters)

Default

Terms and Conditions Description

By clicking the button below you agree to the Terms and Conditions.

(Max 170 characters)

Default

Terms and Conditions Content

(Max 1360 characters)

Facebook Login Description

Log in with Facebook

(Max 170 characters)

Default

Google Login Description

Log in with Google

(Max 170 characters)

Default

Save and Next
Cancel

6. You can set the Whitelist for the profile here to allow specific clients to access the internet or certain websites can be visited without login.

Hotspot Web Portal >> Profile Setup

1

2

3

4

5

Login Method
Background
Login Page Setup
Whitelist Setting
More Options

NAT Rules	Dest Domain	Dest IP	Dest Port	Source IP
Always allow outbound connections from hosts in		<input type="checkbox"/> NAT >> Port Redirection <input type="checkbox"/> NAT >> Open Ports <input type="checkbox"/> NAT >> DMZ		

Save and Next
Cancel

- Set up the Expired Time After Activation and Landing Page After Activation that Hotspot clients will see after they login successfully. Finally, select the interfaces to which you would like this hotspot profile apply to, then click Finish to save the setting.

Hotspot Web Portal >> Profile Setup



Web Portal Options

Expired Time After Activation: 0 days 5 hours 0 min

HTTPS Redirection Enable
 When an unauthenticated client opening a HTTPS page, redirect will work but certificate errors may be shown. Disable this function to redirect only HTTP pages. HTTPS browsing will timeout without redirection and also no certificate errors.

Captive Portal Detection Enable
 Trigger the unauthenticated client to automatically pop-up the Web Portal page when connects to Wi-Fi. This function is not available when using **Social Login** because the page may not be shown correctly due to the limitation of the OS built-in Captive Portal Detection.

Landing Page After Authentication

Fixed URL:

User Requested URL

Bulletin Message:

(Max 511 characters) Default Message

Note:
Landing Page may not be shown correctly when using OS built-in Captive Portal Detection.

Applied Interfaces

Subnet: LAN1 LAN2 LAN3 LAN4 LAN5

WLAN 2.4G: SSID1 (FAE_Victor_2925_VLC_test)
 SSID2 (DrayTek_Guest)
 SSID3
 SSID4

5G: SSID1 (DrayTek_5G)
 SSID2 (DrayTek_5G_Guest)
 SSID3
 SSID4

- Then the Hotspot setup is finished. You may click Preview to check the login page.

Hotspot Web Portal >> Profile Setup

Hotspot Web Portal Profile:

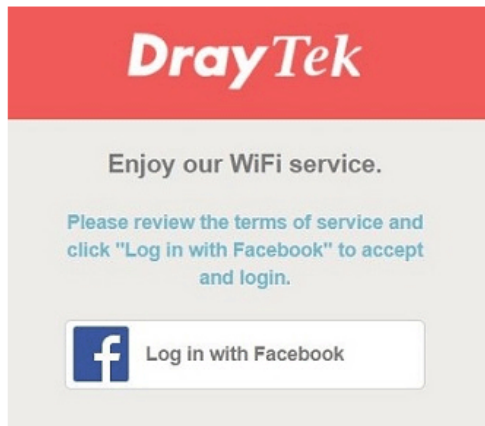
Index	Enable	Comments	Login Mode	Applied Interface	
1.	<input checked="" type="checkbox"/>	DrayTek	Social Login	LAN(1)	<input checked="" type="button" value="Preview"/>
2.	<input type="checkbox"/>		Click-through	None	<input type="button" value="Preview"/>
3.	<input type="checkbox"/>		Click-through	None	<input type="button" value="Preview"/>
4.	<input type="checkbox"/>		Click-through	None	<input type="button" value="Preview"/>

Note:

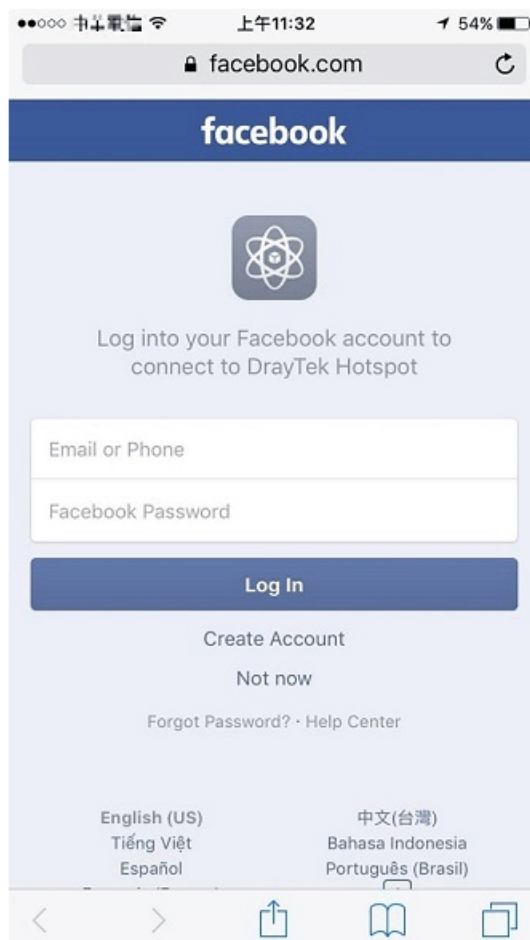
- The router must connect to the Internet before webpage redirection will work.
- If the LAN clients are using another DNS server on LAN, please make sure the DNS query for domain name "portal.draytek.com" will be resolved by the router.

Hotspot Clients Login

9. Now, when clients connect to the selected router interface, and try to access internet, they will be redirected to "portal.draytek.com".



- Due to security concerns, the browser might warn that it cannot verify server identity, the clients would need to tap "Continue" before they can proceed to portal.draytek.com.
 - The client might not be able to access "portal.draytek.com" if this domain name is resolved by a DNS server on LAN. If so, set up LAN DNS to make sure the domain name will be resolved to the router's LAN IP.
10. Tap on a login method, and it will open the social media login page. Enter the social media accounts and password to log in.



- If the credentials are correct, the client will be redirected to the landing page and be able to access the Internet afterward.



User Information

Network administrator can plug the USB disk to router, to record the basic information of the users who connect to the Wi-Fi and login with their social media accounts. The users' basic information will be listed on Hotspot Web Portal >> Users Information page.

Hotspot Web Portal >> Users Information

User Info Database Setup

Select Columns to Filter Users

Profile	Login Method
<input type="checkbox"/> Profile 1	<input type="checkbox"/> Facebook
<input type="checkbox"/> Profile 2	<input type="checkbox"/> Google
<input type="checkbox"/> Profile 3	<input type="checkbox"/> Pincode
<input type="checkbox"/> Profile 4	<input type="checkbox"/> Click

User Table

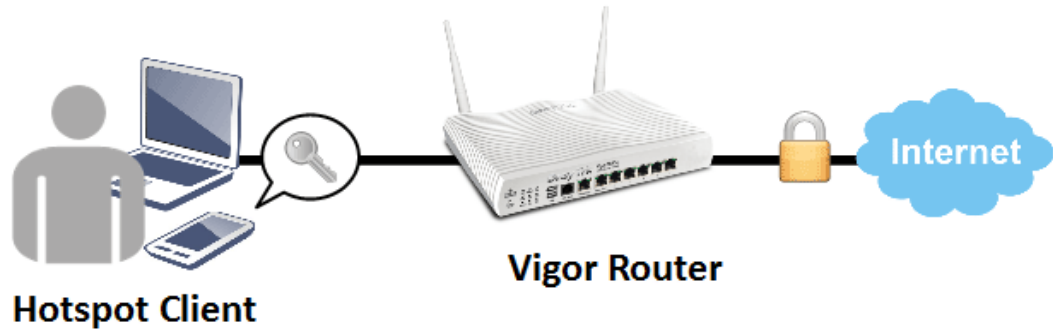
Auto Refresh (per min) | [Refresh Now](#)

2 Online Users / 2 All Users

Index	Status	Profile	User	Login Methods	IP	MAC	Email	Phone Number	Expired Time	
1	Online	1	Anderson	facebook	192.168.162.10	80:7a:bf:d1:bd:c1	yxxxxx111@gmail.com	-	2017-10-25 11:04:54	
2	Online	1	Zhuang	facebook	192.168.162.11	6c:8d:c1:11:11:11	xxxxxx@gmail.com	-	2017-10-25 11:08:57	

A-2 How to allow hotspot clients to get login PIN code via SMS?

Since 3.8.4.3 version firmware, Vigor Router can act as a hotspot gateway and provide internet access only to the authenticated clients. Network Administrator may set up the router to allow hotspot client to get the login PIN code from an SMS message. This note is going to demonstrate how to set up Vigor Router as a hotspot gateway and be able to send the PIN code to clients by SMS messages.



Vigor Router Setup

1. Make sure the router is connected to the Internet.

Online Status

Physical Connection			System Uptime: 0day 0:11:28		
IPv4		IPv6			
LAN Status	Primary DNS: 168.95.1.1		Secondary DNS: 168.95.192.1		
IP Address	TX Packets	RX Packets			
192.168.60.1	5,950	6,130			
WAN 1 Status >> Drop PPPoE					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:11:23	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
192.168.1.1	168.95.1.1	5,041	215	5,689	393

2. Create an SMS Object to send SMS messages. Go to Objects Setting >> SMS Service Object, and click on an available profile.

Objects Setting >> 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		

- Enter the Service Provider details, and click OK to apply.

Objects Setting >> SMS / Mail Service Object

Profile Index: 1

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

- Go to Hotspot Web Portal >> Profile Setup, click on an available profile.

Hotspot Web Portal >> Profile Setup



Hotspot Web Portal Profile:

Index	Enable	Comments	Login Mode	Applied Interface	
1.	<input type="checkbox"/>		Skip Login	None	Preview
2.	<input type="checkbox"/>		Skip Login	None	Preview
3.	<input type="checkbox"/>		Skip Login	None	Preview
4.	<input type="checkbox"/>		Skip Login	None	Preview

- Enable the profile, give a comment, and choose “PIN Code Login”. Then click Next.

Hotspot Web Portal >> Hotspot Web Portal Setup

Profile 1

Enable

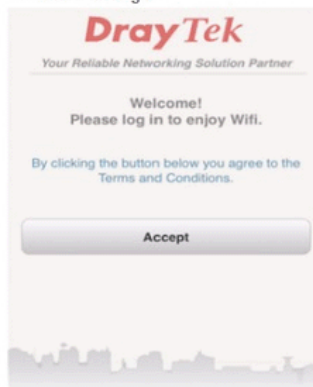
Comments: SMS authenticate

Choose How Users Receive Internet Access

Skip Login

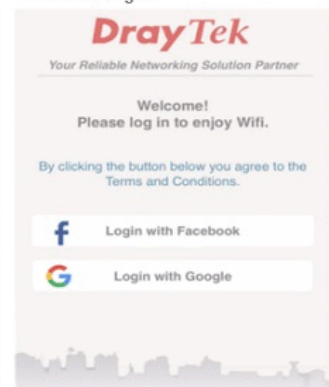
skip login phase and redirect to landing page immediately

Click-through



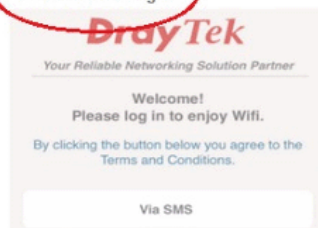
A space for you to display the terms and conditions. Users have to click Accept button (wording configurable) to get WiFi access.

Social Login

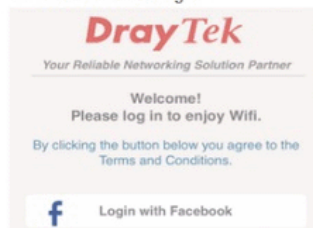


Login with Facebook or Google account.

PIN Code Login



Social or PIN Login



6. Choose a login page design, customize the details, and click Next.

Hotspot Web Portal >> Hotspot Web Portal Setup

Profile 1

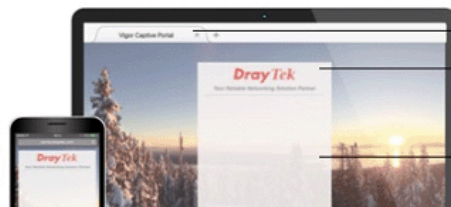
Design Login Page Appearance

Color Background



- 1. Browser Tab Title
- 2. Logo Image & Logo Background Color
- 3. Login Methods Background Color

Image Background



- 1. Browser Tab Title
- 2. Logo Image
- 3. Login Methods Background Color and Opacity

7. Edit the message on the login page, and click Next.

Receiving PIN via SMS Description	<input type="text" value="Get password via SMS"/> (Max 170 characters) Default
Receiving PIN via SMS Content	<input type="text" value="Welcome to DrayTek Hotspot!Your password is <PIN>.This PIN will be valid for 10 min."/> (Max 150 characters) Default
Receiving PIN via SMS Provider	<input type="text" value="1 - hotspot"/> Set SMS Provider in Objects Setting >> SMS / Mail Service Object
Enter PIN Description	<input type="text" value="Enter password"/> (Max 170 characters) Default
Submit Button Description	<input type="text" value="Login</font'>"/> (Max 170 characters) Default
Submit Button Color	<input type="text" value="A2A2A2"/> (format : FFFFFFF) Default

8. Edit the details for SMS settings, then click Next.

Back Button Description

(Max 170 characters) Default

PIN Code Message

Password will be sent over via SMS.

(Max 170 characters) Default

Default Country Code

+ 886 Taiwan

Enter Mobile Number Description

enter your mobile number

(Max 170 characters) Default

Send Button Description

Get password

(Max 170 characters) Default

Send Button Color

A2A2A2 (format : FFFFFFFF) Default

Send Succeeded Message

Password has been sent. Click Get password again if not receiving password in 3 minutes.

(Max 170 characters) Default

9. Edit the landing page, choose the interfaces to which the SMS login should apply, and then click Finish.

Hotspot Web Portal >> Hotspot Web Portal Setup

Profile 1

Configure Landing Page After Login

Fixed URL

User Requested URL

Bulletin Message

(Max 4095 characters) Default Message

Configure Applied Interfaces

Subnet LAN1 LAN2

WLAN 2.4G SSID1 (DrayTek)

SSID2 (DrayTek_Guest)

SSID3

SSID4

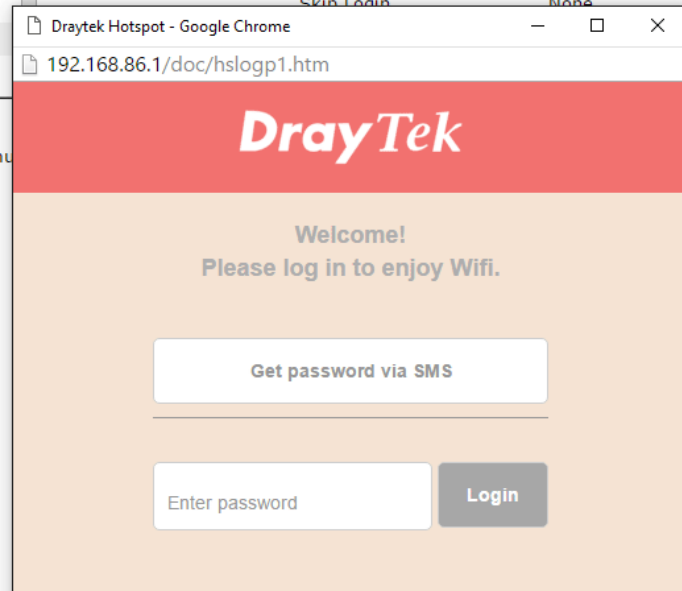
10. Now, the hotspot settings are applied to the selected interfaces. You may click Preview to check how the login page looks.



Hotspot Web Portal Profile:

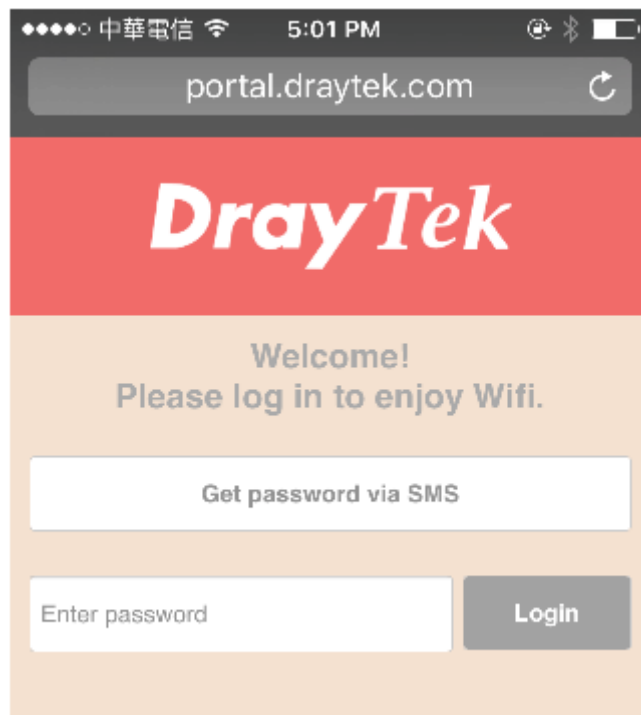
Index	Enable	Comments	Login Mode	Applied Interface	
1.	<input checked="" type="checkbox"/>	SMS authenticate	PIN Code Login	WLAN2.4G(2)	Preview
2.	<input type="checkbox"/>		Skin Login	None	Preview
3.	<input type="checkbox"/>				Preview
4.	<input type="checkbox"/>				Preview

Note:
The router mu



Hotspot Client Login

11. If the client connected to the selected interface of the router and try to open a webpage, they will be redirected to hotspot login page. If they do not have a password yet, they can click on the button to get a password.





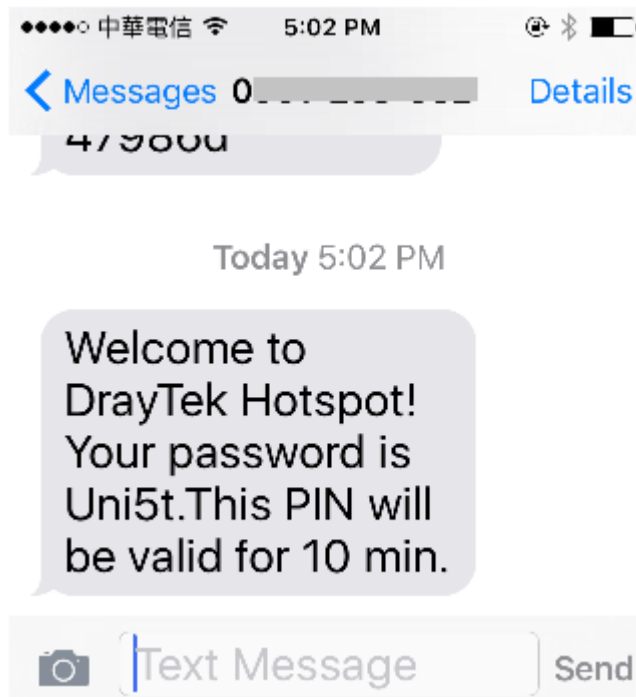
Info

- Due to security concerns, the browser might warn that it cannot verify server identity, the clients would need to tap "continue" before they can proceed to portal.draytek.com.
- The client might not be able to access "portal.draytek.com" if this domain name is resolved by a DNS server on LAN. If so, set up LAN DNS to make sure the domain name will be resolved to the router's LAN IP.

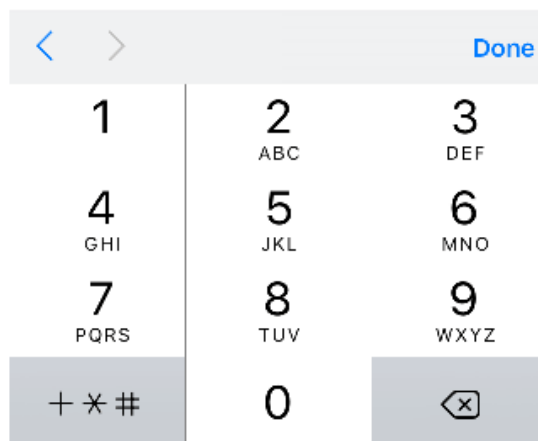
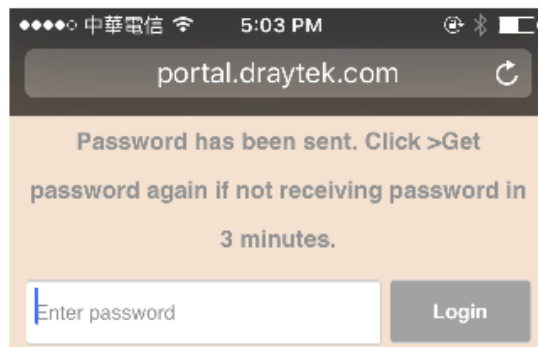
12. Enter the mobile phone number to receive the SMS message.

The screenshot shows a mobile browser interface for the DrayTek portal. At the top, the status bar displays '中華電信' (China Telecom), signal strength, Wi-Fi, and the time '5:02 PM'. The address bar shows 'portal.draytek.com'. Below the address bar is a red header with the 'DrayTek' logo. The main content area has a light beige background and contains the following elements: a back arrow icon, the text 'Password will be sent over via SMS.', a phone number input field with a dropdown menu showing '+ 886' and a text box containing '918', a grey 'Get password' button, a horizontal separator line, a text input field labeled 'Enter password', and a grey 'Login' button.

13. The number will get a message about the password.



14. Enter the password on the login page, and click Login.



15. If the password is correct, the client will be redirected to the landing page, and after that, they will be able to surf the Internet.



VII-4 Central Management (AP)

Vigor2762 can manage the access points supporting AP management via Central AP Management.

AP Map

AP Map is helpful to determine the best location for VigorAP in a room. A floor plan of a room is required to be uploaded first. By dragging and dropping available VigorAP icon from the list to the floor plan, the placement with the best wireless coverage will be clearly indicated through simulated signal strength

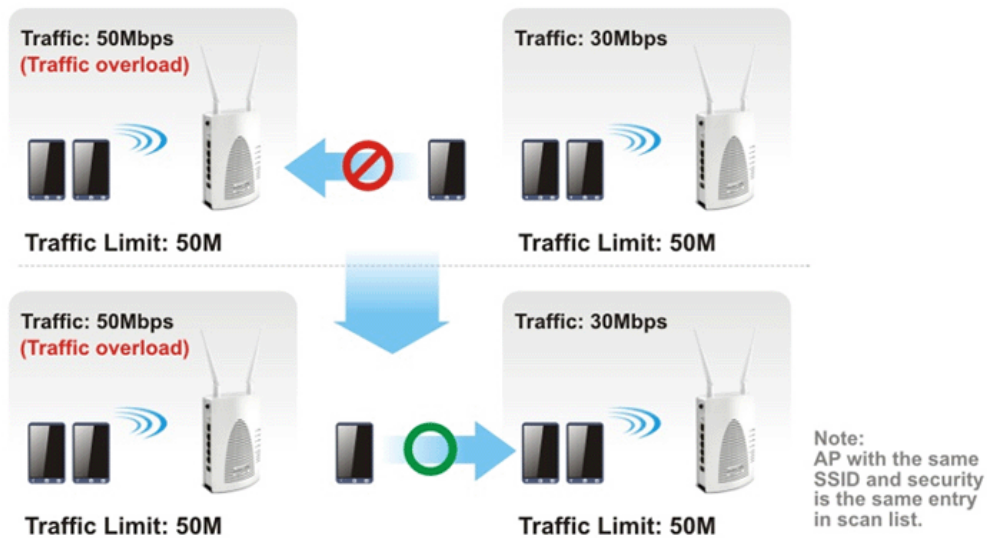
AP Maintenance

Vigor router can execute configuration backup, configuration restoration, firmware upgrade and remote reboot for the APs managed by the router. It is very convenient for the administrator to process maintenance without accessing into the web user interface of the access point.

Load Balance for AP

The parameters configured for Load Balance can help to distribute the traffic for all of the access points registered to Vigor router. Thus, the bandwidth will not be occupied by certain access points.

AP Load Balance (Traffic overload)





Web User Interface

- Central Management
- AP
- Status
- WLAN Profile
- AP Maintenance
- Traffic Graph
- Load Balance
- External Devices

VII-4-1 Status

This page displays current status (online, offline or SSID hidden, IP address, encryption, channel, version, password and etc.) of the access points managed by Vigor router.

Central Management >> AP >> Status

Index	Device Name	IP Address	SSID	Ch.	STA List	AP List	Uptime	Ver.	Password
1	VigorAP902	192.168.1.10	 DrayTek-LAN-A  DrayTek5G-LAN-A	11 36	0/64 0/64	0 0	0d 00:01	1.1.5.1	<input type="text" value="Password"/> <input type="button" value="x"/>

Note:

 : Online
  : Offline
  : Hidden SSID

Maximum support 20 APs.

When AP Devices connect via an intermediary switch, please ensure that **UDP:4944** port and the **HTTP** port of AP Devices are not blocked so that the AP status can be retrieved.

Available settings are explained as follows:

Item	Description
Index	Click the index number link for viewing the settings summary of the access point.
Device Name	The name of the AP managed by Vigor router will be displayed here.
IP Address	Display the IP address of the access point.
SSID	Display the SSID configured for the access point(s) connected to Vigor2762.
Ch.	Display the channel used by the access point.
STA List	Display the number of wireless clients (stations) connecting to the access point. In which, 0/64 means that up to 64 clients are allowed to connect to the access point. But, now no one connects to the access point. The number displayed on the left side means 2.4GHz; and the number displayed on the right side means 5GHz.
AP List	Display the number of the AP around the device.
Uptime	Display the duration of the AP powered up.
Version	Display the firmware version used by the access point.

Password	Vigor2762 can get related information of the access point by accessing into the web user interface of the access point. This button is used to modify the logging password of the connected access point.
----------	--

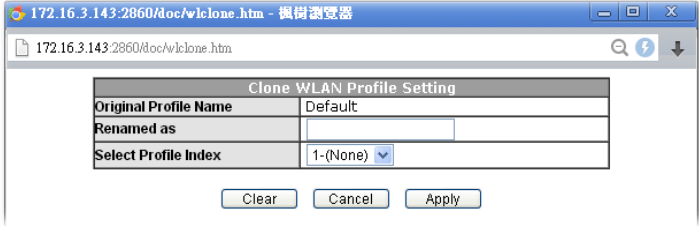
VII-4-2 WLAN Profile

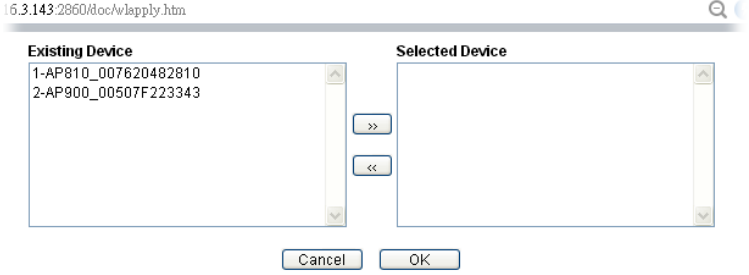
WLAN profile is used to apply to a selected access point. It is very convenient for the administrator to configure the setting for access point without opening the web user interface of the access point.

Central Management >> AP >> WLAN Profile

Set to Factory Default									
Profile	Name	Main SSID	Security	Multi-SSID	WLAN ACL	Rate Ctrl	Clone	To AP	To Local
1	Default	DrayTek-LAN-A	WPA+WPA2/PSK	Enable	None	None			
2	---	---	---	---	---	---	---	---	---
3	---	---	---	---	---	---	---	---	---
4	---	---	---	---	---	---	---	---	---
5	---	---	---	---	---	---	---	---	---

Click the number link of the selected profile to modify the content of the profile. Available settings are explained as follows:

Item	Description
Profile	There are five WLAN profiles offered to be configured. Simply click the index number link to open the modification page.
Name	Display the name of the profile. The default profile cannot be renamed.
Main SSID	Display the SSID configured by such wireless profile.
Security	Display the security mode selected by such wireless profile.
Multi-SSID	Enable means multiple SSIDs (more than one) are active. Disable means only SSID1 is active.
WLAN ACL	Display the name of the access control list.
Rate Ctrl	Display the upload and/or download transmission rate.
Clone	<p>It can copy settings from an existing WLAN profile to another WLAN profile.</p> <p>First, you have to check the box of the existing profile as the original profile. Second, click Clone. The following dialog will appear.</p>  <p>Third, choose the profile index to accept the settings from the original profile. Forth, type a new name in the field of Renamed as. Last, click Apply to save the settings on this dialog.</p> <p>The new profile has been created with the settings coming from the original profile.</p>
To AP	Click it to apply the selected wireless profile to the specified Access Point.

	 <p>Simply choose the device you want from Existing Device field. Click >> to move the device to Selected Device field. Then, click OK.</p> <p>The selected WLAN profile will be applied to the selected access point immediately. Later the access point will reboot.</p>
To Local	<p>WLAN Profile configured in this page is specified for VigorAP connected to Vigor router.</p> <p>If required, these settings also can be applied to Vigor router. Select and check one of wireless profiles and click this button to apply the settings onto the WI-Fi wireless settings configured for such Vigor router.</p>

How to edit the wireless LAN profile?

1. Select the WLAN profile (index number 1 to 5) you want to edit.
2. Click the index number link to display the following page.

Central Management >> AP >> WLAN Profile

WLAN Profile Edit

Device Settings	
Profile Name	Default <input type="checkbox"/> Auto Provision
Administrator	admin
Password
2nd Subnet	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Management VLAN	<input type="checkbox"/> Enable Management VLAN: LAN-A VLAN ID <input type="text" value="0"/> (0 ~ 4095) LAN-B VLAN ID <input type="text" value="0"/> (0 ~ 4095)

WLAN General Setting

	2.4GHz	5GHz	5GHz-2
Wireless LAN	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Limit Client	<input type="checkbox"/> Enable <input type="text" value="64"/> (3 ~ 128, default: 64)		
Operation Mode	AP ▼		
2.4G Mode	Mixed(11b+11g+11n) ▼		
2.4G Channel	2462MHz (Channel 11) ▼		
Airtime Fairness	<input type="checkbox"/> Enable Airtime Fairness: Triggering Client Number <input type="text" value="2"/> (2 ~ 128, default: 2)		
Band Steering	<input type="checkbox"/> Enable Band Steering: Check Time for WLAN Client 5G Cap. <input type="text" value="15"/> seconds (1 ~ 60, default: 15)		
Roaming	<input type="checkbox"/> Minimum Basic Rate <input type="text" value="1"/> Mbps <input checked="" type="radio"/> Disable RSSI Requirement <input type="radio"/> Strictly Minimum RSSI - <input type="text" value="73"/> dbm (<input type="text" value="42"/> %) (default: -73) <input type="radio"/> Minimum RSSI - <input type="text" value="66"/> dbm (<input type="text" value="60"/> %) (default: -66) with Adjacent AP RSSI over <input type="text" value="5"/> dB (default: 5) <input type="checkbox"/> Enable Fast Roaming(WPA2/802.1x): PMK Cache Period <input type="text" value="10"/> minutes (10 ~ 600, default: 10)		
WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Tx Power	100% ▼		
Channel Width	Auto 20/40 MHz ▼		



Info

The function of Auto Provision is available for the default WLAN profile.

- After finished the general settings configuration, click Next to open the following page for 2.4G wireless security settings.

Central Management >> AP >> WLAN Profile

SSID1	SSID2	SSID3	SSID4
2.4G SSID			
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
SSID	DrayTek-LAN-A	LAN-A	<input type="checkbox"/> Hide SSID
VLAN	0 (0:untag)		
Isolate	<input type="checkbox"/> From Member		
Security Settings			
Encryption	WPA+WPA2/PSK		
	Set up RADIUS Server if 802.1X is enabled.		
	WPA		
	WPA Algorithms	<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES	
Pass Phrase	*****		
Key Renewal Interval	3600	Seconds	
WEP	Setup WEP Key if WEP is enabled.		
	802.1X WEP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Access Control			
Mode	None		
List			
	Client's MAC Address : [] : [] : [] : [] : []		
	<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/>		
Bandwidth Limit			
Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Auto Adjustment	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Upload	0 Kbps	Download	0 Kbps
<input type="button" value="Back"/> <input type="button" value="Cancel"/> <input type="button" value="Next"/>			
Backup ACL Cfg : <input type="button" value="Backup"/>		Upload From File: <input type="button" value="選擇檔案"/> 未選擇檔案 <input type="button" value="Restore"/>	

- After finished the above web page configuration, click Next to open the following page for 5G wireless security settings.

Central Management >> AP >> WLAN Profile

5G SSID1	5G SSID2	5G SSID3	5G SSID4
5GHz SSID			
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
SSID	DrayTek-5G	LAN-A ▼	<input type="checkbox"/> Hide SSID
VLAN	0 (0:untag)		
Isolate	<input type="checkbox"/> From Member		
Security Settings			
Encryption	Disable ▼		
	Set up RADIUS Server if 802.1X is enabled.		
	WPA		
	WPA Algorithms	<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES	
Pass Phrase	Max: 64 characters		
Key Renewal Interval	3600	Seconds	
WEP			
Setup WEP Key if WEP is enabled.			
802.1X WEP <input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Access Control			
Mode	None ▼		
List			
	Client's MAC Address : [] : [] : [] : [] : [] : []		
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/>			
Bandwidth Limit			
Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		Auto Adjustment <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Upload	0 Kbps	Download	0 Kbps
Station Control			
Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Connection Time	1 hour ▼	Reconnection Time	1 hour ▼

Note:

- 5GHz SSID Configuration only work with VigorAP800 v1.1.1 and newer APM Client.
- SSID can contain only A-Z a-z 0-9 _ - . @ # \$ % *

- When you finished the above web page configuration, click Finish to exit and return to the first page. The modified WLAN profile will be shown on the web page.

VII-4-3 AP Maintenance

Vigor router can execute configuration backup, configuration restoration, firmware upgrade and remote reboot for the APs managed by the router. It is very convenient for the administrator to process maintenance without accessing into the web user interface of the access point.



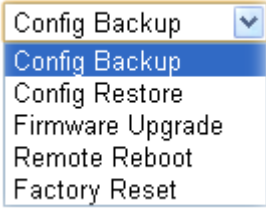
Info

Config Backup can be performed to one AP at one time. Others functions (e.g., Config Restore, Firmware Upgrade, Remote Reboot can be performed to more than one AP at one time by using Vigor2762.

Central Management >> AP >> AP Maintenance

AP Maintenance

Available settings are explained as follows:

Item	Description
Action	<p>There are four actions provided by Vigor router to manage the access points.</p>  <p>Vigor router can backup the configuration of the selected AP, restore the configuration for the selected AP, perform the firmware upgrade of the selected AP, reboot the selected AP remotely and perform the factory reset for the selected AP.</p>
File/Path	Specify the file and the path which will be used to perform Config Restore or Firmware Upgrade.

Select Device	Display all the available access points managed by Vigor router. Simply click << or >> to move the device(s) between Select Device and Selected Device areas.
Selected Device	Display the access points that will be applied by such function after clicking OK.

After finishing all the settings here, please click OK to perform the action.

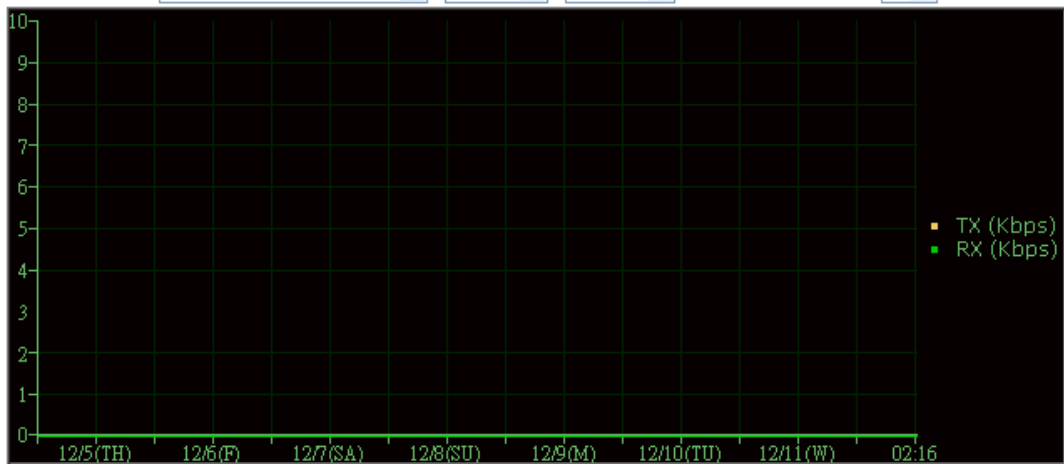
VII-4-4 Traffic Graph

Click Traffic Graph to open the web page. Choose one of the managed Access Points, LAN-A or LAN-B, daily or weekly for viewing data transmission chart. Click Refresh to renew the graph at any time.

Central AP Management >> Traffic Graph

Enable

Show Chart: Refresh Min(s): | **Refresh** |



Note : Enabling/Disabling AP Traffic Graph will also Enable/Disable the External Devices Function.

The horizontal axis represents time; the vertical axis represents the transmission rate (in kbps).



Info

Enabling/Disabling such function will also enable/disable the External Devices function.

VII-4-5 Load Balance

The parameters configured for Load Balance can help to distribute the traffic for all of the access points registered to Vigor router. Thus, the bandwidth will not be occupied by certain access points.

Central Management >> AP >> Load Balance

AP Load Balance By Station Number or Traffic

Station Number Threshold

Wireless LAN (2.4GHz) (3-128)

Wireless LAN (5GHz) (3-128)

Wireless LAN (5GHz-2) (3-128)

Traffic Threshold

Upload Limit bps (Default unit: K)

Download Limit bps (Default unit: K)

Action When Threshold Exceeded

Stop accepting new connections

Dissociate existing station by longest idle time

Dissociate existing station by worst signal strength if it is less than dBm (%)

Choose to Apply

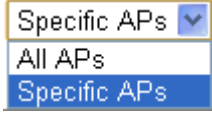
All APs

Note:

The maximum station number of Wireless LAN (2.4GHz) will be applied to both Wireless LAN (2.4GHz) and Wireless LAN (5GHz) if the firmware version of AP900 is less than or equal to 1.1.4.1.

Available settings are explained as follows:

Item	Description
AP Load Balance	<p>It is used to determine the operation mode when the system detects overload between access points.</p> <p>Disable - Disable the function of AP load balance.</p> <p>By Station Number -The operation of load balance will be executed based on the station number configured in this page. It is used to limit the allowed number for the station connecting to the access point. The purpose is to prevent lots of stations connecting to access point at the same time and causing traffic unbalanced. Please define the required station number for WLAN (2.4GHz) and WLAN (5GHz) separately.</p> <p>By Traffic - The operation of load balance will executed according to the traffic configuration in this page.</p> <p>By Station Number or Traffic - The operation of load balance will be executed based on the station number or the traffic configuration.</p>
Station Number Threshold	Set the number of stations as a threshold to activate AP load balance.

Traffic Threshold	<p>Upload Limit -Use the drop down list to specify the traffic limit for uploading.</p> <p>Download Limit - Use the drop down list to specify the traffic limit for downloading.</p>
Action When Threshold Exceeded	<p>Stop accepting new connections - When the number of stations or the traffic reaches the threshold defined in this web page, Vigor router will stop any new connection asked by other access point.</p> <p>Dissociate existing station by longest idel time - When the access point is overload (e.g., reaching the limit of station number or limit of network traffic), it will terminate the network connection of the client's station which is idle for a longest time.</p> <p>Dissociate existing station by worst signal strength if it is less than - When the access point is overload (e.g., reaching the limit of station number or limit of network traffic), it will terminate the network connection of the client's station with the weakest signal.</p>
Choose to Apply	<p>The settings configured for Load Balance can be applied to all of AP devices or selected AP devices.</p> 

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

VII-5 Central Management (External Devices)

Vigor router can be used to connect with many types of external devices. In order to control or manage the external devices conveniently, open External Devices to make detailed configuration.

Central Management >> External Device

- External Device Syslog
- External Device Auto Discovery

External Devices Connected

| [Refresh](#) |

Below shows available devices that connected externally:

For security reason:

If you have changed the administrator password on External Device, please click the **Account** button to retype new username and password. Otherwise, the router will be unable to monitor the External Device device properly. Click the **Clear** button to Clear the off-line information and account information.

OK

Available settings are explained as follows:

Item	Description
External Device Syslog	Check this box to display information of the detected device on Syslog.
External Device Auto Discovery	Check this box to detect the external device automatically and display on this page.

From this web page, check the box of External Device Auto Discovery. Later, all the available devices will be displayed in this page with icons and corresponding information. You can change the device name if required or remove the information for off-line device whenever you want.

- External Device Auto Discovery

External Devices Connected

Below shows available devices that connected externally:

On Line VigorAP900, VigorAP900, Connection Uptime:18:15:27	
IP Address:10.28.60.12	Account Clear
On Line P2261, Connection Uptime:18:15:17	
IP Address:192.168.1.226	Account Clear

For security reason:

If you have changed the administrator password on External Device, please click the **Account** button to retype new username and password. Otherwise, the router will be unable to monitor the External Device device properly. Click the **Clear** button to Clear the off-line information and account information.

OK

When you finished the configuration, click OK to save it.



Info

Only DrayTek products can be detected by this function.

Part VIII Others



Objects Settings

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



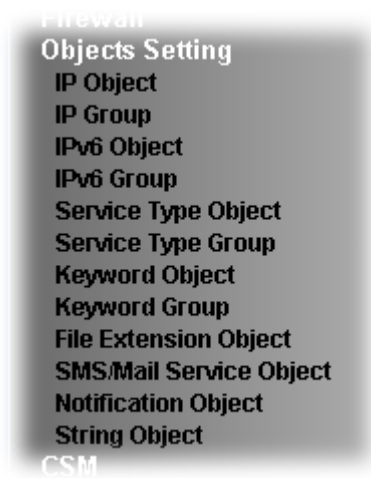
USB

USB device connected on Vigor router can be regarded as a server or WAN interface. By way of Vigor router, clients on LAN can access, write and read data stored in USB storage disk with different applications.

VIII-1 Objects Settings

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

Web User Interface



VIII-1-1 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 for applying 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.

[Create from ARP Table](#)
[Create from Routing Table](#)

| [Set to Factory Default](#) |

IP Object Profiles:

View:

Index	Name	Address	Index	Name	Address
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](#) >>

<p>Export IP Object</p> <p><input checked="" type="radio"/> Backup the current IP Objects with a CSV file</p> <p><input type="radio"/> Download the default CSV template to edit</p> <p><input type="button" value="Download"/></p>	<p>Restore IP Object</p> <p><input type="button" value="選擇檔案"/> 未選擇檔案</p> <p><input type="button" value="Restore"/></p>
--	--

Note:
 For better compatibility, it's suggested to edit IP Objects with the provided default CSV template.

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.
Address	Display the IP address configured for the object profile.
Export IP Object	<p>Usually, the IP objects can be created one by one through the web page of Objects>>IP Object. However, to a user who wants to save more time in bulk creating IP objects, a quick method is offered by Vigor router to modify the IP objects with a single file, a CSV file.</p> <p>All of the IP objects (or the template) can be exported as a file by clicking Download. Then the user can open the CSV file through Microsoft Excel and modify all the IP objects at the same time.</p> <p>Backup the current IP Objects with a CSV file - Click it to backup current IP objects as a CSV file. Such file can be restored for future use.</p> <p>Download the default CSV template to edit - After clicking it, press Download to store the default CSM template (a table</p>

	without any input data) to your hard disk. Download - Download the CSV file from Vigor router and store in your hard disk.
Restore IP Object	Select - Click it to specify a predefined CSV file. Restore - Import the selected CSV file onto Vigor router.

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.
2. The configuration page will be shown as follows:

Objects Setting >> IP Object

Profile Index : 1

Name:	RD Department
Interface:	Any
Address Type:	Range Address
Mac Address:	00 .00 .00 .00 .00 .00
Start IP Address:	192.168.1.59
End IP Address:	192.168.1.65
Subnet Mask:	0.0.0.0
Invert Selection:	<input type="checkbox"/>

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Interface	Choose a proper interface. 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/DMZ/RT/VPN interface will be opened for you to choose in Edit Filter Rule page.
Address Type	Determine the address type for the IP address. Select Single Address if this object contains one IP address only. Select Range Address if this object contains several IPs within a range. Select Subnet Address if this object contains one subnet for IP address. Select Any Address if this object contains any IP address. Select Mac Address if this object contains Mac address.

Range Address ▾

Any Address

Single Address

Range Address

Subnet Address

Mac Address

MAC Address	Enter the MAC address of the network card which will be controlled.
Start IP Address	Enter the start IP address for Single Address type.
End IP Address	Enter the end IP address if the Range Address type is selected.
Subnet Mask	Enter 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.

4. After finishing all the settings here, please click OK to save the configuration. Below is an example of IP objects settings.

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>
6.		22.

VIII-1-2 IP Group

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

Objects Setting >> IP Group

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

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

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.
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

(Empty)

Available settings are explained as follows:

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

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

VIII-1-3 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.
2. The configuration page will be shown as follows:

Objects Setting >> IPv6 Object

Profile Index : 1

Name:	<input type="text"/>
Address Type:	Subnet Address <input type="button" value="v"/>
Mac Address:	<input type="text" value="00:00:00:00:00:00"/>
Start IP Address:	<input type="text" value="FF02::1"/> <input type="button" value="Select"/>
End IP Address:	<input type="text"/> <input type="button" value="Select"/>
Prefix Length:	<input type="text" value="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.
Address Type	<p>Determine the address type for the IPv6 address.</p> <p>Select Single Address if this object contains one IPv6 address only.</p> <p>Select Range Address if this object contains several IPv6s within a range.</p> <p>Select Subnet Address if this object contains one subnet for IPv6 address.</p> <p>Select Any Address if this object contains any IPv6 address.</p> <p>Select Mac Address if this object contains Mac address.</p> <div style="border: 1px solid black; padding: 2px; margin-top: 5px;"> <input type="button" value="Range Address"/> <input type="button" value="v"/> Any Address Single Address Range Address Subnet Address Mac Address </div>
Mac Address	Enter the MAC address of the network card which will be controlled.
Start IP Address	Type or click Select to choose the start IP address for Single Address type.
End IP Address	Type or click Select to choose the end IP address if the Range Address type is selected.
Prefix Length	Enter the number (e.g., 64) for the prefix length of IPv6 address.
Invert Selection	If it is checked, all the IPv6 addresses except the ones listed above will be applied later while it is chosen.

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

VIII-1-4 IPv6 Group

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

Objects Setting >> IPv6 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.
2. The configuration page will be shown as follows:

Objects Setting >> IPv6 Group

Profile Index : 1

Name:

Available IPv6 Objects

Selected IPv6 Objects

Available settings are explained as follows:

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

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

VIII-1-5 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:

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

2. The configuration page will be shown as follows:

Objects Setting >> Service Type Object Setup

Profile Index : 1

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

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Protocol	Specify the protocol(s) which this profile will apply to. <div style="border: 1px solid black; padding: 2px;"> Any ▾ Any ICMP IGMP TCP UDP TCP/UDP ICMPv6 Other </div>
Source/Destination Port	Source Port and the Destination Port columns are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number. (=) - when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this profile. (!=) - when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type. (>) - the port number greater than this value is available. (<) - the port number less than this value is available for this profile.

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

Objects Setting >> Service Type Object

Service Type Object Profiles:

Index	Name	Index
<u>1.</u>	www	<u>17.</u>
<u>2.</u>	SIP	<u>18.</u>
<u>3.</u>		<u>19.</u>
4.		20

VIII-1-6 Service Type Group

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

Objects Setting >> Service Type Group

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

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

Available settings are explained as follows:

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

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

1. Click the number (e.g., #1) under Group column for configuration in details.
2. The configuration page will be shown as follows:

Objects Setting >> Service Type Group Setup

Profile Index : 1

Name:

Available Service Type Objects		Selected Service Type Objects
1-www	<input type="button" value=">>"/> <input type="button" value="<<"/>	
2-SIP		

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
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, please click OK to save the configuration.

VIII-1-7 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.
2. The configuration page will be shown as follows:

Objects Setting >> Keyword Object Setup

Profile Index : 1

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

Limit of Contents: Max 3 Words and 63 Characters.
Each word should be separated by a single space.

You can replace a character with %HEX.
Example:
Contents: backdoo%72 virus keep%20out

Result:
1. backdoor
2. virus
3. keep out

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile, e.g., game. Maximum 15 characters are allowed.
Contents	Enter 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, please click OK to save the configuration.

VIII-1-8 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.
2. The configuration page will be shown as follows:


Objects Setting >> Keyword Group Setup

Profile Index : 1

Name:

Available Keyword Objects	Selected Keyword Objects(Max 16 Objects)
1-Key-1 2-Key-2	

Available settings are explained as follows:

Item	Description
Name	Type a name for this group. Maximum 15 characters are allowed.
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  button to add the selected Keyword objects in this box.

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

VIII-1-9 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
<u>1.</u>		<u>5.</u>	
<u>2.</u>		<u>6.</u>	
<u>3.</u>		<u>7.</u>	
<u>4.</u>		<u>8.</u>	

Available settings are explained as follows:

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

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

1. Click the number (e.g., #1) under Profile column for configuration in details.
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"/> .vrm
Compression <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for this profile. The maximum length of the name you can set is 7 characters.

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

VIII-1-10 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.
2. The configuration page will be shown as follows:

Objects Setting >> SMS / Mail Service Object

Profile Index: 1

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

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.

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such SMS profile. The maximum length of the name you can set is 31 characters.
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. The maximum length of the name you can set is 31 characters.
Password	Type a password that the sender can use to register to selected SMS provider. The maximum length of the password you can set is 31 characters.
Quota	Enter 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	
<u>1.</u>	Line_down	kotsms.com.tw (TW)	
<u>2.</u>		kotsms.com.tw (TW)	
<u>3.</u>		kotsms.com.tw (TW)	
<u>4.</u>		kotsms.com.tw (TW)	

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	<input type="text" value="Custom 1"/>
Service Provider	<input type="text"/>
<div style="border: 1px solid black; height: 50px; width: 100%;"></div>	
<p>Please contact with your SMS provide to get the exact URL String eg: bulksms.vsms.net:5567/eapi/submission/send_sms/2/2.0? username=###txtUser### &password=###txtPwd###&msisdn=###txtDest###&message=###txtMsg###</p>	
Username	<input type="text"/>
Password	<input type="text"/>
Quota	<input type="text" value="10"/>
Sending Interval	<input type="text" value="3"/> (seconds)

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.

Available settings are explained as follows:

Item	Description
Profile Name	Display the name of this profile. It cannot be modified.
Service Provider	Enter the website of the service provider. Enter 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. The maximum length of the name you can set is 31 characters.
Password	Type a password that the sender can use to register to selected SMS provider. The maximum length of the password you can set is 31 characters.
Quota	Enter the total number of the messages that the router will send out.
Sending Interval	Enter 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	
<u>1.</u>		
<u>2.</u>		
<u>3.</u>		
<u>4.</u>		
<u>5.</u>		
<u>6.</u>		
<u>7.</u>		
<u>8.</u>		
<u>9.</u>		
<u>10.</u>		

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.
Index	Display the profile number that you can configure.
Profile	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.
2. The configuration page will be shown as follows:

Object Settings >> SMS / Mail Service Object

Profile Index: 1

Profile Name	<input type="text" value="Mail_Notify"/>
SMTP Server	<input type="text" value="192.168.1.98"/>
SMTP Port	<input type="text" value="25"/>
Sender Address	<input type="text" value="carrie_ni@draytek.com"/>
<input type="checkbox"/> Use SSL	
<input checked="" type="checkbox"/> Authentication	
Username	<input type="text" value="John"/>
Password	<input type="password" value="••••"/>
Sending Interval	<input type="text" value="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.

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such mail service profile. The maximum length of the name you can set is 31 characters.
SMTP Server	Enter the IP address of the mail server.
SMTP Port	Enter the port number for SMTP server.
Sender Address	Enter 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. The maximum length of the name you can set is 31 characters. Password - Type a password for authentication. The maximum length of the password you can set is 31 characters.
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.

VIII-1-11 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

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

[Set to Factory Default](#)

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.
2. The configuration page will be shown as follows:

Objects Setting >> Notification Object

Profile Index: 1

Profile Name	<input type="text" value="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
Temperature Alert	<input type="checkbox"/> Out of Range	
WAN Budget	<input type="checkbox"/> Limit Reached	

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such notification profile. The maximum length of the name you can set is 15 characters.
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.

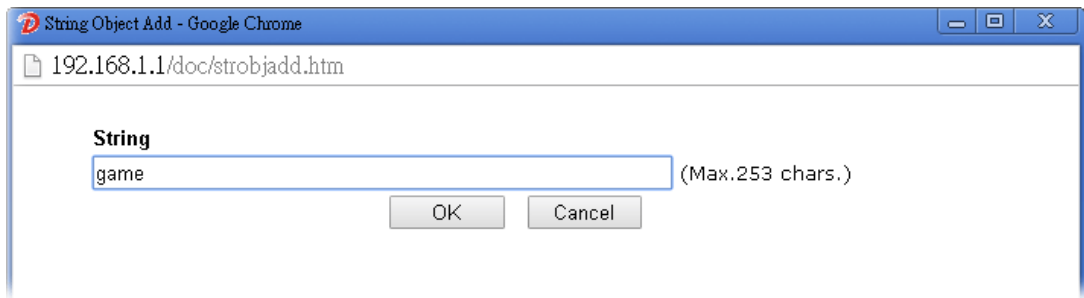
VIII-1-12 String Object

This page allows you to set several profiles of string object.

Objects Setting >> String Object

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

Click Add to open the following dialog.



Enter the string you want and click OK. A new profile (e.g., index #1) with the defined string will be shown on the web page.

Objects Setting >> String Object

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

Index	String	Clear
1	game	<input type="checkbox"/>

In general, there is no limit in the number of string profiles created. Each page can display 10, 20, 30, 40 or 50 profiles.

Application Notes

A-1 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

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, Enter the username and password and set the quota that the router can send the message out.

Objects Setting >> 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)

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.

- After finished the settings, click OK to return to previous page. Now you have finished the configuration of the SMS Provider profile setting.

Objects Setting >> 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		

- Open Object Settings>>Notification Object to configure the event conditions of the notification.

Objects Setting >> Notification Object

			Set to Factory Default
Index	Profile Name	Settings	
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			

- Choose any index number (e.g., Index 1 in this case) to configure conditions for sending the SMS. In the following page, Enter the name of the profile and check the Disconnected and Reconnected boxes for WAN to work in concert with the topic of this paper.

Objects Setting >> 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
Temperature Alert	<input type="checkbox"/> Out of Range	
WAN Budget	<input type="checkbox"/> Limit Reached	

- After finished the settings, click OK to return to previous page. You have finished the configuration of the notification object profile setting.

Objects Setting >> 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, Enter the phone number in the field of Recipient (the one who will receive the SMS).

Applications >> SMS / Mail Alert Service

SMS Alert		Mail Alert		Set to Factory Default	
Index	SMS Provider	Recipient Number	Notify Profile	Schedule(1-15)	
1 <input checked="" type="checkbox"/>	1 - Local number ▼	0910123456	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 ▼		

Note:

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

- 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.

Remark: How the customize the SMS Provider

Choose one of the Index numbers (9 or 10) allowing you to customize the SMS Provider. In the web page, Enter the URL string of the SMS provider and Enter the username and password. After clicking OK, the new added SMS provider will be added and will be available for you to specify for sending SMS out.

Objects Setting >> SMS / Mail Service Object

Profile Index: 9

Profile Name	<input type="text" value="Custom 1"/>
Service Provider	<input type="text" value="clickatell"/>
<div style="border: 1px solid gray; height: 50px; width: 100%;"></div>	
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###&msisdh=###txtDest###&message=###txtMsg###	
Username	<input type="text" value="ilan123"/>
Password	<input type="password" value="*****"/>
Quota	<input type="text" value="10"/>
Sending Interval	<input type="text" value="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.

VIII-2 USB Application

USB device connected on Vigor router can be regarded as a server or WAN interface. 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 Enter 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 SMB service through Vigor router.



Info

USB ports on Vigor router are allowed to connect to USB modem. Models of the modems supported by Vigor router can be seen from USB Application>>Modem Support List. For network connection via USB modem, refer to WAN>>Internet Access and WAN>>General Setup for detailed information.

Web User Interface

- SSL VPN
- USB Application**
- USB General Settings
- USB User Management
- File Explorer
- USB Device Status
- Temperature Sensor
- Modem Support List
- SMB Client Support List
- System Maintenance

VIII-2-1 USB General Settings

This page will determine the number of concurrent FTP connection, default charset for FTP server and enable SMB 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).

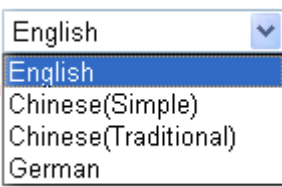
USB Application >> USB General Settings

USB General Settings

General Settings	
Simultaneous FTP Connections	<input type="text" value="5"/> (Maximum 6)
Default Charset	<input type="text" value="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	<input type="text" value="WORKGROUP"/>
Host Name	<input type="text" value="Vigor"/>
Printer Server	
<input checked="" type="radio"/> Enable <input type="radio"/> Disable	

Available settings are explained as follows:

Item	Description
General Settings	<p>Simultaneous FTP Connections - This field is used to specify the quantity of the FTP sessions. The router allows up to 6 FTP sessions connecting to USB storage disk at one time.</p> <p>Default Charset - At present, Vigor router supports four types of character sets. Default Charset is for English based file name.</p>

	
SMB File Sharing Service	Click Enable to invoke SMB file sharing service 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 - Enter 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 finishing all the settings here, please click OK to save the configuration.

VIII-2-2 USB User Management

This page allows you to set profiles for FTP/SMB users. Any user who wants to access into the USB storage disk must Enter 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
<u>1.</u>			<u>9.</u>		
<u>2.</u>			<u>10.</u>		
<u>3.</u>			<u>11.</u>		
<u>4.</u>			<u>12.</u>		
<u>5.</u>			<u>13.</u>		
<u>6.</u>			<u>14.</u>		
<u>7.</u>			<u>15.</u>		
<u>8.</u>			<u>16.</u>		

Click index number to access into configuration page.


Profile Index: 1

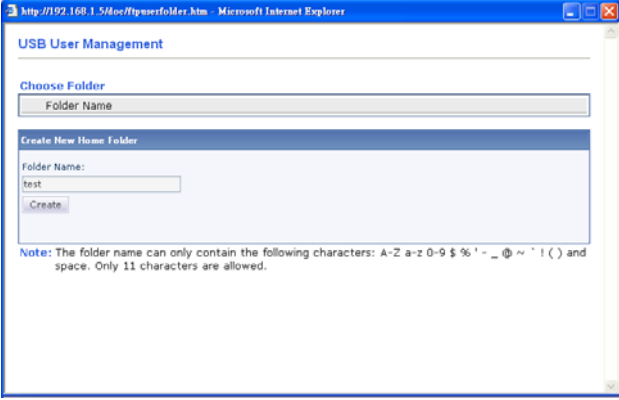
<input type="checkbox"/> Enable	
Username	<input type="text" value="Max: 11 characters"/>
Password	<input type="text" value="Max: 11 characters"/>
Confirm Password	<input type="text"/>
Home Folder	<input type="text"/> 
Access Rule	
File	<input type="checkbox"/> Read <input type="checkbox"/> Write <input type="checkbox"/> Delete
Directory	<input type="checkbox"/> List <input type="checkbox"/> Create <input type="checkbox"/> Remove

Note:

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

Available settings are explained as follows:

Item	Description
Enable	Activate this profile (account) for FTP service or SMB file sharing service. Later, the user can use the username specified in this page to login into FTP server.
Username	Enter the username for FTP/SMB 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 Enter the username specified here for accessing into USB storage disk. The length of the name is limited to 11 characters. Note: "Admin" could not be typed here as username, for the word is specified for accessing into web pages of Vigor router only. Also, it is reserved for FTP firmware upgrade usage. Note: FTP Passive mode is not supported by Vigor Router. Please disable the mode on the FTP client.
Password	Enter the password for FTP/SMB users for accessing FTP server. Later, you can open FTP client software and Enter the password specified here for accessing into USB storage disk. The length of the password is limited to 11 characters.
Confirm Password	Enter the password again to make confirmation.
Home Folder	It determines the folder for the client to access into. The user can enter a directory name in this field. Then, after clicking OK, the router will create the specific/new folder in the USB storage disk. In addition, if the user types "/" here, he/she can access into all of the disk folders and files in USB storage disk. Note: When write protect status for the USB storage disk is ON, you cannot type any new folder name in this field. Only "/" can be used in such case. You can click  to open the following dialog to add any new folder which can be specified as the Home Folder.

	
<p>Access Rule</p>	<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.

VIII-2-3 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

USB Disk Connection Status: **No Disk Connected**

| [Refresh](#) |

Note:

1. File Explorer cannot be used, if USB disk is disconnected.
2. The folder can not be deleted when it is not empty.

After inserting a USB, the following page will be shown on the screen.

USB Application >> File Explorer

USB Disk Connection Status: **Disk Connected**

| [Refresh](#) |

File Explorer

The screenshot shows the File Explorer interface with the following elements:

- Navigation icons: Refresh (circular arrows), Back (upward arrow), and Create (folder icon).
- Current Path: /
- Table of files:

Name	Size	Delete	Rename
??2014_2016		X	[Icon]
System Volume Information		X	[Icon]
C?2014_2016		X	[Icon]
???2016		X	[Icon]
C?2016		X	[Icon]
USB DISK	1 KB	X	[Icon]
- Upload File section:
 - Upload File button (upward arrow icon)
 - Select a file:
 - Buttons: 選擇檔案 (Select File), 未選擇檔案 (No File Selected)
 - Upload button

Note:

1. File Explorer cannot be used, if USB disk is disconnected.
2. 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.

VIII-2-4 USB Device Status

This page is to monitor the status for USB device connecting to Vigor router. In addition, the status of the USB modem or USB printer or USB sensor 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 device later.

USB Application >> USB Device Status

Disk	Modem	Printer	Sensor	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	

Available settings are explained as follows:

Item	Description
Connection Status	If there is no USB device 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 connects to FTP server.
IP Address	It displays the IP address of the user’s host which connects to the FTP server.
Username	It displays the username that user uses to login to the FTP server.

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

USB Application >> USB Device Status

Disk	Modem	Printer	Sensor	Refresh
USB Mass Storage Device Status				
Connection Status: Disk Connected				Disconnect USB Disk
Write Protect Status: No				
Disk Capacity: 7666 MB				
Free Capacity: 6864 MB Refresh				
USB Disk Users Connected				
Index	Service	IP Address(Port)	Username	

Note:

1. Only support FAT16 and FAT32 format, FAT32 is recommended.
2. Only support to mount single partition, maximum capacity is 500GB. If there are more than one partition, only one of them will be mounted.
3. Single file size can be up to 4GB, which is the limitation of FAT32 format.
4. 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.

VIII-2-5 Temperature Sensor

A USB Thermometer is now available. It complements your installed DrayTek router installations which will help you monitor the server or data communications room environment and notify you if the server room or data communications room is overheating.



During summer in particular, it is important to ensure that your server or data communications equipment are not overheating due to cooling system failures.

The inclusion of a USB thermometer in compatible Vigor routers will continuously monitor the temperature of its environment. When a pre-determined threshold is reached you will be alerted by either an email or SMS so you can undertake appropriate action.

Temperature Sensor Settings

USB Application >> Temperature Sensor Setting

Temperature Chart	Temperature Sensor Settings
Display Settings	
Temperature Calibration	<input type="text" value="0.00"/>
Temperature Unit	<input checked="" type="radio"/> Celsius <input type="radio"/> Fahrenheit
Alarm Settings	
<input type="checkbox"/> Enable Syslog Alarm	
Upper temperature limit	<input type="text" value="30.00"/>
Lower temperature limit	<input type="text" value="18.00"/>
<input type="button" value="OK"/>	

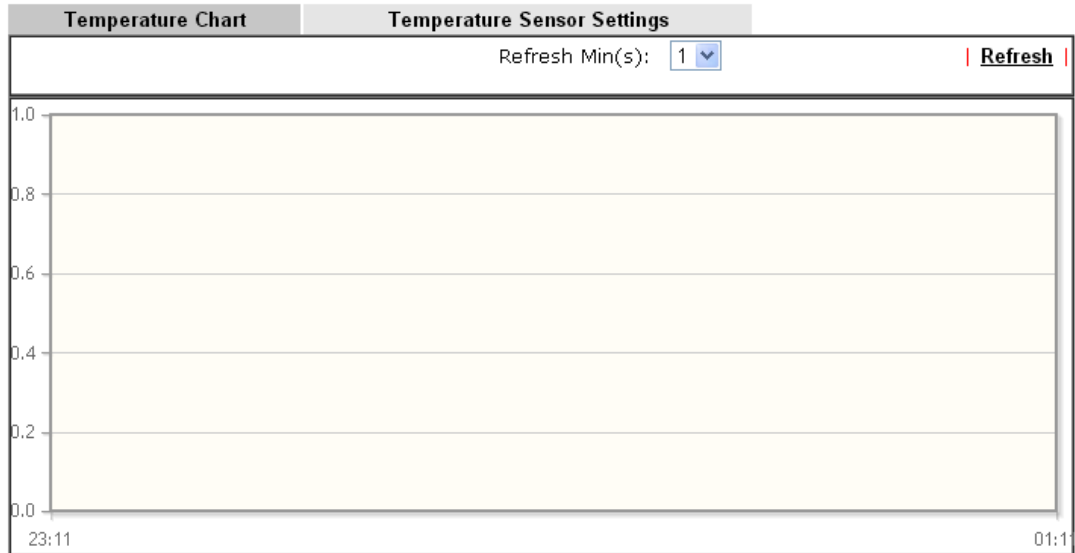
Available settings are explained as follows:

Item	Description
Display Settings	Temperature Calibration - Type a value used for correcting the temperature error. Temperature Unit - Choose the display unit of the temperature. There are two types for you to choose.
Alarm Settings	Enable Syslog Alarm - The temperature log will be recorded on Syslog if it is enabled. Upper temperature limit/Lower temperature limit - Enter the upper limit and lower limit for the system to send out temperature alert.

Temperature Chart

Below shows an example of temperature graph:

USB Application >> Temperature Sensor Graph



Manufacturer:
Product:
Current Temperature:
Average Temperature:
Maximum Temperature:
Minimum temperature:

VIII-2-6 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.

Brand	Model	LTE	Access Mode	Status
4G system	XSPlug P3		PPP	Y
Alcatel	Alcatel L100V	✔	PPP	Y
	Alcatel L800	✔	DHCP	Y
	Alcatel W100	✔	DHCP	Y
	Alcatel W800	✔	DHCP	Y
	Alcatel X080S		PPP	Y
	Alcatel Y855	✔	DHCP	M
Alfa	ALFA Flyppp		PPP	Y
BandRich	Bandlux C270		PPP	Y
	Bandlux C321		PPP	Y
	Bandlux C330		PPP	Y
	Bandlux C331		PPP	Y
	Bandlux C502		PPP	Y
BigPond	BigPond Next G Wireless		PPP	Y
D-Link	<u>D_LINK DWM156</u>		DHCP	Y
	<u>D_LINK DWM222</u>	✔	PPP	Y
	Huawei E150		PPP	Y
	Huawei E171		PPP	Y
	Huawei E1762		PPP	M
	Huawei E230		PPP	Y
	Huawei E303		DHCP	Y
	<u>Huawei E3131</u>		DHCP	Y
	<u>Huawei E3131</u>		PPP	Y

VIII-2-7 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

Application Notes

A-1 How can I get the files from USB storage device connecting to Vigor router?

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

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

1. Plug the USB device to the USB port on the router. Open USB Application>>USB Device Status. 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	<input type="button" value="Disconnect USB Disk"/>	
Write Protect Status:	No		
Disk Capacity:	2009 MB		
USB Disk Users Connected		<input type="button" value="Refresh"/>	
Index	Service	IP Address(Port)	Username

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

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

USB Application >> USB General Settings

USB General Settings


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

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: . ; : " < > * + = / \ | ?.

3. Setup a user account for the FTP service by using **USB Application >>USB User Management**. Click index #1 link, and click Enable to enable FTP/SMB User account. Here we add a new account "user1" and assign authorities "Read", "Write" and "List" to it.

USB Application >> USB User Management

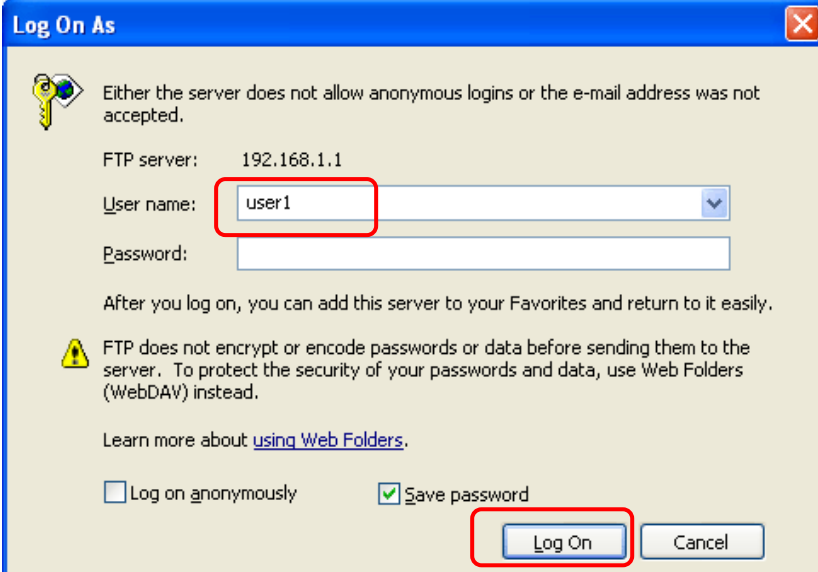
Profile Index: 1

FTP/SMB User	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	<input type="text" value="user1"/>
Password	<input type="password"/> (Maximum 11 Characters)
Confirm Password	<input type="password"/>
Home Folder	<input type="text"/> 
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

4. Click OK to save the configuration.
5. Make sure the FTP service is running properly. Please open a browser and type *ftp://192.168.1.1*. Use the account "user1" to login.



Log On As


Either the server does not allow anonymous logins or the e-mail address was not accepted.

FTP server: 192.168.1.1

User name:

Password:

After you log on, you can add this server to your Favorites and return to it easily.

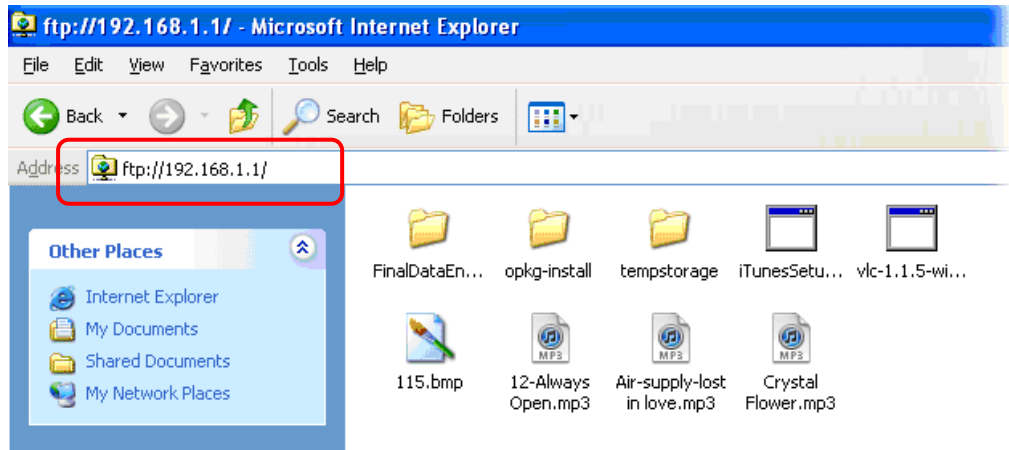
 FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use Web Folders (WebDAV) instead.

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

Log on anonymously Save password

Log On Cancel

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



7. 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

USB Disk Users Connected | Refresh |

Index	Service	IP Address(Port)	Username	Drop
1.	FTP	192.168.1.10(1963)	user1	Drop

Now, users in LAN of Vigor2762 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.

Part IX Troubleshooting



Troubleshooting

This part will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration

IX-1 Diagnostics

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 or DrayTek technical support for advanced help.

Web User Interface

First, take a look at the menu items under Diagnostics. Diagnostic Tools provide a useful way to view or diagnose the status of your Vigor router.

System Maintenance
Diagnostics
Dial-out Triggering
Routing Table
ARP Cache Table
IPv6 Neighbour Table
DHCP Table
NAT Sessions Table
DNS Cache Table
Ping Diagnosis
Data Flow Monitor
Traffic Graph
Trace Route
Syslog Explorer
IPv6 TSPC Status
DSL Status
DoS Flood Table
Route Policy Diagnosis

IX-1-1 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.

IX-1-2 Routing Table

Click Diagnostics and click Routing Table to open the web page.

Diagnostics >> View Routing Table

IPv4

Key	Destination	Gateway	Interface
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
S~	211.100.88.0/ 255.255.255.0	via 192.168.1.3	LAN1

Key

C: Connected S: Static R: RIP *: default ~: private

Note:

WAN4, WAN5, WAN6 are router-borne WANs.

IPv6

Destination	Interface	Flags	Metric	Next Hop
FE80::/64	LAN1	U	256	::
FE80::/64	LAN2	U	256	::
FE80::/64	DMZ	U	256	::
FF00::/8	LAN1	U	256	::
FF00::/8	LAN2	U	256	::
FF00::/8	DMZ	U	256	::

Show Detail

Flag

U: Route UP F: Default Route G: Use Next Hop S: Static Route R: RIPng

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

IX-1-3 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-	A1000351	LAN1	VLAN0	P1

Show Comment

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

IX-1-4 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	
FF02::2	33-33-00-00-00-02	LAN	
FF02::1:3	33-33-00-01-00-03	LAN	
FE80::3D5E:E74:8751:A44B	e8-9d-87-87-69-2f	LAN	
FF02::1:FF51:A44B	33-33-ff-51-a4-4b	LAN	
FE80::250:7FFF:FEC9:1E79	00-50-7f-c9-1e-79	LAN	
FE80::250:7FFF:FEC8:4305	00-50-7f-c8-43-05	LAN	
FF02::1	33-33-00-00-00-01	LAN	
FF02::1	00-00-00-00-00-00	USB2	
FF02::1:2	00-00-00-00-00-00	USB2	
FE80::9D5C:CA86:5428:3CA7	00-26-2d-fe-63-4f	LAN	
FF02::1:FF0A:673C	33-33-ff-0a-67-3c	LAN	

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

IX-1-5 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

Show :

DHCP IP Assignment Table		Other IP Assignment Table			Refresh
LAN1 : DHCP Server On IP Pool: 192.168.1.10 ~ 192.168.1.209					
Index	IP Address	MAC Address	Leased Time	HOST ID	

LAN1					
1	192.168.1.10	00-50-7F-F1-05-FD	22:08:44		

Show Comment

DHCPv6 IP Assignment Table

| Refresh |

Index	IPv6 Address	IAID	Link-layer Address	Lease

Available settings are explained as follows:

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

IX-1-6 NAT Sessions Table

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

Diagnostics >> NAT Sessions Table

NAT Active Sessions Table [Refresh](#)

Private IP :Port	#Pseudo Port	Peer IP :Port	Interface
192.168.1.11 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.

IX-1-7 DNS Cache Table

Click Diagnostics and click DNS Cache Table to open the web page.

The record of domain Name and the mapping IP address for answering the DNS query from LAN will be stored on Vigor router's Cache temporarily and displayed on Diagnostics >> DNS Cache Table.

Diagnostics >> DNS Cache Table

IPv4 DNS Cache Table

| [Clear](#) | [Refresh](#) |

Domain Name	IP Address	TTL (s)
-------------	------------	---------

IPv6 DNS Cache Table

| [Clear](#) | [Refresh](#) |

Domain Name	IP Address	TTL (s)
-------------	------------	---------

Note:

The LAN DNS entry's TTL is static.

When an entry's TTL is larger than s, this entry will be deleted from the table.

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...	Check the box the Enter the value of TTL (time to live) for each entry. Click OK to enable such function. It means when the TTL value of each DNS query reaches the threshold of the value specified here, the corresponding record will be deleted from router's Cache automatically.

IX-1-8 Ping Diagnosis

Click Diagnostics and click Ping Diagnosis to open the web page.

Diagnostics >> Ping Diagnosis

Ping Diagnosis

IPV4 IPV6

Ping through: Auto

Source IP: Auto

Ping to: Host / IP
Host / IP
DNS
Gateway 1
Gateway 2
Gateway 3

IP Address:

Run

Result | Clear |

Note:

1. If you want to ping a LAN PC or you don't want to specify which WAN to ping through, please select "Auto" in Ping Through.
2. If you select "Auto" in Source IP, we will fill Source IP according to the interface you ping through.

or

Diagnostics >> Ping Diagnosis

Ping Diagnosis

IPV4 IPV6

Ping through: Auto

Ping IPv6 Address:

Auto
WAN1
WAN2
WAN3

Run

Result | Clear |

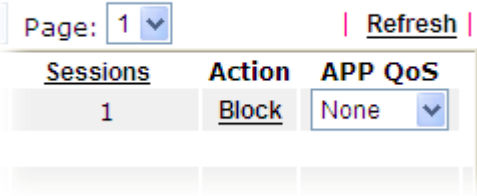
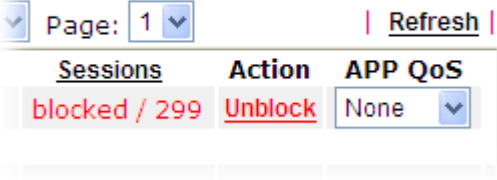
Note:

1. If you want to ping a LAN PC or you don't want to specify which WAN to ping through, please select "Auto" in Ping Through.
2. If you select "Auto" in Source IP, we will fill Source IP according to the interface you ping through.

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.

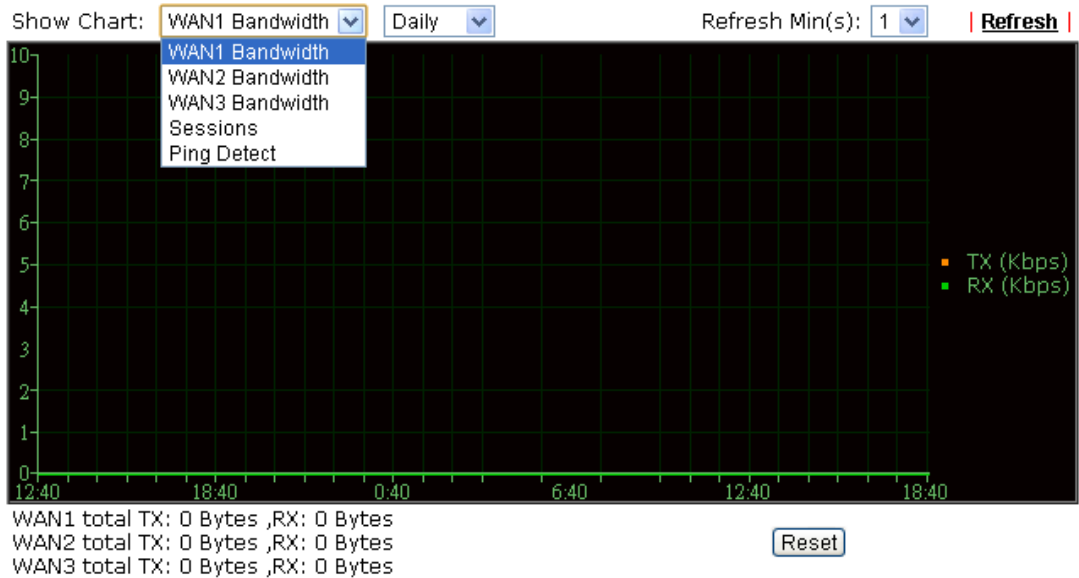
Ping to	Use the drop down list to choose the destination that you want to ping.
IP Address	Enter the IP address of the Host/IP that you want to ping.
Ping IPv6 Address	Enter the IPv6 address that you want to ping.
Run	Click this button to start the ping work. The result will be displayed on the screen.
Clear	Click this link to remove the result on the window.

	refreshing data flow that will be done by the system automatically.
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 for five minutes. The remaining time will be shown on the session column. Click it to cancel the IP address blocking.</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>

IX-1-10 Traffic Graph

Click Diagnostics and click Traffic Graph to open the web page. Choose WAN1/WAN2/WAN3 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. Click Reset to zero the accumulated RX/TX (received and transmitted) data of WAN. Click Refresh to renew the graph at any time.

Diagnostics >> Traffic Graph



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.

IX-1-11 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 Enter 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.

IX-1-12 Syslog Explorer

Such page provides real-time syslog and displays the information on the screen.

For Web Syslog

This page displays the time and message for User/Firewall/call/WAN/VPN settings. You can check Enable Web Syslog, specify the type of Syslog and choose the display mode you want. Later, the event of Syslog with specified type will be shown for your reference.

Diagnostics >> Syslog Explorer

Web Syslog
USB Syslog

Enable Web Syslog

[Export](#) | [Refresh](#) | [Clear](#)

Syslog Type User
Display Mode Stop record when fulls

Time	Message

Available settings are explained as follows:

Item	Description
Enable Web Syslog	Check this box to enable the function of Web Syslog.
Syslog Type	Use the drop down list to specify a type of Syslog to be displayed.
Export	Click this link to save the data as a file.
Refresh	Click this link to refresh this page manually.
Clear	Click this link to clear information on this page.
Display Mode	<p>There are two modes for you to choose.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> Stop record when fulls </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> Stop record when fulls </div> <div style="border: 1px solid #ccc; padding: 5px;"> Always record the new event </div> <p>Stop record when fulls - when the capacity of syslog is full, the system will stop recording.</p> <p>Always record the new event - only the newest events will be recorded by the system.</p>
Time	Display the time of the event occurred.
Message	Display the information for each event.

For USB Syslog

This page displays the syslog recorded on the USB storage disk.

Diagnostics >> Syslog Explorer

Web Syslog	USB Syslog
------------	------------

Note: The syslog will show while the saved syslog file size is over 1MB.

Folder: n/a File: n/a Page: n/a Log Type: n/a

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.

IX-1-13 IPv6 TSPC Status

IPv6 TSPC status web page could help you to diagnose the connection status of TSPC.

If TSPC has configured properly, the router will display the following page when the user connects to tunnel broker successfully.

Diagnostics >> IPv6 TSPC Status

WAN1	WAN2	WAN3	Refresh
TSPC Enabled			
TSPC Connection Status			
Local Endpoint v4 Address :	114.44.54.220		
Local Endpoint v6 Address :	2001:05c0:1400:000b:0000:0000:0000:10b9		
Router DNS name :	88886666.broker.freenet6.net		
Remote Endpoint v4 Address :	81.171.72.11		
Remote Endpoint v6 Address :	2001:05c0:1400:000b:0000:0000:0000:10b8		
Tspc Prefix :	2001:05c0:1502:0d00:0000:0000:0000:0000		
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.

IX-1-14 DSL Status

Such page is useful for RD debug or web technician.

Diagnostics >> DSL Status

General		Refresh		
ATU-R Information				
Type:	ADSL2/2+			
Hardware:	Annex A			
Firmware:	05-04-04-04-00-01			
Power Mngt Mode:	DSL_G997_PMS_NA			
Line State:	TRAINING			
Running Mode:				
Vendor ID:	b5004946 544e0000			
ATU-C Information				
Vendor ID:	00000000 00000000 [unknown]			
Line Statistics				
	<u>Downstream</u>		<u>Upstream</u>	
Actual Rate	0	Kbps	0	Kbps
Attainable Rate	0	Kbps	0	Kbps
Path Mode	Fast		Fast	
Interleave Depth	0		0	
Actual PSD	0.0	dB	0.0	dB
	<u>Near End</u>		<u>Far End</u>	
Trellis	ON		ON	
Bitswap	OFF		OFF	

IX-1-15 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	Refresh
Tracing IP		Destination Port	

192.168.1.22	80	Block	
192.168.1.205	40005(⊗)	Block	

IPv6

SYN Flood	UDP Flood	ICMP Flood	Refresh
Tracing IP		Destination Port	



Info

The icon - (⊗) - means there is something wrong (e.g., attacking the system) with that IP address.

IX-1-16 Route Policy Diagnosis

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.

Diagnostics >> Route Policy Diagnosis

Test how the packets will be routed

- Mode** Analyze a single packet
 Analyze multiple packets by uploading an input file

Packet Information

Protocol

Src IP

Dst IP

Dst Port

Analyze

Available settings are explained as follows:

Item	Description
Mode	Analyze a single packet - Choose such mode to make Vigor router analyze how a single packet will be sent by a route policy. Analyze multiple packets... - Choose such mode to make Vigor router analyze how multiple packets in a specified file will be sent by a route policy.
Packet Information	Specify the nature of the packets to be analyzed by Vigor router. ICMP/UDP/TCP/ANY- Specify a protocol for diagnosis. Src IP - Type an IP address as the source IP. Dst IP - Type an IP address as the destination IP. Dst Port - Use the drop down list to specify the destination port. Analyze - Click it to perform the job of analyzing. The analyzed result will be shown on the page.
Input File	It is available when Analyze multiple packets.. is selected as Mode. 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.

Mode

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

Input File

選擇檔案
Analyze



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.

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

選擇檔案 未選擇檔案 (download an example input file)

Analyze

Analysis [export analysis](#)

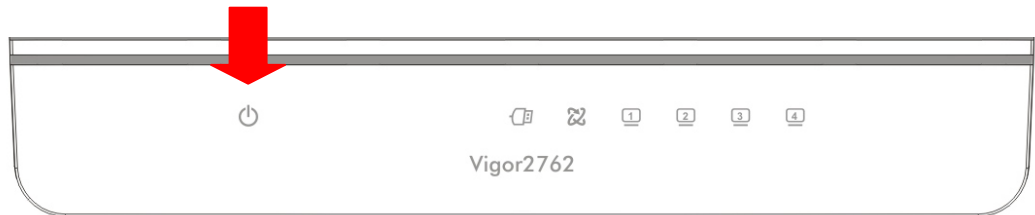
Profile	Input Packet Information			Matched Route		Matched Policy			Final Result		
	Proto	Src IP	Out IP	Route	Priority	Policy	Priority	Is/overlapped	Interface	Reason	
LA-branch	ICMP	192.168.1.10	19.10.10.10	N/A	No Match	N/A	No Match	N/A	N/A	N/A	The packet was dropped because neither "route" or "policy" was matched
Nr-branch	TCP	192.168.1.20	20.20.20.20	5060	No Match	N/A	No Match	N/A	N/A	N/A	The packet was dropped because neither "route" or "policy" was matched
											The packet was dropped because neither "route" or "policy" was matched

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.

IX-2 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 “I-2 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 “I-2 Hardware Installation” to execute the hardware installation again. And then, try again.

IX-3 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



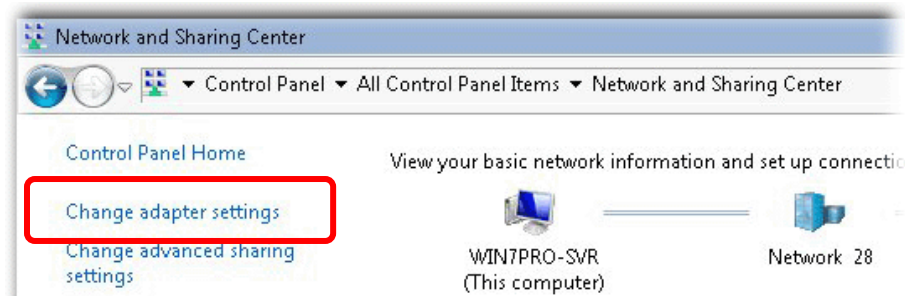
Info

The example is based on Windows 7. As to the examples for other operation systems, please refer to the similar steps or find support notes in www.DrayTek.com.

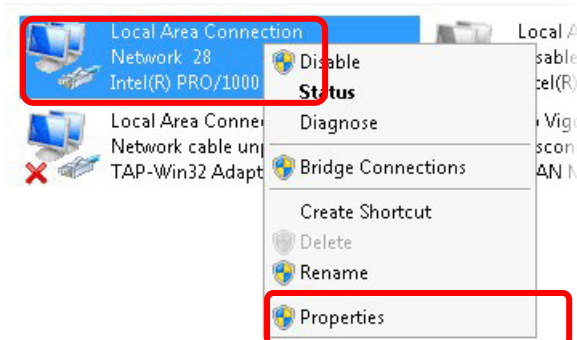
1. Open All Programs>>Getting Started>>Control Panel. Click Network and Sharing Center.



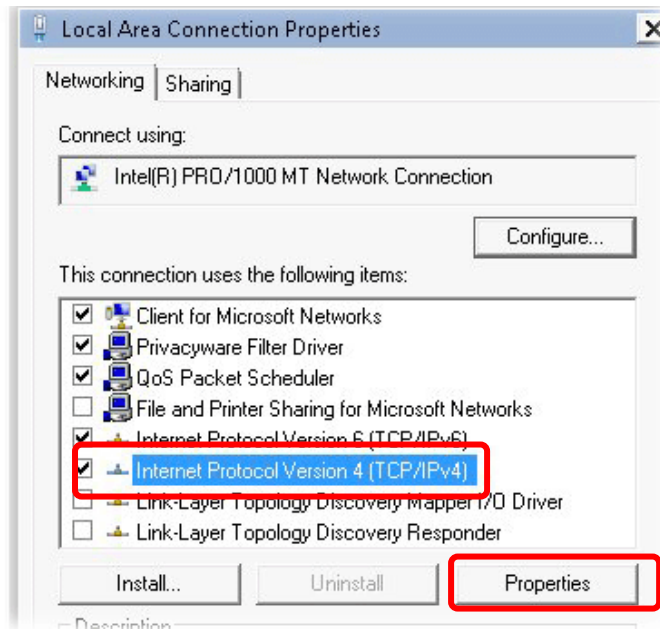
2. In the following window, click Change adapter settings.



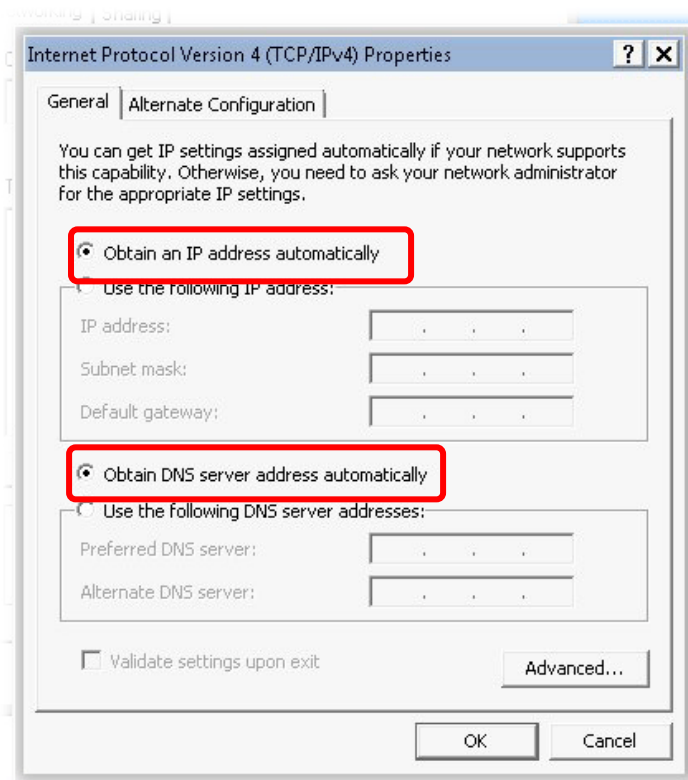
3. Icons of network connection will be shown on the window. Right-click on Local Area Connection and click on Properties.



4. Select Internet Protocol Version 4 (TCP/IP) and then click Properties.

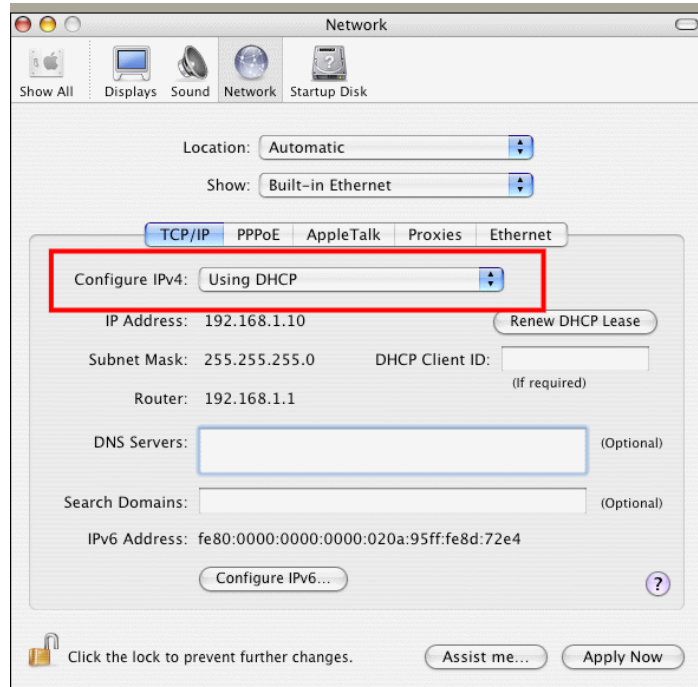


5. Select Obtain an IP address automatically and Obtain DNS server address automatically. Finally, click OK.



For Mac OS

1. Double click on the current used Mac OS on the desktop.
2. Open the Application folder and get into Network.
3. On the Network screen, select Using DHCP from the drop down list of Configure IPv4.



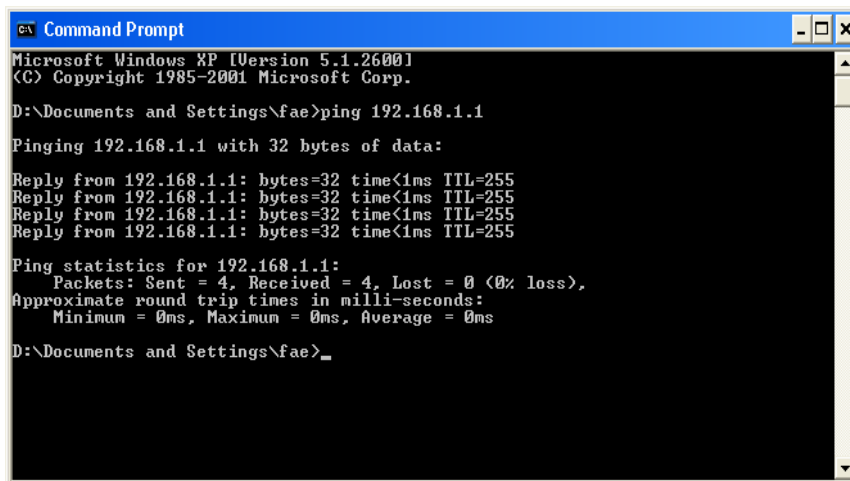
IX-4 Pinging the Router from Your Computer

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 VIII-3).

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/7/8). The DOS command dialog will appear.



```
Command Prompt
Microsoft Windows XP [Version 5.1.2600.1
(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 MacOs on the desktop.
2. Open the Application folder and get into Utilities.
3. Double click Terminal. The Terminal window will appear.
4. Type ping 192.168.1.1 and press [Enter]. If the link is OK, the line of “64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxx ms” will appear.


```
Terminal — bash — 80x24
Last login: Sat Jan  3 02:24:18 on ttty1
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$ █
```

IX-5 Checking If the ISP Settings are OK or Not

If WAN connection cannot be up, check if the LEDs (according to the LED explanations listed on section I-1) are correct or not. If the LEDs are off, please:

- Change the Physical Type from Auto negotiation to other values (e.g., 100M full duplex).
- Next, change the physical type of modem (e.g., DSL) offered by ISP with the same value configured in Vigor router. Check if the LEDs on Vigor router are on or not.
- If not, please install an additional switch for connecting both Vigor router and the modem offered by ISP. Then, check if the LEDs on Vigor router are on or not.
- If the problem of LEDs cannot be solved by the above measures, please contact with the nearest reseller, or send an e-mail to DrayTek FAE for technical support.
- Check if the settings offered by ISP are configured well or not.

When the LEDs are on and correct, yet the WAN connection still cannot be up, please:

- Open WAN >> Internet Access page and then check whether the ISP settings are set correctly. Click Details Page of WAN1~WAN4 to review the settings that you configured previously.

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode	Details Page	IPv6
WAN1		ADSL / VDSL2	PPPoE / PPPoA	Details Page	IPv6
WAN2		Ethernet	None	Details Page	IPv6
WAN3		USB	MPoA / Static or Dynamic IP	Details Page	IPv6

IX-6 Problems for 3G/4G Network Connection

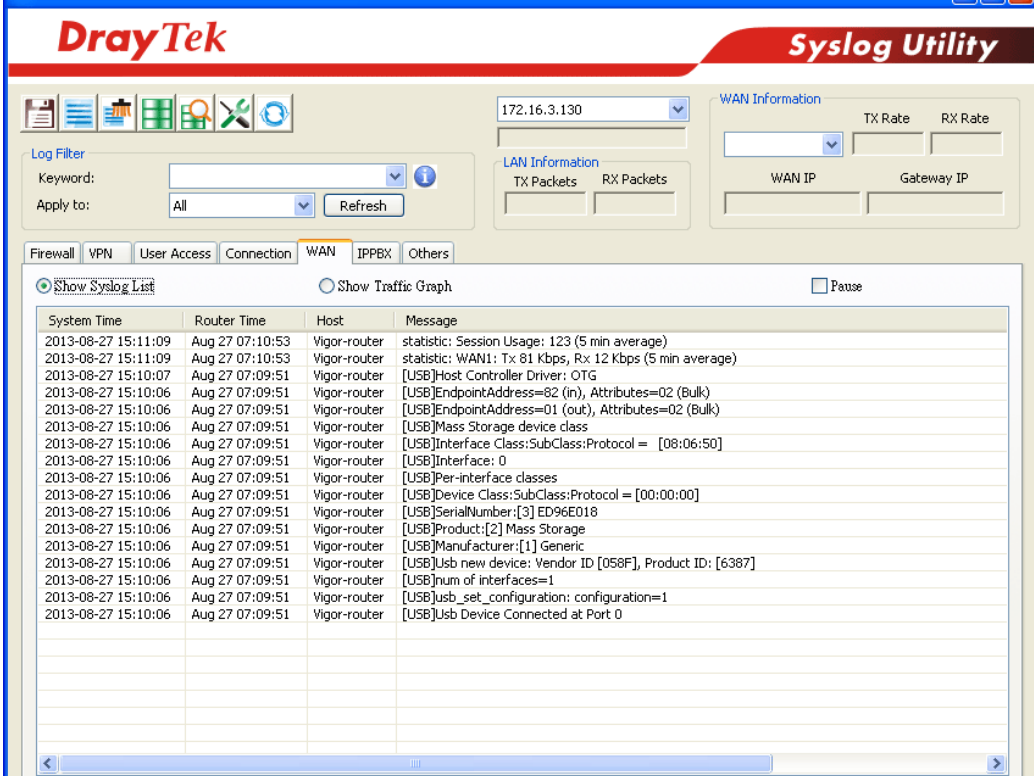
When you have trouble in using 3G/4G network transmission, please check the following:

Check if USB LED lights on or off

You have to wait about 15 seconds after inserting 3G/4G USB Modem into your Vigor2762. 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 Vigor2762.

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.



The screenshot displays the DrayTek Syslog Utility web interface. At the top, the DrayTek logo is on the left and 'Syslog Utility' is on the right. Below the logo is a navigation bar with icons for various system functions. The main area is divided into several sections:

- Log Filter:** Includes a 'Keyword:' input field, an 'Apply to:' dropdown menu set to 'All', and a 'Refresh' button.
- WAN Information:** Shows the WAN IP address as 172.16.3.130. It also has fields for TX Rate, RX Rate, WAN IP, and Gateway IP.
- LAN Information:** Includes fields for TX Packets and RX Packets.
- Navigation Tabs:** 'Firewall', 'VPN', 'User Access', 'Connection', 'WAN' (selected), 'IPPEX', and 'Others'.
- Display Options:** Radio buttons for 'Show Syslog List' (selected) and 'Show Traffic Graph', along with a 'Pause' checkbox.
- Syslog List Table:** A table with columns for System Time, Router Time, Host, and Message. The messages show statistics and USB device connection details.

System Time	Router Time	Host	Message
2013-08-27 15:11:09	Aug 27 07:10:53	Vigor-router	statistic: Session Usage: 123 (5 min average)
2013-08-27 15:11:09	Aug 27 07:10:53	Vigor-router	statistic: WAN1: Tx 81 Kbps, Rx 12 Kbps (5 min average)
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Host Controller Driver: OTG
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]EndpointAddress=82 (in), Attributes=02 (Bulk)
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]EndpointAddress=01 (out), Attributes=02 (Bulk)
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Mass Storage device class
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Interface Class:SubClass:Protocol = [08:06:50]
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Interface: 0
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Per-interface classes
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Device Class:SubClass:Protocol = [00:00:00]
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]SerialNumber:[3] ED96E018
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Product:[2] Mass Storage
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Manufacturer:[1] Generic
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]usb new device: Vendor ID [058F], Product ID: [6387]
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]num of interfaces=1
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]usb_set_configuration: configuration=1
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]usb Device Connected at Port 0

Transmission Rate is not fast enough

Please connect your Notebook with 3G/4G USB Modem to test the connection speed to verify if the problem is caused by Vigor2762. In addition, please refer to the manual of 3G/4G 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.

IX-7 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.



Info

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.

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

Schedule Profile : None ▾, None ▾, None ▾, None ▾

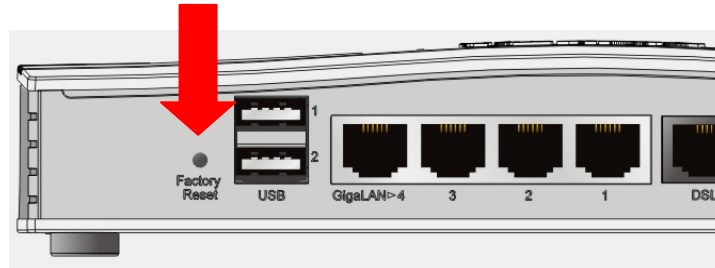
Note: Action and Idle Timeout settings will be ignored.

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.

IX-8 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.

This page is left blank.

Part X DrayTek Tools

X-1 SmartVPN Client

X-1-1 DrayTek Android-based SmartVPN APP for the establishment of SSL VPN connection

DrayTek has been the world-leading company to integrate VPN with Vigor SOHO routers to serve professionals and business customers with secure data transactions over Internet. The facilities of VPN let businesses are able to receive and send data over Internet with secure tunnels. We provide multiple protocol VPN connections such as IPSec/PPTP/L2TP protocols for secure data exchange and communication. With SSL VPN embedded on Vigor routers, teleworkers can have convenient and simple 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.



DrayTek provided free SmartVPN for Windows-based users to easily establish VPN tunnels. There were million downloads. Now, DrayTek released Android-based SmartVPN app for those who would like to set up SSL VPN connection with the VPN server working at the main office. The SmartVPN app is available for your free download! Then, you can use the SmartVPN App on smartphone/tablet PC to establish SSL VPN tunnels with your main office.

X-1-2 How to Use SmartVPN Android APP to Establish SSL VPN Tunnel?

SmartVPN APP for Android is now available on Google play. This document demonstrates how to use the APP to establish a SSL VPN tunnel.

1. On VPN server, create a SSL user account. Please refer to “How to Set up SSL VPN” on www.draytek.com for detailed instructions.

SSL VPN >> Remote Dial-in User

Index No. 1

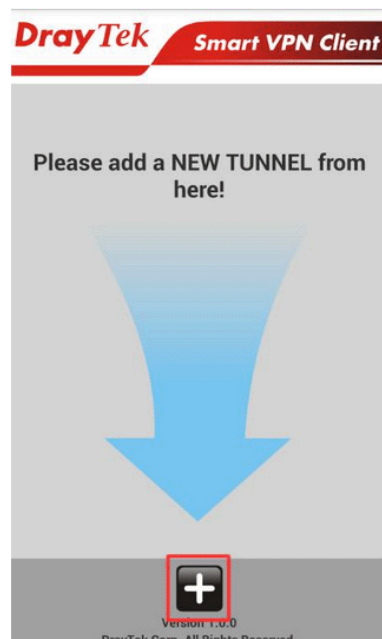
User account and Authentication <input checked="" type="checkbox"/> Enable this account Idle Timeout: <input type="text" value="300"/> second(s)	Username: <input type="text" value="draytek"/> Password(Max 19 char): <input type="password" value="****"/> <input type="checkbox"/> Enable Mobile One-Time 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 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 IKE Pre-Shared Key: <input type="text"/> <input type="checkbox"/> Digital Signature(X.509) <input type="text" value="None"/>
Subnet <input type="text" value="LAN 1"/> <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"/>

OK Clear Cancel

2. Download the APP from Google play, and run the APP.



3. Click “+” to add a new profile.



4. Edit the profile.
 - a. Enter description of this profile.
 - b. Enter VPN Server's IP in Server.
 - c. Enter Port as the port which VPN server uses for SSL VPN; for Vigor Routers, it is 443 by default.
 - d. Tap SAVE to save the profile or "<" to cancel.



Info

Installation of relevant Root CA is required to enable server certificate authentication.

If you check "Use default gateway on remote network", all the traffic of this smart device will be forwarded to the remote gateway.

5. Tap the profile bar to establish SSL VPN tunnel.



6. Enter Username and Password, then tap Dial.

7. When the tunnel is up, the profile will turn green. Tap the bar again will disconnect the tunnel.



8. Tap the pencil icon to edit or remove the profile.



This page is left blank.

Part XI Telnet Commands

Accessing Telnet of Vigor2762

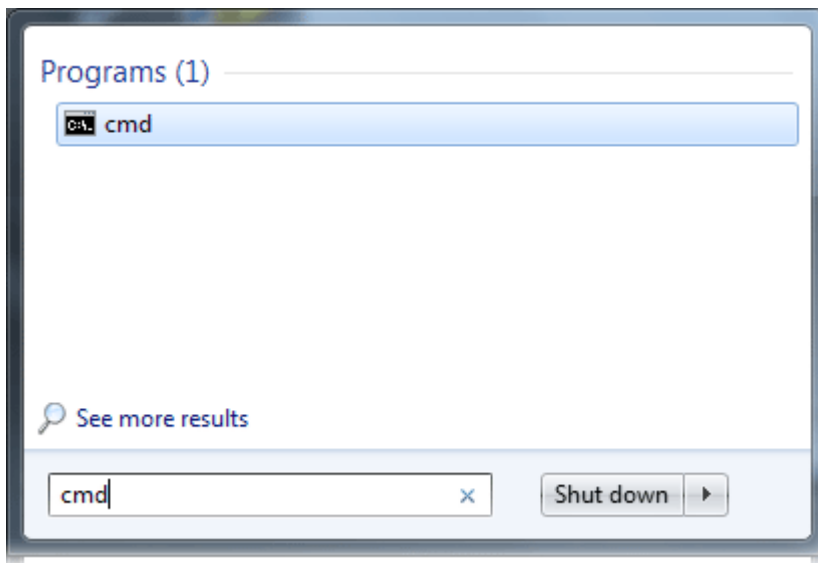
This chapter also gives you a general description for accessing telnet and describes the firmware versions for the routers explained in this manual.



Info

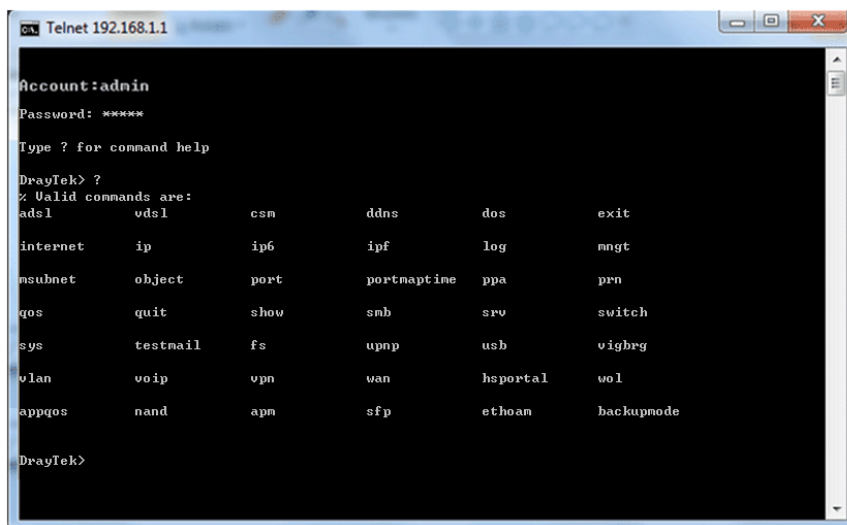
For Windows 7 user, please make sure the Windows Features of Telnet Client has been turned on under Control Panel>>Programs.

Type cmd and press Enter. The Telnet terminal will be open later.



In the following window, type Telnet 192.168.1.1 as below and press Enter. Note that the IP address in the example is the default address of the router. If you have changed the default, enter the current IP address of the router.

Next, type admin/admin for Account/Password. Then, type ?. You will see a list of valid/common commands depending on the router that you use.



Telnet Command: adsl txpct /adsl rxpct

This command allows the user to adjust the percentage of data transmission (receiving/transmitting) for QoS application.

Syntax

adsl txpct [auto:percent]

adsl rxpct [auto:percent]

Syntax	Description
auto	It means auto detection of ADSL transmission packet.
percent	It means to specify the percentage of ADSL transmission packet. Available range is 10-100.

Example

```
> adsl txpct auto
% tx percentage : 80
> adsl txpct 75
% tx percentage : 75
```

Telnet Command: adsl status

This command is used to display current status of ADSL setting.

Syntax

adsl status

Example

```
> adsl status
----- ATU-R Info (hw: annex A, f/w: annex A) -----
Running Mode      :                               State      : TRAINING
DS Actual Rate    :          0 bps   US Actual Rate    :          0 bps
DS Attainable Rate :          0 bps   US Attainable Rate :          0 bps
DS Path Mode      :          Fast   US Path Mode      :          Fast
DS Interleave Depth :          0     US Interleave Depth :          0
NE Current Attenuation :          0 dB   Cur SNR Margin    :          0 dB
DS actual PSD     :          0.0 dB   US actual PSD     :          0.0 dB
NE Rcvd Cells     :          0       NE Xmitted Cells   :          0
NE CRC Count      :          0       FE CRC Count      :          0
NE ES Count       :          0       FE ES Count       :          0
Xdsl Reset Times  :          0       Xdsl Link Times   :          0
ITU Version[0]    : b5004946        ITU Version[1]    : 544e0000
ADSL Firmware Version : 06-06-01-07-00-01
Power Management Mode : DSL_G997_PMS_NA
Test Mode        : DISABLE
----- ATU-C Info -----
Far Current Attenuation :          0 dB   Far SNR Margin    :          0 dB
CO ITU Version[0]      : 00000000      CO ITU Version[1] : 00000000
DSLAM CHIPSET VENDOR   : < ----- >
>
```

Telnet Command: adsl ppp

This command can set the Internet Access mode for the router.

Syntax

`adsl ppp [? | pvc_no vci vpi Encap Proto modu acqIP idle [Username Password]`

Syntax Description

Parameter	Description
?	Display the command syntax of “adsl ppp”.
pvc_no	It means the PVC number and the adjustable range is from 0 (Channel-1) to 7(Channel-8).
Encap	Different numbers represent different modes. 0 : VC_MUX, 1: LLC/SNAP, 2: LLC_Bridge, 3: LLC_Route, 4: VCMUX_Bridge 5: VCMUX_Route, 6: IPoE.
Proto	It means the protocol used to connect Internet. Different numbers represent different protocols. 0: PPPoA, 1: PPPoE, 2: MPoA.
Modu	0: T1.413, 2: G.dmt, 4: Multi, 5: ADSL2, 7:ADSL2_AnnexM 8:ADSL2+ 14:ADSL2+_AnnexM.
acqIP	It means the way to acquire IP address. Enter the number to determine the IP address by specifying or assigned dynamically by DHCP server. 0 : fix_ip, 1: dhcp_client/PPPoE/PPPoA.(acquire IP method)
idle	Type number to determine the network connection will be kept for always or idle after a certain time. -1: always on, else idle timeout secs. Only for PPPoE/PPPoA.
Username	This parameter is used only for PPPoE/PPPoA.
Password	This parameter is used only for PPPoE/PPPoA.

You have to reboot the system when you set it on Route mode.

Example


```

> adsl ppp o 35 8 1 1 4 1 -1 draytek draytek
pvc no.=0
vci=35
vpi=8
encap=LLC(1)
proto=PPPoE(1)
modu=MULTI(4)
AcquireIP: Dhcp_client(1)
Idle timeout:-1
Username=draytek
Password=draytek

```

Telnet Command: adsl bridge

This command can specify a LAN port (LAN1 to LAN4) for mapping to certain PVC, and the mapping port/PVC will be operated in bridge mode.

`adsl bridge [pvc_no/status/save/enable/disable] [on/off/clear/tag tag_no] [service type] [px ...]`

Syntax Description

Parameter	Description
<i>pvc_no</i>	It means <i>pvc</i> number and must be between 0(Channel 1) to 7(Channel 8).
<i>status</i>	It means to shown the whole bridge status.
<i>save</i>	It means to save the configuration to flash.
<i>enable</i>	It means to enable the Multi-VLAN function.
<i>disable</i>	It means to disable the Multi-VLAN function.
<i>on/off</i>	It means to turn on/off bridge mode for the specific channel.
<i>clear</i>	It means to turn off and clear all the PVC settings.
<i>tag tag_no</i>	No tag: -1 Available number for tag: 0-4095
<i>pri pri_no</i>	The number 0 to 7 can be set to indicate the priority. "7" is the highest.
<i>service type</i>	Two number can be set: 0: for Normal (all the applications will be processed with the same PVC). 1: for the IGMP with different PVC which is used for special ISP.
<i>px...</i>	It means the number of LAN port (x=2-4). Port 1 is locked for NAT.

Example

```

> adsl bridge 4 on p2 p3
PVC Bridge p1 p2 p3 p4 Service Type Tag Pri

```

```
-----  
4   ON      0   0   1   0   Normal   -1(OFF)  0  
PVC 0 & 1 can't set for bridge mode.  
Please use 'save' to save config.
```

Telnet Command: adsl drivermode

This command is useful for laboratory to measure largest power of data transmission. Please follow the steps below to set adsl drivermode.

1. Please connect dsl line to the DSLAM.
2. Waiting for dsl SHOWTIME.
3. Drop the dsl line.
4. Now, it is on continuous sending mode, and adsl2/2+ led is always ON.
5. Use 'adsl reboot' to restart dsl to normal mode.

Telnet Command: adsl reboot

This command can wake up the idle router.

Example

```
> adsl reboot  
% Adsl is Rebooting...
```

Telnet Command: adsl oamlb

This command is used to test if the connection between CPE and CO is OK or not.

`adsl oamlb [n][type]`

`adsl oamlb chklink [on/off]`

`adsl oamlb [log_on/log_off]`

Syntax Description

Parameter	Description
<i>n</i>	It means the total number of transmitted packets.
<i>type</i>	It means the protocol that you can use. 1 - for F4 Seg-to-Seg (VP level) 2 - for F4 End-to-End (VP level) 4 - for F5 Seg-to-Seg (VC level) 5 - for F5 End-to-End (VC level)
<i>chklink</i>	Check the DSL connection.
<i>Log_on/log_off</i>	Enable or disable the OAM log for debug.

Example

```
> adsl oamlb chklink on
OAM checking dsl link is ON.
> adsl oamlb F5 4
Tx cnt=0
Rx Cnt=0
>
```

Telnet Command: adsl vcilimit

This command can cancel the limit for vci value.

Some ISP might set the vci value under 32. In such case, we can cancel such limit manually by using this command. Do not set the number greater than 254.

`adsl vcilimit [n]`

Syntax Description

Parameter	Description
<i>n</i>	The number shall be between 1 - 254.

Example

```
> adsl vcilimit 33
change VCI limitation from 32 to 33.
```

Telnet Command: adsl annex

This command can display the annex interface of this router.

Example

```
> adsl annex
% hardware is annex B.
% modem code is annex B; built at 01/15,07:34.
```

Telnet Command: adsl automode

This command is used to add or remove ADSL modes (such as ANNEXL, ANNEXM and ANNEXJ) supported by Multimode.

`adsl automode [add/remove/set/default/show] [adsl_mode]`

Syntax Description

Parameter	Description
<i>add</i>	Add ADSL mode.
<i>remove</i>	Remove ADSL mode.
<i>set</i>	Use default settings plus the new added ADSL mode.
<i>default</i>	Use default settings.
<i>show</i>	Display current setting.
<i>adsl_mode</i>	There are three modes to be choose, ANNEXL, ANNEXM and ANNEXJ.

Example

```
>Vigor> adsl automode set ANNEXJ
Automode supported : T1.413, G.DMT, ADSL2, ADSL2+, ANNEXJ,

Vigor> adsl automode default
Automode supported : T1.413, G.DMT, ADSL2, ADSL2+,
```

Telnet Command: adsl showbins

This command can display the allocation for each Bin (Tone) SNR, Gain, and Bits.

`adsl showbins [startbin endbin [up]]`

Syntax Description

Parameter	Description
<i>startbin</i>	The number is between 0 ~ 4092.
<i>endbin</i>	The number is between 4 ~ 4095.
<i>up</i>	Show upstream information.

Example

```
> adsl showbins 2 30
DOWNSTREAM :
-----
Bin  SNR  Gain Bi - Bin  SNR  Gain Bi - Bin  SNR  Gain Bi - Bin  SNR  Gain Bi
```

```

dB .1dB ts      dB .1dB ts      dB .1dB ts      dB .1dB ts
-----
-----
Bin SNR Gain Bi - Bin SNR Gain Bi - Bin SNR Gain Bi - Bin SNR Gain Bi
dB .1dB ts      dB .1dB ts      dB .1dB ts      dB .1dB ts
>

```

Telnet Command: adsl optn

This command allows you to configure DSL line feature. This feature is depended on modem firmware. For G.Vector feature, modem firmware needs to support VDSL2 G.Vector.

adsl optn FUNC [*us/ds/bi* [*value/on/off*]

Syntax Description

Parameter	Description
<i>FUNC</i>	Available functions include: 'trellis', 'bitswap', 'sra', 'retx', 'aelem', 'status', 'g.vector', 'default'. default: Set all features back to default settings.
<i>us/ds/bi</i>	us: means "upstream" ds: means "downstream" bi: means "bidirection"
<i>value</i>	The values for different functions change slightly. bitswap=0-2, sra=0,2,3,4.
<i>on/off</i>	Type "on" for enabling such function. Type "off" for disabling such function. Functions of 'aelem' and 'g.vector' are only on/off.

Example

```

> adsl optn status
trellis      [US] =    ON, [DS] =    ON.
bitswap      [US] =    0, [DS] =    0.
              [0: default(ON), 1: ON, 2: OFF]
sra          [US] =    0, [DS] =    0.
              [0: default(=3), 2: OFF, 3: ON , 4: DYNAMIC_SOS]
retx         [US] =    ON, [DS] =    ON.
aelem        ON
G.Vector     ON

```

Telnet Command: adsl savecfg

This command can save the configuration into FLASH with a file format of cfg.

Example

```

> adsl savecfg
% Xdsl Cfg Save OK!

```

Telnet Command: adsl vendorid

This command allows you to configure user-defined CPE vendor ID.

adsl vendorid [*status/on/off/ set vid0 vid1*]

Syntax Description

Parameter	Description
<i>status</i>	Display current status of user-defined vendor ID.
<i>on</i>	Enable the user-defined function.
<i>off</i>	Disable the user-defined function.
<i>set vid0 vid1</i>	It means to set user-defined vendor ID with vid0 and vid1. The vendor ID shall be set with HEX format, ex: 00fe7244: 79612f21.

Example

```
> adsl vendorid status
% User define CPE Vendor ID is OFF
% vid0:vid1 = 0x00fe7244:79612f21
> adsl vendorid on set vid0 vid1
% User define CPE Vendor ID is ON
```

Telnet Command: adsl atm

This command can set QoS parameter for ATM.

```
adsl atm pcr [pvc_no][PCR][max][status]
```

```
adsl atm scr [pvc_no][SCR][status]
```

```
adsl atm mbs [pvc_no][MBS][status]
```

```
adsl atm status
```

Syntax Description

Parameter	Description
<i>pvc_no</i>	It means <i>pvc</i> number and must be between 0(Channel 1) to 7(Channel 8).
<i>PCR</i>	It means Peak Cell Rate for upstream. The range for the number is "1" to "2539".
<i>max</i>	Get the highest speed for the upstream.
<i>SCR</i>	Mean Sustainable Cell Rate. The range for the number is "1" to "2539".
<i>MBS</i>	Maximum Burst Size. The range for the number is "1" to "2539".
<i>status</i>	Display PCR/SCR/MBS setting.

Example

```
> adsl atm pcr 1 200 max
% PCR is 0 for pvc 1.
> adsl atm pcr status
pvc  channel      PCR
-----
0     1             0
1     2             0
2     3             0
3     4             0
4     5             0
5     6             0
```

6	7	0
7	8	0
8	9	0
9	10	0

Telnet Command: adsl pvcbinding

This command can configure PVC to PVC binding. Such command is available only for PPPoE and MPoA 1483 Bridge mode.

`adsl pvcbinding [pvc_x pvc_y | status | -1]`

Syntax Description

Parameter	Description
<i>pvc_x</i>	The PVC number for the source.
<i>pvc_y</i>	The PVC number that the source PVC will be bound to.
<i>status</i>	Display a table for PVC binding group.
<i>-1</i>	It means to clear specific PVC binding.

Example

```
> adsl pvcbinding 3 5
set done. bind pvc3 to pvc5.
```

The above example means PVC3 has been bound to PVC5.

```
> adsl pvcbinding 3 -1
clear pvc-1 binding
```

The above example means the PVC3 binding group has been removed.

Telnet Command: adsl inventory

This command is used to display information about CO or CPE.

Syntax

`adsl inventory [co/cpe]`

Syntax Description

Parameter	Description
<i>co</i>	It means DSLAM (Digital Subscriber Line Access Multiplexer) or CO (Central Office).
<i>cpe</i>	It means CPE (Customer Premise Equipment).

Example

```
> adsl inventory co
xDSL inventory info only available in showtime.
> adsl inventory cpe
G.994 vendor ID           : 0XB5004946544E5444
  G.994.1 country code    : 0XB500
  G.994.1 provider code   : IFTN
  G.994.1 vendor info     : 0X5444
```

```

System vendor ID      : 0XB5004946544E0000
  System country code : 0XB500
  System provider code : IFTN
  System vendor info   : 0X000
Version number       : 3.8.2_RC4a_STD
Version number(16 octets) : 0X332E382E325F524334615F5354440000
Self-test result     : PASS
Transmission mode capability : 0X40004004C010400
>

```

Telnet Command: csm appe prof

Commands under CSM allow you to set CSM profile to define policy profiles for different policy of IM (Instant Messenger)/P2P (Peer to Peer) application.

“csm appe prof “ is used to configure the APP Enforcement Profile name. Such profile will be applied in Default Rule of Firewall>>General Setup for filtering.

Syntax

```
csm appe prof -i INDEX [-v | -n NAME|setdefault]
```

Syntax Description

Parameter	Description
<i>INDEX</i>	Specify the index number of CSM profile, from 1 to 32.
-v	View the configuration of the CSM profile.
-n	Set a name for the CSM profile.
<i>NAME</i>	Specify a name for the CSM profile, less then 15 characters.
<i>setdefault</i>	Reset to default settings.

Example

```

> csm appe prof -i 1 -n games
The name of APPE Profile 1 was setted.

```

Telnet Command: csm appe set

It is used to configure group settings for IM/P2P/Protocol and Others in APP Enforcement Profile.

Syntax

```
csm appe set -i INDEX [-v GROUP| -e AP_IDX | -d AP_IDX| -a AP_IDX [ACTION]]
```

Syntax Description

Parameter	Description
<i>INDEX</i>	Specify the index number of CSM profile, from 1 to 32.
-v	View the IM/P2P/Protocol and Others configuration of the CSM profile.
-e	Enable to block specific application.
-d	Disable to block specific application.
-a	Set the action of specific application
<i>GROUP</i>	Specify the category of the application. Available options are: IM,

	P2P, Protocol and Others.
<i>AP_IDX</i>	Each application has independent index number for identification in CLI command. Specify the index number of the application here. If you have no idea of the index number, do the following (Take IM as an example): Type "csm appe set -l 1 -v IM", the system will list all of the index numbers of the applications categorized under IM.
<i>ACTION</i>	Specify the action of the application, 0 or 1. 0: Block. All of the applications meet the CSM rule will be blocked. 1: Pass. All of the applications meet the CSM rule will be passed.

Example

```
>csm appe set -i 1 -a 1 1
Profile 1 - : <NULL> action set to Pass.
>
```

Telnet Command: csm appe show

It is used to display group (IM/P2P/Protocol and Others) information APP Enforcement Profile.

Syntax

csm appe show [-a|-i|-p|-t|-m]

Syntax Description

Parameter	Description
-a	View the configuration status for All groups.
-i	View the configuration status of IM group.
-p	View the configuration status of P2P group.
-t	View the configuration status of protocol group.
-m	View the configuration status of Others group.

Example

```
>csm appe show -t

      Type      Index      Name      Version  Advance
Advanced Option: (M)essage, (F)ile Transfer, (G)ame, (C)onference, and (O)ther
Activities
-----
PROTOCOL      52      DB2
PROTOCOL      53      DNS
PROTOCOL      54      FTP
PROTOCOL      55      HTTP      1.1
PROTOCOL      56      IMAP      4.1
PROTOCOL      57      IMAP STARTTLS 4.1
PROTOCOL      58      IRC      2.4.0      .....
```

Telnet Command: csm appe config

It is used to display the configuration status (enabled or disabled) for IM/P2P/Protocol/Other applications.

Syntax

`csm appe config -v INDEX [-i/-p/-t/-m]`

Syntax Description

Parameter	Description
<i>INDEX</i>	Specify the index number of CSM profile, from 1 to 32.
<i>-i</i>	View the configuration status of IM group.
<i>-p</i>	View the configuration status of P2P group.
<i>-t</i>	View the configuration status of protocol group.
<i>-m</i>	View the configuration status of Others group.

Example

```
> csm appe config -v 1 -m
Group      Type      Index      Name      Enable      A
vance Enable
Advance abbreviation: Message, File Transfer, Game, Conference, and Other
Advance abbreviation: : M, F, G, C, and O
-----
OTHERS     TUNNEL    75         DNSCrypt   Disable
OTHERS     TUNNEL    76         DynaPass   Disable
OTHERS     TUNNEL    77         FreeU      Disable
OTHERS     TUNNEL    78         HTTP Proxy Disable
OTHERS     TUNNEL    79         HTTP Tunnel Disable
OTHERS     TUNNEL    80         Hamachi    Disable
OTHERS     TUNNEL    81         Hotspot Shield Disable
OTHERS     TUNNEL    82         MS Teredo  Disable
OTHERS     TUNNEL    83         PGPNet     Disable
OTHERS     TUNNEL    84         Ping Tunnel Disable
.
.
.
-----
Total 66 APPs
>
```

Telnet Command: csm appe interface

It is used to configure APPE signature download interface.

Syntax

`csm appe interface [AUTO/WAN#]`

Syntax Description

Parameter	Description
<i>AUTO</i>	Vigor router specifies WAN interface automatically.
<i>WAN</i>	Specify the WAN interface for signature downloading.

Example

```
> csm appe interface wan1
Download interface is set as "WAN1" now.
> csm appe interface auto
Download interface is set as "auto-selected" now.
```

Telnet Command: csm appe email

It is used to set notification e-mail for APPE signature based on the settings configured in System Maintenance>>SysLog/Mail Alert Setup (in which, the box of APPE Signature is checked under Enable E-Mail Alert).

Syntax

```
csm appe email [-e/-d/-s]
```

Syntax Description

Parameter	Description
-e	Enable notification e-mail mechanism.
-d	Disable notification e-mail mechanism.
-s	Send an example e-mail.

Example

```
> csm appe email -e
Enable APPE email.
```

Telnet Command: csm ucf

It is used to configure settings for URL control filter profile.

```
csm ucf show
```

```
csm ucf setdefault
```

```
csm ucf msg MSG
```

```
csm ucf obj INDEX [-n PROFILE_NAME | -I [P/B/A/N] | uac | wf ]
```

```
csm ucf obj INDEX -n PROFILE_NAME
```

```
csm ucf obj INDEX -p VALUE
```

```
csm ucf obj INDEX -I P/B/A/N
```

```
csm ucf obj INDEX uac
```

```
csm ucf obj INDEX wf
```

Syntax Description

Parameter	Description
<i>show</i>	Display all of the profiles.
<i>setdefault</i>	Return to default settings for all of the profile.
<i>msg MSG</i>	Set the administration message. MSG means the content (less than 255 characters) of the message itself.
<i>obj</i>	Specify the object for the profile.
<i>INDEX</i>	Specify the index number of CSM profile, from 1 to 8.
<i>-n</i>	Set the profile name.
<i>PROFILE_NAME</i>	Specify the name of the profile (less than 16 characters)
<i>-p</i>	Set the priority (defined by the number specified in VALUE) for the profile.
<i>VALUE</i>	Number 0 to 3 represent different conditions.

	0: It means Bundle: Pass. 1: It means Bundle: Block. 2: It means Either: URL Access Control First. 3: It means Either: Web Feature First.
<i>-l</i>	It means the log type of the profile. They are: P: Pass, B: Block, A: All, N: None
<i>MSG</i>	Specify the Administration Message, less than 255 characters
<i>uac</i>	Set URL Access Control part.
<i>wf</i>	Set Web Feature part.

Example

```
> csm ucf obj 1 -n game -l B
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
Action:[pass]
[ ]Prevent web access from IP address.
No Obj NO.    Object Name
-----
No Grp NO.    Group Name
-----
```

Telnet Command: csm ucf obj INDEX uac

It means to configure the settings regarding to URL Access Control (uac).

csm ucf obj *INDEX* uac -v

csm ucf obj *INDEX* uac -e

csm ucf obj *INDEX* uac -d

csm ucf obj *INDEX* uac -a P|B

csm ucf obj *INDEX* uac -i E|D

csm ucf obj *INDEX* uac -o *KEY_WORD_Object_Index*

csm ucf obj *INDEX* uac -g *KEY_WORD_Group_Index*

Syntax Description

Parameter	Description
<i>INDEX</i>	Specify the index number of CSM profile, from 1 to 8.
-v	View the protocol configuration of the CSM profile.
-e	Enable the function of URL Access Control.
-d	Disable the function of URL Access Control.

<i>-a</i>	Set the action of specific application, P or B. B: Block. The web access meets the URL Access Control will be blocked. P: Pass. The web access meets the URL Access Control will be passed.
<i>-i</i>	Prevent the web access from any IP address. E: Enable the function. The Internet access from any IP address will be blocked. D: Disable the function.
<i>-o</i>	Set the keyword object.
<i>KEY_WORD_Object_Index</i>	Specify the index number of the object profile.
<i>-g</i>	Set the keyword group.
<i>KEY_WORD_Group_Index</i>	Specify the index number of the group profile.

Example

```

> csm ucf obj 1 uac -i E
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
Action:[pass]
[v]Prevent web access from IP address.
  No  Obj NO.   Object Name
-----
  No  Grp NO.   Group Name
-----

> csm ucf obj 1 uac -a B
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
Action:[block]
[v]Prevent web access from IP address.
  No  Obj NO.   Object Name
-----
  No  Grp NO.   Group Name
-----

```

Telnet Command: csm ucf obj INDEX wf

It means to configure the settings regarding to Web Feature (wf).

csm ucf obj *INDEX wf -v*

csm ucf obj *INDEX wf -e*

csm ucf obj *INDEX wf -d*

csm ucf obj *INDEX wf -a P/B*

csm ucf obj *INDEX wf -s WEB_FEATURE*

csm ucf obj *INDEX wf -u WEB_FEATURE*

csm ucf obj *INDEX wf -f File_Extension_Object_index*

Syntax Description

Parameter	Description
<i>INDEX</i>	Specify the index number of CSM profile, from 1 to 8.
<i>-v</i>	View the protocol configuration of the CSM profile.
<i>-e</i>	Enable the restriction of web feature.
<i>-d</i>	Disable the restriction of web feature.
<i>-a</i>	Set the action of web feature, P or B. B: Block. The web access meets the web feature will be blocked. P: Pass. The web access meets the web feature will be passed.
<i>-s</i>	Enable the the Web Feature configuration. Features available for configuration are: c: Cookie p: Proxy u: Upload
<i>-u</i>	Cancel the web feature configuration.
<i>-f</i>	Set the file extension object index number.
<i>File_Extension_Object_index</i>	Enter the index number (1 to 8) for the file extension object.

Example

```
> csm ucf obj 1 wf -s c
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
Action:[block]
[v] Prevent web access from IP address.
No Obj NO.    Object Name
-----

No Grp NO.    Group Name
-----

[ ]Enable Restrict Web Feature
Action:[pass]
```

File Extension Object Index : [0]	Profile Name : []
[V] Cookie [] Proxy [] Upload	

Telnet Command: csm wcf

It means to configure the settings regarding to web control filter (wcf).

csm wcf show

csm wcf look

csm wcf cache

csm wcf server WCF_SERVER

csm wcf msg MSG

csm wcf setdefault

csm wcf obj *INDEX* -v

csm wcf obj *INDEX* -a P/B

csm wcf obj *INDEX* -n *PROFILE_NAME*

csm wcf obj *INDEX* -I N/P/B/A

csm wcf obj *INDEX* -o *KEY_WORD* Object Index

csm wcf obj *INDEX* -g *KEY_WORD* Group Index

csm wcf obj *INDEX* -w E/D/P/B

csm wcf obj *INDEX* -s *CATEGORY*/*WEB_GROUP*

csm wcf obj *INDEX* -u *CATEGORY*/*WEB_GROUP*

Syntax Description

Parameter	Description
<i>show</i>	Display the web content filter profiles.
<i>Look</i>	Display the license information of WCF.
<i>Cache</i>	Set the cache level for the profile.
<i>Server WCF_SERVER</i>	Set web content filter server.
<i>Msg MSG</i>	Set the administration message. MSG means the content (less than 255 characters) of the message itself.
<i>setdefault</i>	Return to default settings for all of the profile.
<i>obj</i>	Specify the object profile.
<i>INDEX</i>	Specify the index number of web content filter profile, from 1 to 8.
- v	View the web content filter profile.
-a	Set the action of web content filter profile, P or B. B: Block. The web access meets the web feature will be blocked. P: Pass. The web access meets the web feature will be passed.
-n	Set the profile name.
<i>PROFILE_NAME</i>	Specify the name of the profile (less than 16 characters)
-I	It means the log type of the profile. They are: P: Pass, B: Block, A: All, N: None
-o	Set the keyword object.

<i>KEY_WORD_Object_Index</i>	Specify the index number of the object profile.
<i>-g</i>	Set the keyword group.
<i>KEY_WORD_Group_Index</i>	Specify the index number of the group profile.
<i>-w</i>	Set the action for the black and white list. E:Enable, D:Disable, P:Pass, B:Block
<i>-s</i>	It means to choose the items under CATEGORY or WEB_GROUP.
<i>-u</i>	It means to discard items under CATEGORY or WEB_GROUP.
WEB_GROUP	Child_Protection, Leisure, Business, Chating, Computer Internet, Other
CATEGORY	Includes: Alcohol & Tobacco, Criminal Activity, Gambling, Hate & Intoleranc, Illegal Drug, Nudity, Pornography/Sexually Explicit, Weapons, Violence, School Cheating,Sex Education, Tasteless, Child Abuse Imges, Entertainment, Games, Sports, Travel, Leisure & Recreation, Fashin & Beauty, Business, Job Search, Web-based Emai, Chat, Instant Messaging, Anonymizers, Forums & Newsgroups, Computers & Technology, Download Sites, Streaming Media & Downloads, Phishing & Fraud, Search Engines & Portals, Social Networking, Spam Sites,Malware, Botnets, Hacking, Illegal Software, Information Security,Peer-to-eer, Advertisements & Pop-Ups, Arts, Transportation, Compromised, Dating & Personals, , Education, Finance, Government,Health & Medcine, News, Non-profits & NGOs, Personal Sites,Politics, Real Estate, Rligion, Restaurants & Dining,Shopping, Translators, General, Cults,Greetig cards, Image Sharing, Network Errors, Parked Domains, Private IP Addresses)

Example

```
> csm wcf obj 1 -n test_wcf
Profile Index: 1
Profile Name:[test_wcf]
[ ]White/Black list
Action:[block]
  No  Obj NO.   Object Name
  ---  ---
  No  Grp NO.   Group Name
  ---  ---

Action:[block]
Log:[block]

-----

child Protection Group:
  [v]Alcohol & Tobacco      [v]Criminal & Activity   [v]Gambling
  [v]Hate & Intolerance     [v]Illegal Drug         [v]Nudity
  [v]Pornography & Sexually explicit [v]Violence
  [v]Weapons

  [v]School Cheating       [v]Sex Education        [v]Tasteless
  [v]Child Abuse Images

-----

leisure Group:
  [ ]Entertainment          [ ]Games                 [ ]Sports
  [ ]Travel                 [ ]Leisure & Recreation [ ]Fashion & Beauty
.
.
>
```

Telnet Command: csm dnsf

It means to configure the settings regarding to DNS filter.

```
csm dnsf enable ON/OFF
csm dnsf syslog N/P/B/A
csm dnsf service WCF_PROFILE
csm dnsf service_ucf UCF_PROFILE
csm dnsf time CACHE_TIME
csm dnsf blockpage show/on/off
csm dnsf profile_show
csm dnsf profile_edit INDEX
csm dnsf profile_edit INDEX -n PROFILE_NAME
csm dnsf profile_edit INDEX -l N/P/B/A
csm dnsf profile_edit INDEX -w WCF_PROFILE
csm dnsf profile_edit INDEX -u UCF_PROFILE
csm dnsf profile_edit INDEX -c CACHE_TIME
```

Syntax Description

Parameter	Description
<i>enable</i>	Enable or disable DNS Filter. ON: enable. OFF: disable.
<i>syslog</i>	Determine the content of records transmitting to Syslog. P: Pass. Records for the packets passing through DNS filter will be sent to Syslog. B: Block. Records for the packets blocked by DNS filter will be sent to Syslog. A: All. Records for the packets passing through or blocked by DNS filter will be sent to Syslog. N: None. No record will be sent to Syslog.
<i>service WCF_PROFILE</i>	WCF_PROFILE: Specify a WCF profile as the base of DNS filtering. Type a number to indicate the index number of WCF profile (1 is first profile, 2 is second profile, and so on ...).
<i>time CACHE_TIME</i>	CACHE_TIME: It means to set the time for cache to live (available values are 1 to 24; 1 is one hour, 2 is two hours, and so on ...) for DNS filter.
<i>blockpage</i>	DNS sends block page for redirect port. When a web page is blocked by DNS filter, the router system will send a message page to describe that the page is not allowed to be visited. ON: Enable the function of displaying message page. OFF: Disable the function of displaying message page. SHOW: Display the function of displaying message page is ON or OFF.
<i>profile_show</i>	Display the table of the DNS filter profile.
<i>profile_edit</i>	Modify the content of the DNS filter profile.
<i>-n PROFILE_NAME</i>	PROFILE_NAME: Enter the name of the DNS filter profile that you want to modify.
<i>-l N P B A</i>	Specify the log type of the profile. P: Pass. B: Block. A: All. N: None.
<i>-w WCF_PROFILE</i>	WCF_PROFILE: Enter the index number of the WCF profile.
<i>-u UCF_PROFILE</i>	UCF_PROFILE: Enter the index number of the UCF profile.
<i>-c CACHE_TIME</i>	-c means to set the cache time for DNS filter. CACHE_TIME: It means to set the time for cache to live (available values are 1 to 24; 1 is one hour, 2 is two hours, and so on ...) for DNS filter.

Example

```
> csm dnsf service 2
dns service set up!!!
>csm dnsf service 3
wcf profile 3 is empty.....
>csm dnsf cachetime 1
dns cache time set up!!!
```

Telnet Command: ddns log

Displays the DDNS log.

Example

```
>ddns log
>
```

Telnet Command: ddns time

Sets and displays the DDNS time.

`ddns time <update in minutes>`

Syntax Description

Parameter	Description
<i>Update in minutes</i>	Enter the value as DDNS time. The range is from 1 to 14400.

Example

```
> ddns time
ddns time <update in minutes>
Valid: 1 ~ 14400
%Now: 14400
> ddns time 1000
ddns time <update in minutes>
Valid: 1 ~ 14400
%Now: 1000
```

Telnet Command: dos

This command allows users to configure the settings for DoS defense system.

`dos [-V | D | A]`

`dos [-s ATTACK_F [THRESHOLD][TIMEOUT]]`

`dos [-a | e [ATTACK_F][ATTACK_0] | d [ATTACK_F][ATTACK_0]]`

Syntax Description

Parameter	Description
<i>-V</i>	View the configuration of DoS defense system.
<i>-D</i>	Deactivate the DoS defense system.
<i>-A</i>	Activate the DoS defense system.
<i>-s</i>	Enable the defense function for a specific attack and set its parameter(s).
<i>ATTACK_F</i>	Specify the name of flooding attack(s) or portscan, e.g., synflood, udpflood, icmpflood, or postscan.
<i>THRESHOLD</i>	It means the packet rate (packet/second) that a flooding attack will be detected. Set a value larger than 20.
<i>TIMEOUT</i>	It means the time (seconds) that a flooding attack will be blocked. Set a value larger than 5.
<i>-a</i>	Enable the defense function for all attacks listed in ATTACK_0.

-e	Enable defense function for a specific attack(s).
ATTACK_0	Specify a name of the following attacks: ip_option, tcp_flag, land, teardrop, smurf, pingofdeath, traceroute, icmp_frag, syn_frag, unknow_proto, fraggle.
-d	Disable the defense function for a specific attack(s).

Example

```
>dos -A
The Dos Defense system is Activated
>dos -s synflood 50 10
Synflood is enabled! Threshold=50 <pke/sec> timeout=10 <pke/sec>
```

Telnet Command: exit

Type this command will leave telnet window.

Telnet Command: Internet

This command allows you to configure detailed settings for WAN connection.

Syntax

internet -W n -M n [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
-W n	W means to set WAN interface. 1=WAN1, 2=WAN2,.... Default is WAN1.
-M n	M means to set Internet Access Mode (Mandatory) and n means different modes (represented by 0 - 3) n=0: Offline n=1: PPPoE n=2: Dynamic IP n=3: Static IP n=4: PPTP with Dynamic IP, n=5: PPTP with Static IP, n=6: L2TP with Dynamic IP n=7: L2TP with Static IP n=A: 3G/4G USB Modem(PPP mode), n=B: 3G/4G USB Modem(DHCP mode)
<command><parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-S <isp name>	Set ISP Name (max. 23 characters).
-P <on/off>	Enable PPPoE Service.
-u <username>	Set username (max. 49 characters) for Internet accessing.
-p <password>	Set password (max. 49 characters) for Internet accessing.
-a n	It means to set PPP Authentication Type and n means different types (represented by 0-1). n=0: PAP/CHAP (this is default setting) n=1: PAP Only
-t n	Set connection duration and n means different conditions. n=-1: Always-on

	n=1 - 999: Idle time for offline (default 180 seconds)
-i <ip address>	It means that PPPoE server will assign an IP address specified here for CPE (PPPoE client). If you type 0.0.0.0 as the <ip address>, ISP will assign suitable IP address for you. However, if you type an IP address here, the router will use that one as a fixed IP.
-w <ip address>	It means to assign WAN IP address for such connection. Please type an IP address here for WAN port.
-n <netmask>	It means to assign netmask for WAN connection. You have to type 255.255.255.xxx (x is changeable) as the netmask for WAN port.
-g <gateway>	Assign gateway IP for such WAN connection.
-V	View Internet Access profile.
-C <sim pin code>	Set (PPP mode) SIM PIN code (max. 15 characters).
-O <init string>	Set (PPP mode) Modem Initial String (max. 47 characters).
-T <init string2>	Set (PPP mode) Modem Initial String2 (max. 47 characters)
-D <dial string>	Set (PPP mode) Modem Dial String (max. 31 characters).
-v <service name>	Set (PPP mode) Service Name (max. 23 characters).
-m <ppp username>	Set (PPP mode) PPP Username (max. 63 characters).
-o <ppp password>	Set (PPP mode) PPP Password (max. 62 characters).
-e n	Set (PPP mode) PPP Authentication Type. n= 0: PAP/CHAP (default), 1: PAP Only
-q n	(PPP mode) Index(1-15) in Schedule Setup-One
-x n	(PPP mode) Index(1-15) in Schedule Setup-Two
-y n	(PPP mode) Index(1-15) in Schedule Setup-Three
-z n	(PPP mode) Index(1-15) in Schedule Setup-Four
-Q <mode>	Set (PPP mode or DHCP mode) WAN Connection Detection Mode. <mode> 0: ARP Detect; 1: Ping Detect
-I <ping ip>	Set (PPP mode or DHCP mode) WAN Connection Detection Ping IP. <ping ip>= ppp.qqq.rrr.sss: WAN Connection Detection Ping IP
-L n	Set (PPP mode) WAN Connection Detection TTL (1-255) value.
-E <sim pin code>	Set (DHCP mode) SIM PIN code (max. 19 characters).
-G <mode>	Set (DHCP mode) Network Mode. <mode> 0: 4G/3G/2G; 1: 4G Only; 2: 3G Only; 3: 2G Only
-N <apn name>	Set (DHCP mode) APN Name (max. 47 characters)
-U n	(DHCP mode) MTU(1000-1440)

Example

```
>internet -M 1 -S tcom -u username -p password -a 0 -t -1 -i 0.0.0.0
WAN1 Internet Mode set to PPPoE/PPPoA
```

```

WAN1 ISP Name set to tcom
WAN1 Username set to username
WAN1 Password set successful
WAN1 PPP Authentication Type set to PAP/CHAP
WAN1 Idle timeout set to always-on
WAN1 Gateway IP set to 0.0.0.0
> internet -V
WAN1 Internet Mode:PPPoE
ISP Name: tcom
Username: username
Authentication: PAP/CHAP
Idle Timeout: -1
WAN IP: Dynamic IP
> internet -W 1 -M 1 -u link1 -p link1 -a 0
You are going to watching and setting in WAN 1
WAN1 Internet Mode set to PPPoE/PPPoA
WAN1 Username set to link1
WAN1 Password set successful
WAN1 PPP Authentication Type set to PAP/CHAP
>

```

Telnet Command: ip pubsubnet

This command allows users to enable or disable the IP routing subnet for your router.

Syntax

ip pubsubnet <Enable/Disable>

Syntax Description

Parameter	Description
<i>Enable</i>	Enable the function.
<i>Disable</i>	Disable the function.

Example

```

> ip 2ndsubnet enable
public subnet enabled!

```

Telnet Command: ip pubaddr

This command allows to set the IP routed subnet for the router.

Syntax

ip pubaddr ?

ip pubaddr <public subnet IP address>

Syntax Description

Parameter	Description
<i>?</i>	Display an IP address which allows users set as the public subnet IP address.
<i>public subnet IP address</i>	Specify an IP address. The system will set the one that you specified

as the public subnet IP address.

Example

```
> ip pubaddr ?
% ip addr <public subnet IP address>
% Now: 192.168.0.1

> ip pubaddr 192.168.2.5
% Set public subnet IP address done !!!
```

Telnet Command: ip pubmask

This command allows users to set the mask for IP routed subnet of your router.

Syntax

```
ip pubmask ?
ip pubmask <public subnet mask>
```

Syntax Description

Parameter	Description
<i>?</i>	Display an IP address which allows users set as the public subnet mask.
<i>public subnet IP address</i>	Specify a subnet mask. The system will set the one that you specified as the public subnet mask.

Example

```
> ip pubmask ?
% ip pubmask <public subnet mask>
% Now: 255.255.255.0

> ip pubmask 255.255.0.0
% Set public subnet mask done !!!
```

Telnet Command: ip aux

This command is used for configuring WAN IP Alias.

Syntax

```
ip aux add [IP] [Join to NAT Pool][wanX]
ip aux remove [index]
```

Syntax Description

Parameter	Description
<i>add</i>	Create a new WAN IP address.
<i>remove</i>	Delete an existed WAN IP address.
<i>IP</i>	It means the auxiliary WAN IP address.
<i>Join to NAT Pool</i>	0 (disable) or 1 (enable).
<i>wanX</i>	Add or remove an address for WAN interface.
<i>index</i>	Enter the index number of the table displayed on your screen.

Example

```
> ip aux add 192.168.1.65 1
% 192.168.1.65 has added in index 3.
```

When you type *ip aux?*, the current auxiliary WAN IP Address table will be shown as the following:

Index no.	Status	IP address	IP pool
1	Enable	172.16.3.229	Yes
2	Enable	172.16.3.56	No
3	Enable	172.16.3.113	No

Telnet Command: ip addr

This command allows users to set/add a specified LAN IP your router.

Syntax

`ip addr [IP address]`

Syntax Description

Parameter	Description
<i>IP address</i>	The LAN IP address.

Example

```
>ip addr 192.168.50.1
% Set IP address OK !!!
```



Info

When the LAN IP address is changed, the start IP address of DHCP server are still the same. To make the IP assignment of the DHCP server being consistent with this new IP address (they should be in the same network segment), the IP address of the PC must be fixed with the same LAN IP address (network segment) set by this command for accessing into the web user interface of the router. Later, modify the start addresses for the DHCP server.

Telnet Command: ip nmask

This command allows users to set/add a specified netmask for your router.

Syntax

`ip nmask [IP netmask]`

Syntax Description

Parameter	Description
<i>IP netmask</i>	The netmask of LAN IP.

Example


```
> ip netmask 255.255.0.0
% Set IP netmask OK !!!
```

Telnet Command: ip arp

ARP displays the matching condition for IP and MAC address.

Syntax

```
ip arp add [IP address] [MAC address] [LAN or WAN]
```

```
ip arp del [IP address] [LAN or WAN]
```

```
ip arp flush
```

```
ip arp status
```

```
ip arp accept [0/1/2/3/4/5status]
```

```
ip arp setCacheLife [time]
```

In which, arp add allows users to add a new IP address into the ARP table; arp del allows users to remove an IP address; arp flush allows users to clear arp cache; arp status allows users to review current status for the arp table; arp accept allows to accept or reject the source /destination MAC address; arp setCacheLife allows users to configure the duration in which ARP caches can be stored on the system. If ip arp setCacheLife is set with “60”, it means you have an ARP cache at 0 second. Sixty seconds later without any ARP messages received, the system will think such ARP cache is expired. The system will issue a few ARP request to see if this cache is still valid.

Syntax Description

Parameter	Description
<i>IP address</i>	It means the LAN IP address.
<i>MAC address</i>	It means the MAC address of your router.
<i>LAN or WAN</i>	It indicates the direction for the arp function.
<i>0/1/2/3/4/5</i>	0: disable to accept illegal source mac address 1: enable to accept illegal source mac address 2: disable to accept illegal dest mac address 3: enable to accept illegal dest mac address 4: Decline VRRP mac into arp table 5: Accept VRRP mac into arp table status: display the setting status.
<i>Time</i>	Available settings will be 10, 20, 30,...2550 seconds.

Example

```
> ip arp status
[ARP Table]
  Index IP Address      MAC Address           Netbios Name   Interface  VLAN
  Port
   1   192.168.1.5      00-05-5D-E4-D8-EE
VLAN0  P1
>
```

Telnet Command: ip dhcpc

This command is available for WAN DHCP.

Syntax

`ip dhcpc option`

`ip dhcpc option -h/l`

`ip dhcpc option -d [idx]`

`ip dhcpc option -e [1 or 0] -w [wan unumber] -c [option number] -v [option value]`

`ip dhcpc option -e [1 or 0] -w [wan unumber] -c [option number] -x "[option value]"`

`ip dhcpc option -e [1 or 0] -w [wan unumber] -c [option number] -a [option value]`

`ip dhcpc option -u [idx unumber]`

`ip dhcpc release [wan number]`

`ip dhcpc renew [wan number]`

`ip dhcpc status`

Syntax Description

Parameter	Description
<i>option</i>	It is an optional setting for DHCP server. -h: display usage -l: list all custom set DHCP options -d: delete custom dhcp client option by index number -e: enable/disable option feature, 1:enable, 0:disable -w: set WAN number (e.g., 1=WAN1) -c: set option number: 0-255 -v: set option value by string -x: set option value by raw byte (hex) -u: update by index number
<i>release</i>	It means to release current WAN IP address.
<i>renew</i>	It means to renew the WAN IP address and obtain another new one.
<i>status</i>	It displays current status of DHCP client.

Example

```
>ip dhcpc status
I/F#3 DHCP Client Status:

DHCP Server IP      : 172.16.3.7
WAN Ipm             : 172.16.3.40
WAN Netmask         : 255.255.255.0
WAN Gateway         : 172.16.3.1
Primary DNS         : 168.95.192.1
Secondary DNS       : 0.0.0.0
Leased Time         : 259200
Leased Time T1      : 129600
Leased Time T2      : 226800
Leased Elapsed      : 259194
Leased Elapsed T1   : 129594
```

```
Leased Elapsed T2 : 226794
```

Telnet Command: ip ping

This command allows users to ping IP address of WAN1/WAN2 for verifying if the WAN connection is OK or not.

Syntax

```
ip ping [IP address] [WAN1/WAN2]
```

Syntax Description

Parameter	Description
<i>IP address</i>	It means the WAN IP address.
<i>WAN1/WAN2</i>	It means the WAN interface that the above IP address passes through.

Example

```
>ip ping 172.16.3.229 WAN1
Pinging 172.16.3.229 with 64 bytes of Data:
Receive reply from 172.16.3.229, time=0ms
Receive reply from 172.16.3.229, time=0ms
Receive reply from 172.16.3.229, time=0ms
Packets: Sent = 5, Received = 5, Lost = 0 <0% loss>
```

Telnet Command: ip tracert

This command allows users to trace the routes from the router to the host.

```
ip tracert [Host/IP address] [WAN1/WAN2/WAN3/WAN4/WAN5] [Udp/Icmp]
```

Syntax Description

Parameter	Description
<i>IP address</i>	The target IP address.
<i>WAN1/WAN2</i>	It means the WAN port that the above IP address passes through.
<i>Udp/Icmp</i>	The UDP or ICMP.

Example

```
>ip tracert 22.128.2.62 WAN1
Traceroute to 22.128.2.62, 30 hops max
 1  172.16.3.7  10ms
 2  172.16.1.2  10ms
 3  Request Time out.
 4  168.95.90.6650ms
 5  211.22.38.134  50ms
 6  220.128.2.6250ms
Trace complete
```

Telnet Command: ip telnet

This command allows users to access specified device by telnet.

Syntax

ip telnet [*IP address*][*Port*]

Syntax Description

Parameter	Description
<i>IP address</i>	Enter the WAN or LAN IP address of the remote device.
<i>Port</i>	Type a port number (e.g., 23). Available settings: 0 -65535.

Example

```
> ip telnet 172.17.3.252 23
>
```

Telnet Command: ip rip

This command allows users to set the RIP (routing information protocol) of IP.

Syntax

ip rip [*0/1/2*]

Syntax Description

Parameter	Description
<i>0/1/2</i>	0 means disable; 1 means LAN1 and 2 means IP Routed.

Example

```
> ip rip 1
%% Set RIP LAN1.
```

Telnet Command: ip wanrip

This command allows users to set the RIP (routing information protocol) of WAN IP.

Syntax

ip wanrip [*ifno*] -e [*0/1*]

Syntax Description

Parameter	Description
<i>ifno</i>	It means the connection interface. 1: WAN1,2: WAN2, 3: PVC3,4: PVC4,5: PVC5 Note: PVC3 -PVC5 are virtual WANs.
-e	It means to disable or enable RIP setting for specified WAN interface. 1: Enable the function of setting RIP of WAN IP. 0: Disable the function.

Example

```

> ip wanrip ?
Valid ex:ip wanrip <ifno> -e <0/1>
<ifno> 1: WAN1,2: WAN2
       3: PVC3,4: PVC4,5: PVC5
-e <0/1> 0: disable, 1: enable
Now status:
WAN[1] Rip Protocol disable
WAN[2] Rip Protocol disable
WAN[3] Rip Protocol disable
WAN[4] Rip Protocol disable
WAN[5] Rip Protocol disable
> ip wanrip 5 -e 1
> ip wanrip ?
Valid ex:ip wanrip <ifno> -e <0/1>
<ifno> 1: WAN1,2: WAN2
       3: PVC3,4: PVC4,5: PVC5
-e <0/1> 0: disable, 1: enable
Now status:
WAN[1] Rip Protocol disable
WAN[2] Rip Protocol disable
WAN[3] Rip Protocol disable
WAN[4] Rip Protocol disable
WAN[5] Rip Protocol enable
>

```

Telnet Command: ip route

This command allows users to set static route.

Syntax

ip route add [dst] [netmask][gateway][ifno][rtype]

ip route del [dst] [netmask][rtype]

ip route status

ip route cnc

ip route default [wan1/wan2/off/?]

ip route clean [1/0]

Syntax Description

Parameter	Description
<i>add</i>	It means to add an IP address as static route.
<i>del</i>	It means to delete specified IP address.
<i>status</i>	It means current status of static route.
<i>dst</i>	It means the IP address of the destination.
<i>netmask</i>	It means the netmask of the specified IP address.
<i>gateway</i>	It means the gateway of the connected router.
<i>ifno</i>	It means the connection interface. 3=WAN1, 4=WAN2, 5=WAN3, 6=WAN4

<i>rtype</i>	It means the type of the route. default : default route; static: static route.
cnc	It means current IP range for CNC Network.
default	Set WAN1/WAN2/off as current default route.
clean	Clean all of the route settings. 1: Enable the function. 0: Disable the function.

Example

```
> ip route add 172.16.2.0 255.255.255.0 172.16.2.4 3 static
> ip route status

Codes: C - connected, S - static, R - RIP, * - default, ~ - private
C~    192.168.9.0/    255.255.255.0 is directly connected, DMZ
C~    192.168.1.0/    255.255.255.0 is directly connected, LAN1
S     172.16.2.0/    255.255.255.0 via 172.16.2.4, WAN1
```

Telnet Command: ip igmp_proxy

This command allows users to enable/disable igmp proxy server.

Syntax

`ip igmp_proxy set`

`ip igmp_proxy reset`

`ip igmp_proxy wan`

`ip igmp_proxy query`

`ip igmp_proxy ppp [0/1]`

`ip igmp_proxy status`

Syntax Description

Parameter	Description
<i>set</i>	It means to enable proxy server.
<i>reset</i>	It means to disable proxy server.
<i>wan</i>	It means to specify WAN interface for IGMP service.
<i>query</i>	It means to set IGMP general query interval. The default value is 125000 ms.
<i>ppp</i>	0 - No need to set IGMP with PPP header. 1 - Set IGMP with PPP header.
<i>status</i>	It means to display current status for proxy server.

Example

```
This command is for setting IGMP General Query Interval
The default value is 125000 ms
Current Setting is:130000 ms
> ip igmp_proxy set
% ip igmp_proxy [set|reset|wan|status], IGMP Proxy is ON
> ip igmp_proxy status
%% ip igmp_proxy [set|reset|wan|status], IGMP Proxy is ON
%%% igmp_proxy WAN:
    239.255.255.250    state=1
    239.255.255.250    timer=0
```

Telnet Command: ip igmp_snoop

This command is used to enable/disable igmp snoop server.

Syntax

```
ip igmp_snoop enable
ip igmp_snoop disable
ip igmp_snoop status
ip igmp_snoop txquery [on/off] [v2/v3]
ip igmp_snoop chkleave [on/off]
ip igmp_snoop separate [on/off]
```

Syntax Description

Parameter	Description
<i>enable</i>	It means to enable proxy server.
<i>disable</i>	It means to disable proxy server.
<i>status</i>	It means to display current status for proxy server.
<i>table</i>	Display the whole table of IGMP Snoop configuration.
<i>txquery [on/off] [v2/v3]</i>	IGMP query will be sent out to LAN periodically.
<i>mode [hw/sw]</i>	Make IGMP snooping work on software or hardware.
<i>chkleave [on/off]</i>	Off - Vigor router will drop LEAVE if clients still on the same group.
<i>separate [on/off]</i>	On - IGMP packets will be separated by NAT/Bridge mode.

Example

```
> ip igmp_snoop enable
% ip igmp snooping [enable|disable|status], IGMP Snooping is Enabled.
>
```

Telnet Command: ip igmp_fl

This command is used to enable/disable igmp fast leave.

Syntax

```
ip igmp_fl enable
ip igmp_fl disable
ip igmp_fl status
```

Syntax Description

Parameter	Description
<i>enable</i>	Enable IGMP fast leave.
<i>disable</i>	Disable IGMP fast leave.
<i>status</i>	Display current status of IGMP Fast Leave.

Example


```

> ip igmp_fl enable
%% ip igmp_fl [enable|disable|status], IGMP Fast Leave is Enabled.
>

```

Telnet Command: ip dmz

Specify MAC address of certain device as the DMZ host.

Syntax

ip dmz *[mac]*

Syntax Description

Parameter	Description
<i>mac</i>	It means the MAC address of the device that you want to specify.

Example

```

>ip dmz ?
% ip dmz <mac>, now : 00-00-00-00-00-00
> ip dmz 11-22-33-44-55-66
> ip dmz ?
% ip dmz <mac>, now : 11-22-33-44-55-66
>

```

Telnet Command: ip dmzswitch

This command is to enable /disable private IP DMZ or Active True IP DMZ for DMZ host.

Syntax

ip dmzswitch *off*

ip dmzswitch *private*

ip dmaswitch *active_trueip*

Syntax Description

Parameter	Description
<i>off</i>	Disable the function of DMZ host.
<i>private</i>	Enable private IP address of the DMZ host.
<i>Active_trueip</i>	Enable active true IP address of the DMZ host.

Example

```

> ip dmzswitch ?
%% ip dmzswitch [off|private|active_trueip], DMZ is OFF
> ip dmzswitch private
%% ip dmzswitch [off|private|trueip|active_trueip], PRIVATE IP DMZ is ON
> ip dmzswitch trueip
> ip dmzswitch active_trueip
%% ip dmzswitch [off|private|trueip|active_trueip], ACTIVE TRUE IP DMZ is ON

```

Telnet Command: ip session

This command allows users to set maximum session limit number for the specified IP; set message for exceeding session limit and set how many seconds the IP session block works.

`ip session on`

`ip session off`

`ip session default [num]`

`ip session defaultp2p [num]`

`ip session status`

`ip session show`

`ip session timer [num]`

`ip session [block/unblock][IP]`

`ip session [add/del][IP1-IP2][num][p2pnum]`

Syntax Description

Parameter	Description
<i>on</i>	Turn on session limit for each IP.
<i>off</i>	Turn off session limit for each IP.
<i>default [num]</i>	Set the default number of session num limit.
<i>Defaultp2p [num]</i>	Set the default number of session num limit for p2p.
<i>status</i>	Display the current settings.
<i>show</i>	Display all session limit settings in the IP range.
<i>timer [num]</i>	Set when the IP session block works. The unit is second.
<i>[block/unblock][IP]</i>	Block/unblock the specified IP address. Block: The IP cannot access Internet through the router. Unblock: The specified IP can access Internet through the router.
<i>add</i>	Add the session limits in an IP range.
<i>del</i>	Delete the session limits in an IP range.
<i>IP1-IP2</i>	It means the range of IP address specified for this command.
<i>num</i>	It means the number of the session limits, e.g., 100.
<i>p2pnum</i>	It means the number of the session limits, e.g., 50 for P2P.

Example

```
>ip session default 100
> ip session add 192.168.1.5-192.168.1.100 100 50
> ip session on
> ip session status

IP range:
  192.168.1.5 - 192.168.1.100 : 100
Current ip session limit is turn on

Current default session number is 100
```

Telnet Command: ip bandwidth

This command allows users to set maximum bandwidth limit number for the specified IP.

`ip bandwidth on`

`ip bandwidth off`

`ip bandwidth default [tx_rate][rx_rate]`

`ip bandwidth status`

`ip bandwidth show`

`ip bandwidth [add/del] [IP1-IP2][tx][rx][shared]`

Syntax Description

Parameter	Description
<code>on</code>	Turn on the IP bandwidth limit.
<code>off</code>	Turn off the IP bandwidth limit.
<code>default [tx_rate][rx_rate]</code>	Set default tx and rx rate of bandwidth limit. The range is from 0 - 65535 Kpbs.
<code>status</code>	Display the current settings.
<code>show</code>	Display all the bandwidth limits settings within the IP range.
<code>add</code>	Add the bandwidth within the IP range.
<code>del</code>	Delete the bandwidth within the IP range.
<code>IP1-IP2</code>	It means the range of IP address specified for this command.
<code>tx</code>	Set transmission rate for bandwidth limit.
<code>rx</code>	Set receiving rate for bandwidth limit.
<code>shared</code>	It means that the bandwidth will be shared for the IP range.

Example

```
> ip bandwidth default 200 800
> ip bandwidth add 192.168.1.50-192.168.1.100 10 60
> ip bandwidth status

IP range:
 192.168.1.50 - 192.168.1.100 : Tx:10K Rx:60K

Current ip Bandwidth limit is turn off

Auto adjustment is off
```

Telnet Command: ip bindmac

This command allows users to set IP-MAC binding for LAN host.

`ip bindmac on`

`ip bindmac off`

`ip bindmac strict_on`

ip bindmac show

ip bindmac add [IP][MAC][Comment]

ip bindmac del [IP]/all

Syntax Description

Parameter	Description
<i>on</i>	Turn on IP bandmac policy. Even the IP is not in the policy table, it can still access into network.
<i>off</i>	Turn off all the bindmac policy.
<i>strict_on</i>	It means that only those IP address in IP bindmac policy table can access into network.
<i>show</i>	Display the IP address and MAC address of the pair of binded one.
<i>add</i>	Add one IP bindmac.
<i>del</i>	Delete one IP bindmac.
<i>IP</i>	Enter the IP address for binding with specified MAC address.
<i>MAC</i>	Enter the MAC address for binding with the IP address specified.
<i>Comment</i>	Type words as a brief description.
<i>All</i>	Delete all the IP bindmac settings.

Example

```
> ip bindmac add 192.168.1.46 00:50:7f:22:33:55 just for test
> ip bindmac show
ip bind mac function is turned ON
IP : 192.168.1.46 bind MAC : 00-50-7f-22-33-55 Comment : just
```

Telnet Command: ip maxnatuser

This command is used to set the maximum number of NAT users.

Syntax

ip maxnatuser *user no*

Syntax Description

Parameter	Description
<i>User no</i>	A number specified here means the total NAT users that Vigor router supports. 0 - It means no limitation.

Example

```
> ip maxnatuser 100
% Max NAT user = 100
```

Telnet Command: ip policy_rt

This command is used to set the IP policy route profile.

Syntax

ip policy_rt [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
<command><parameter>[...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
General Setup for Policy Route	
-i [value]	Specify an index number for setting policy route profile. Value: 1 to 60. "-1" means to get a free policy index automatically.
-e [0/1]	0: Disable the selected policy route profile. 1: Enable the selected policy route profile.
-o [value]	Determine the operation of the policy route. Value: add - Create a new policy route profile. del - Remove an existed policy route profile. edit - Modify an existed policy route profile. flush - Reset policy route to default setting.
-1 [any/range]	Specify the source IP mode. Range: Indicate a range of IP addresses. Any: It means any IP address will be treated as source IP address.
-2 [any/ip_range/ip_subnet/do main]	Specify the destination IP mode. Any: No need to specify an IP address for any IP address will be treated as destination IP address. ip_range: Indicates a range of IP addresses. ip_subnet: Indicates the IP subnet. domain: Indicates the domain name.
-3 [any/range]	Specify the destination port mode. Range: Indicate a range of port number.

	Any: It means any port number can be used as destination port.
<i>-G [default/specific]</i>	Specify the gateway mode.
<i>-L [default/specific]</i>	Specify the failover gateway mode.
<i>-s [value]</i>	Indicate the source IP start. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.1.0)
<i>-S [value]</i>	Indicate the source IP end. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.1.100)
<i>-d [value]</i>	Indicate the destination IP start. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.2.0)
<i>-D [value]</i>	Indicate the destination IP end. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.2.100)
<i>-p [value]</i>	Indicate the destination port start. Value: Type a number (1 - 65535) as the port start (e.g., 1000).
<i>-P [value]</i>	Indicate the destination port end. Value: Type a number (1 - 65535) as the port end (e.g., 2000).
<i>-y [value]</i>	Indicate the priority of the policy route profile. Value: Type a number (0 - 250). The default value is “150”.
<i>-I [value]</i>	Indicate the interface specified for the policy route profile. Value: Available interfaces include, LAN1 - LAN8, IP_Routed_Subnet, DMZ_Subnet, WAN1 - WAN5, VPN_PROFILE_1 - VPN_PROFILE_100, WAN_1_IP_ALIAS_1 - WAN_4_IP_ALIAS_8
<i>-g [value]</i>	Indicate the gateway IP address. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.3.1)
<i>-I [value]</i>	Indicate the failover IP address. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.4.1)
<i>-t [value]</i>	It means “protocol”. Value: Available settings include “TCP”, “UDP”, “TCP/UDP”, “ICMP” and “Any”.
<i>-n [0/1]</i>	Indicates the function of “Force NAT”. 0: Disable the function. 1: Enable the function.
<i>-a [0/1]</i>	Indicates to enable the function of failover. 0: Disable the function. 1: Enable the function.
<i>-f [value]</i>	It means to specify the interface for failover. Value: Available interfaces include, NO_FAILOVER, Default_WAN, Policy1 - Policy60 LAN1 - LAN8 IP_Routed_Subnet, DMZ_Subnet, WAN1 - WAN5, VPN_PROFILE_1 - VPN_PROFILE_100, WAN_1_IP_ALIAS_1 - WAN_4_IP_ALIAS_8
<i>-b [value]</i>	It means “failback”.

	Value: Available settings include, 0: Disable the function of “failback”. 1: Enable the function of “failback”. -v: View current failback setting.
Diagnose for Policy Route	
<code>-s [value]</code>	It means “source IP”. Value: Available settings include: Any: It indicates any IP address can be used as source IP address. “xxx.xxx.xxx.xxx”: The type format (e.g, 192.168.1.0).
<code>-d [value]</code>	It means “destination IP”. Value : Available settings include: Any: It indicates any IP address can be used as destination IP address. “xxx.xxx.xxx.xxx”: Specify an IP address.
<code>-p [value]</code>	It means “destination port”. Value: Specify a number or type Any (indicating any number).
<code>-t [value]</code>	It means “protocol”. Value: Available settings include “ICMP”, “TCP”, “UDP” and “Any”.

Example

```
> ip policy_rt diagnose -s 192.168.1.100 -d any -p any -t ICMP

-----
      Matched Route  (Priority)
-----
* No_Match

-----
      Matched Policy (Priority)
-----
* Policy_1 (200)

* Conclusion:The packet was dropped because the send-to interface
of the mat
ched policy "policy 1" was inactive and there was no failover setting
> ip policy_rt -i -1 -o add -1 range -s 192.168.1.10 -S 192.168.1.20 -2
ip_range -d 202.211.100.10 -D 202.211.100.20 -g 202.211.100.1 -I WAN2
```

Telnet Command: ip lanDNSRes

This command is used to set LAN DNS profile.

Syntax

`ip lanDNSRes [-<command> <parameter> | ...]`

Syntax Description

Parameter	Description
<code>[<command> <parameter> ...]</code>	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
<code>-a <IP Address></code>	Set IP Address that domain name mapped.
<code>-c <CNAME></code>	Set CNAME value.
<code>-d <address mapping index number></code>	Delete the selected LAN DNS profile.

-e <0/1>	0: disable the selected LAN DNS profile. 1: enable the selected LAN DNS profile.
-i <profile setting index number>	Enter the index number of the profile.
-l	List the content of LAN DNS profile (including domain name, IP address and message).
-n <domain name>	Set domain name.
-p <profile name>	Set profile name for LAN DNS.
-r	Reset the settings for selected profile.
-s <0/1>	0:reply all 1:reply only same subnet packet
-z	update LAN DNS config to DNS Cache

Example

```
>
ip lanDNSRes -i 1 -p test
% Configure Set1's Profile:test
> ip lanDNSRes -i 1 -l
% Idx: 1
% State: Disable
% Profile: test
% Domain Name:
% ----- Address Mapping Table -----
% Not Set Address Mapping.
>
```

Telnet Command: ip dnsforward

This command is used to set LAN DNS profile for conditional DNS forwarding.

ip dnsforward [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-a <IP Address>	Set forwarded DNS server IP Address.
-d <DNS server mapping index number>	Delete the selected LAN DNS profile.
-e <0/1>	0: disable such function. 1: enable such function.
-i <profile setting index number>	Enter the index number of the profile.
-l	List the content of LAN DNS profile (including domain name, IP address and message).
-n <domain name>	Set domain name.
-p <profile name>	Set profile name for LAN DNS.
-r	Reset the settings for selected profile.

Example


```

> ip dnsforward -i 1 -n ftp.drayTek.com
% Configure Set1's DomainName:ftp.drayTek.com
> ip dnsforward -i 1 -a 172.16.1.1
% Configure Set1's IP:172.16.1.1
> ip dnsforward -i 1 -l
% Idx: 1
% State: Disable
% Profile: test
% Domain Name: ftp.drayTek.com
% DNS Server IP: 172.16.1.1
>

```

Telnet Command: ip6 addr

This command allows users to set the IPv6 address for your router.

```
ip6 addr -s [prefix] [prefix-length] [LAN|WAN1|WAN2|iface#]
```

```
ip6 addr -d [prefix] [prefix-length] [LAN|WAN1|WAN2|iface#]
```

```
ip6 addr -a [LAN|WAN1|WAN2|iface#]
```

Syntax Description

Parameter	Description
-s	It means to add a static ipv6 address.
-d	It means to delete an ipv6 address.
-a	It means to show current address(es) status.
-u	It means to show only unicast addresses.
prefix	It means to Enter the prefix number of IPv6 address.
prefix-length	It means to type a fixed value as the length of the prefix.
LAN WAN1 WAN2 iface#	It means to specify LAN or WAN interface for such address.

Example

```

> ip6 addr -a
LAN
Unicast Address:
FE80::250:7FFF:FE00:0/64 (Link)
Multicast Address:
FF02::2
FF02::1:FF00:0
FF02::1

```

Telnet Command: ip6 dhcp req_opt

This command is used to configure option-request settings for DHCPv6 client.

```
ip6 dhcp req_opt [LAN|WAN1|WAN2|iface#] [-<command> <parameter>| ... ]
```

Syntax Description

Parameter	Description
req_opt	It means option-request.

<i>LAN WAN1 WAN2 iface#</i>	It means to specify LAN or WAN interface for such address.
<i>[<command> <parameter> ...]</i>	The available commands with parameters are listed below. <i>[...]</i> means that you can type in several commands in one line.
<i>-a</i>	It means to show current DHCPv6 status.
<i>-s</i>	It means to ask the SIP.
<i>-S</i>	It means to ask the SIP name.
<i>-d</i>	It means to ask the DNS setting.
<i>-D</i>	It means to ask the DNS name.
<i>-n</i>	It means to ask NTP.
<i>-i</i>	It means to ask NIS.
<i>-I</i>	It means to ask NIS name.
<i>-p</i>	It means to ask NISP.
<i>-P</i>	It means to ask NISP name.
<i>-b</i>	It means to ask BCMCS.
<i>-B</i>	It means to ask BCMCS name.
<i>-r</i>	It means to ask refresh time.
<i>Parameter</i>	1: the parameter related to the request will be displayed. 0: the parameter related to the request will not be displayed.

Example

```
> ip6 dhcp req_opt WAN2 -S 1
> ip6 dhcp req_opt WAN2 -r 1
> ip6 dhcp req_opt WAN2 -a
% Interface WAN2 is set to request following DHCPv6 options:
%   sip name
>
```

Telnet Command: ip6 dhcp client

This command allows you to use DHCPv6 protocol to obtain IPv6 address from server.

ip6 dhcp client *[WAN1|WAN2|iface#]* *[-<command> <parameter>| ...]*

Syntax Description

Parameter	Description
<i>client</i>	It means the dhcp client settings.
<i>[<command> <parameter> ...]</i>	The available commands with parameters are listed below. <i>[...]</i> means that you can type in several commands in one line.
<i>-a</i>	It means to show current DHCPv6 status.
<i>-p [IAID]</i>	It means to request identity association ID for Prefix Delegation.
<i>-n [IAID]</i>	It means to request identity association ID for Non-temporary Address.
<i>-c [parameter]</i>	It means to send rapid commit to server.
<i>-i [parameter]</i>	It means to send information request to server.
<i>-e[parameter]</i>	It means to enable or disable the DHCPv6 client. 1: Enable 0: Disable

Example

```
> ip6 dhcp client WAN2 -p 2008::1
> ip6 dhcp client WAN2 -a
Interface WAN2 has following DHCPv6 client settings:
    DHCPv6 client enabled
    request IA_PD whose IAID equals to 2008
> ip6 dhcp client WAN2 -n 1023456
> ip6 dhcp client WAN2 -a
Interface WAN2 has following DHCPv6 client settings:
    DHCPv6 client enabled
    request IA_NA whose IAID equals to 2008
> system reboot
```

Telnet Command: ip6 dhcp server

This command allows you to configure DHCPv6 server.

`ip6 dhcp server [-<command> <parameter>| ...]`

Syntax Description

Parameter	Description
<i>server</i>	It means the dhcp server settings.
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-a	It means to show current DHCPv6 status.
-i<pool_min_addr>	It means to set the start IPv6 address of the address pool.
-x<pool_max_addr>	It means to set the end IPv6 address of the address pool.
-d<addr>	It means to set the first DNS IPv6 address.
-D<addr>	It means to set the second DNS IPv6 address.
-c<parameter>	It means to send rapid commit to server. 1: Enable 0: Disable
-e<parameter>	It means to enable or disable the DHCPv6 server. 1: Enable 0: Disable

Example

```
> ip6 dhcp server -d FF02::1
> ip6 dhcp server -i ff02::1
> ip6 dhcp server -x ff02::3
> ip6 dhcp server -a
% Interface LAN has following DHCPv6 server settings:
%   DHCPv6 server disabled
%   maximum address of the pool: FF02::3
%   minimum address of the pool: FF02::1
%   1st DNS IPv6 Addr: FF02::1
```

Telnet Command: ip6 internet

This command allows you to configure settings for accessing Internet.

Syntax

ip6 internet *-W n -M n [-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
<i>-W n</i>	W means to set WAN interface and n means different selections. Default is WAN1. n=1: WAN1 n=2: WAN2 n=3: WAN3 . . n=X: WANx
<i>-M n</i>	M means to set Internet Access Mode (Mandatory) and n means different modes (represented by 0 - 5) n= 0: Offline, n=1: PPP, n=2: TSPC, n=3: AICCU, n=4: DHCPv6, n=5: Static n=6: 6in4-Static n=7: 6rd
<i>[<command> <parameter> /...]</i>	The available commands with parameters are listed below. [...] <i>]</i> means that you can type in several commands in one line.
<i>For 6rd</i>	
<i>-C n</i>	Set 6rd Connection Mode. n = 0: Auto n = 1: Static.
<i>-s [server]</i>	Set 6rd IPv4 Border Relay. server= IPv4 address
<i>-m n</i>	Set 6rd IPv4 address mask length. n=1 to 32.
<i>-p [prefix]</i>	Set 6rd IPv6 prefix. prefix= IPv6 address
<i>-l n</i>	Set 6rd IPv6 prefix length. n=1 to 64.
<i>For 6in4</i>	
<i>-s [server]</i>	Set 6in4 Remote Endpoint IPv4 Address. server= IPv4 address
<i>-l [IPv6 Addr]</i>	Set 6in4 IPv6 Address. IPv6 Addr= IPv6 address.
<i>-P n</i>	Set 6in4 IPv6 WAN prefix length. n=1 to 64. (Default number is 64)
<i>-p [prefix]</i>	Set 6in4 LAN Routed Prefix. prefix= IPv6 address
<i>-l n</i>	Set 6in4 LAN Routed Prefix length. n=1 to 64. (Default number is 64)

<i>-T n</i>	Set 6in4 Tunnel TTL. n=1 to 255. (Default number is 255)
<i>For TSPC/AICCU</i>	
<i>-u [username]</i>	Set Username (max. 63 characters).
<i>-P [password]</i>	Set Password (max. 63 characters).
<i>-s [server]</i>	Set Tunnel Server IP. server= IPv4 Address or URL (max. 63 characters).
<i>For AICCU</i>	
<i>-p [prefix]</i>	Set Subnet Prefix (AICCU). prefix=IPv6 address.
<i>-l n</i>	Subnet Prefix length (AICCU) n=1 to 64. (Default number is 64).
<i>-o [0/1]</i>	Set AICCU always on. On = 1, Off = 0.
<i>-f [Tunnel ID]</i>	Set AICCU tunnel ID. Tunnel ID= the number (e.g., T345678) offered by tunnel broker.
<i>For Static</i>	
<i>-w [addr]</i>	Set Default Gateway. Addr= IPv6 address.
<i>For others</i>	
<i>-d <server></i>	Set 1st DNS Server IP server= IPv6 Address.
<i>-D <server></i>	Set 2nd DNS Server IP. server= IPv6 Address.
<i>-t <dhcp/ra/none></i>	Set ipv6 PPP WAN test mode for DHCP or RA.
<i>-V</i>	View IPv6 Internet Access Profile.
<i>-k</i>	Dial the Tunnel on the WAN.
<i>-j</i>	Drop the Tunnel on the WAN.
<i>-r n</i>	Set Prefix State Machine RA timeout. n=any value (default is 15), (unit: second)
<i>-c n</i>	Set Prefix State Machine DHCPv6 Client timeout. n=any value (default is 15), (unit: second)
<i>-q [value]</i>	Set WAN detection mode. 0: NS Detect. 1: Ping Detect. 2: Always On.
<i>-z [value]</i>	Set Ping Detect TTL. value= 0 ~ 255.
<i>-x [hostname/IPv6 address]</i>	Set Ping Detect Host (hostname or IPv6 address).
<i>-l [interval]</i>	Set ipv6 connection interval. Interval = 1500-60000 (unit:10ms).
<i>-b [0/1]</i>	Enable DNSv6 based on DHCPv6. 0= off 1= on

Example

```

> ip6 internet -W 1 -M 2 -u userid -p passwd -s broker.freenet6.net
This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
>

```

Telnet Command: ip6 neigh

This command allows you to display IPv6 neighbour table.

Syntax

```
ip6 neigh -s [inet6_addr] [eth_addr] [LAN1/LAN2/.../LAN4/WAN1/WAN2/USB1/USB2]
```

```
ip6 neigh -d [inet6_addr] [LAN1/LAN2/.../LAN4/WAN1/WAN2/USB1/USB2]
```

```
ip6 neigh -a [inet6_addr] [-N LAN1/LAN2/.../LAN4/WAN1/WAN2/USB1/USB2]
```

Syntax Description

Parameter	Description
-s	It means to add a neighbour.
-d	It means to delete a neighbour.
-a	It means to show neighbour status.
inet6_addr	Type an IPv6 address
eth_addr	Type submask address.
LAN/WAN1/WAN2	Specify an interface for the neighbor.

Example

```

> ip6 neigh -s 2001:2222:3333::1111 00:50:7F:11:ac:22:WAN2
      Neighbour 2001:2222:3333::1111 successfully added!
> ip6 neigh -a

I/F  ADDR                               MAC                               STATE
-----
LAN  FF02::1                             33-33-00-00-00-01                CONNECTED
WAN2  2001:5C0:1400:B::10B8              00-00-00-00-00-00                CONNECTED
WAN2  2001:2222:3333::1111                00-00-00-00-00-00                CONNECTED
WAN2  2001:2222:6666::1111                00-00-00-00-00-00                CONNECTED
WAN2  ::                                  00-00-00-00-00-00                CONNECTED
LAN   ::                                  NONE
>

```

Telnet Command: ip6 neigh

This command allows you to add a proxy neighbour.

Syntax

```
ip6 neigh -s inet6_addr [LAN1|LAN2|...|LAN4|WAN1|WAN2|USB1|USB2]
```

```
ip6 neigh -d inet6_addr [LAN1|LAN2|...|LAN4|WAN1|WAN2|USB1|USB2]
```

```
ip6 neigh -a [inet6_addr] [-N LAN1|LAN2|...|LAN4|WAN1|WAN2|USB1|USB2]
```

Syntax Description

Parameter	Description
-s	It means to add a proxy neighbour.
-d	It means to delete a proxy neighbour.
-a	It means to show proxy neighbour status.
inet6_addr	Type an IPv6 address
LAN1 LAN2 ... LAN4 WAN1 WAN2 USB1 USB2	Specify an interface for the proxy neighbor.

Example

```
> ip6 neigh -s FE80::250:7FFF:FE12:300 LAN
% Neighbour FE80::250:7FFF:FE12:300 successfully added!
```

Telnet Command: ip6 route

This command allows you to

Syntax

```
ip6 route -s [prefix] [prefix-length] [gateway] [LAN|WAN1|WAN2|iface#> [-D]
```

```
ip6 route -s [prefix] [prefix-length] [gateway] [LAN1|LAN2|...|LAN4|WAN1|WAN2|
USB1|USB2|VPN1|...|VPN32] [-D]
```

```
ip6 route -d [prefix] [prefix-length]
```

```
ip6 route -a LAN1|LAN2|...|LAN4|WAN1|WAN2|USB1|USB2|VPN1|...|VPN32]
```

Syntax Description

Parameter	Description
-s	It means to add a route.
-d	It means to delete a route.
-a	It means to show the route status.
-D	It means that such route will be treated as the default route.
prefix	It means to Enter the prefix number of IPv6 address.
prefix-length	It means to type a fixed value as the length of the prefix.
gateway	It means the gateway of the router.
LAN1 LAN2 ... LAN4 WAN1 WAN2 USB1 USB2 VPN1 ... VPN32]	It means to specify LAN or WAN interface for such address.

Example

```

> ip6 route -s FE80::250:7FFF:FE12:500 16 FE80::250:7FFF:FE12:100 LAN
%      Route FE80::250:7FFF:FE12:500/16 successfully added!
> ip6 route -a LAN

PREFIX/PREFIX-LEN  _EXPIRES_  _NEXT-HOP_  I/F  METRIC  STATE  FLAGS
-----
FE80::/128
                0   ::
                LAN    0   UNICAST  U
FE80::250:7FFF:FE00:0/128
                0   ::
                LAN    0   UNICAST  U
FE80::/64
                0
                LAN   256  UNICAST  U
FE80::/16
                0   FE80::250:7FFF:FE12:100
                LAN   1024 UNICAST  UGA
FF02::1/128
                0   FF02::1
                LAN    0   UNICAST  UC
FF00::/8
                0
                LAN   256  UNICAST  U
::/0
                0
                LAN   -1  UNREACHABLE !

```

Telnet Command: ip6 ping

This command allows you to ping an IPv6 address or a host.

Syntax

ip6 ping [*IPV6 address/Host*] [*LAN1/LAN2/.../LAN4/WAN1/WAN2/USB1/USB2*][*send count*]
 [*data_size(1-1452)*]

Syntax Description

Parameter	Description
<i>IPV6 address/Host</i>	It means to specify the IPv6 address or host for ping.
<i>LAN1/LAN2/.../LAN4/WAN1/WAN2/USB1/USB2</i>	It means to specify LAN or WAN interface for such address.

Example

```

> ip6 ping 2001:4860:4860::8888 WAN2

Pinging 2001:4860:4860::8888 with 64 bytes of Data:

Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms

Packets: Sent = 5, Received = 5, Lost = 0 <% loss>
>

```


Telnet Command: ip6 tracert

This command allows you to trace the routes from the router to the host.

`ip6 tracert [IPv6 address/Host] [LAN1/LAN2/.../LAN4/WAN1/WAN2/USB1/USB2]`

Syntax Description

Parameter	Description
<code>IPv6 address/Host</code>	It means to specify the IPv6 address or host for ping.
<code>LAN1/LAN2/.../LAN4/WAN1/WAN2/USB1/USB2</code>	It means to specify LAN or WAN interface for such address.

Example

```
> ip6 tracert 2001:4860:4860::8888
traceroute to 2001:4860:4860::8888, 30 hops max through protocol ICMP
 1 2001:5C0:1400:B::10B8      340 ms
 2 2001:4DE0:1000:A22::1     330 ms
 3 2001:4DE0:A::1           330 ms
 4 2001:4DE0:1000:34::1     340 ms
 5 2001:7F8:1: :A501:5169:1 330 ms
 6 2001:4860::1:0:4B3       350 ms
 7 2001:4860::8:0:2DAF      330 ms
 8 2001:4860::2:0:66E      340 ms
 9 Request timed out.      *
10 2001:4860:4860::8888    350 ms
Trace complete.
>
```

Telnet Command: ip6 tpsc

This command allows you to display TSPC status.

Syntax

`ip6 tpsc [ifno]`

Syntax Description

Parameter	Description
<code>ifno</code>	It means the connection interface. Ifno=1 (means WAN1) Info=2 (means WAN2) ... etc.

Example

```
> ip6 tpsc 2
Local Endpoint v4 Address : 111.243.177.223
Local Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b9
Router DNS name : 88866666.broker.freenet6.net
Remote Endpoint v4 Address :81.171.72.11
Remote Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b8
Tspc Prefixlen : 56
Tunnel Broker: Amsterdam.freenet.net
```

```
Status: Connected
>
```

Telnet Command: ip6 radvd

This command allows you to enable or disable RADVD server.

Syntax

```
ip6 radvd [LAN1|LAN2|...|LAN4] [-<command> <parameter>| ... ]
```

```
ip6 radvd [R/u]
```

Syntax Description

Parameter	Description
<i>LAN1 LAN2 ... LAN4</i>	It means to specify LAN interface for such address.
<i><command> <parameter></i>	
<i>-s</i>	It means to enable or disable the default lifetime of the RADVD server. 1: Enable the RADVD server. 0: Disable the RADVD server.
<i>-D <1/0></i>	Enable/Disable the RDNSS.
<i>-d <lifetime></i>	Set the default lifetime for RADVD server.
<i>-i <lifetime></i>	Set the minimum interval time(sec) for RADVD server.
<i>-l <lifetime></i>	Set the maximum interval time(sec) for RADVD server.
<i>Lifetime</i>	It means to set the lifetime. The lifetime associated with the default router in units of seconds. It's used to control the lifetime of the prefix. The maximum value corresponds to 18.2 hours. A lifetime of 0 indicates that the router is not a default router and should not appear on the default router list. Enter the number (unit: second) you want.
<i>-h <hoplimit></i>	Set hop limit for RADVD server.
<i>-m <mtu/auto></i>	Set MTU value for RADVD server. Range: 1280-1500. auto - auto select MTU from WAN.
<i>-e <time></i>	Set reachable time.
<i>-a <time/infinity></i>	Set retransmit timer /infinity.
<i>-p <0/1/2></i>	Set default preference Low/Medium/High for RADVD server.
<i>-v</i>	View the RADVD server configuration.
<i>-V</i>	It means to show the RADVD configuration.
<i>-L <time/infinity>:</i>	Set prefix valid lifetime.
<i>-P <time/infinity></i>	Set prefix preferred lifetime.
<i>-r [num]</i>	Make RADVD test for item [num]. num - 0-default, 121:logo 121, 124:logo 124.
<i>-R</i>	Reload Config and send RA for subnets.
<i>-u</i>	View MTU on all interfaces.

Example

```

> ip6 radvd LAN1 -v
% [LAN1] setting !
% Status          : Enable
% RDNSS           : Enable
% Default Lifetime : 1800 seconds
% min interval time: 200 seconds
% MAX interval time: 600 seconds
% Hop limit       : 64
% MTU             : auto
% Reachable time  : 0
% Retransmit time : 0
% Preference      : Medium
% Prefix valid lifetime : 2592000
% Prefix preferred lifetime : 604800

```

Telnet Command: ip6 mngt

This command allows you to manage the settings for access list.

ip6 mngt list

ip6 mngt list [*add*<index> <prefix> <prefix-length>|*remove* <index>|*flush*]

ip6 mngt status

ip6 mngt [*http*|*telnet*|*ping*|*https*|*ssh*] [*on*|*off*]

Syntax Description

Parameter	Description
<i>list</i>	It means to show the setting information of the access list.
<i>status</i>	It means to show the status of IPv6 management.
<i>add</i>	It means to add an IPv6 address which can be used to execute management through Internet.
<i>index</i>	It means the number (1, 2 and 3) allowed to be configured for IPv6 management.
<i>prefix</i>	It means to Enter the IPv6 address which will be used for accessing Internet.
<i>prefix-length</i>	It means to type a fixed value as the length of the prefix.
<i>remove</i>	It means to remove (delete) the specified index number with IPv6 settings.
<i>flush</i>	It means to clear the IPv6 access table.
<i>http</i> <i>telnet</i> <i>ping</i> <i>https</i> <i>ssh</i>	These protocols are used for accessing Internet.
<i>on</i> <i>off</i>	It means to enable (on) or disable (off) the Internet accessing through http/telnet/ping.

Example

```

> ip6 mngt list add 1 FE80::250:7FFF:FE12:1010 128
> ip6 mngt list add 2 FE80::250:7FFF:FE12:1020 128
> ip6 mngt list add 3 FE80::250:7FFF:FE12:2080 128
> ip6 mngt list
% IPv6 Access List :
Index  IPv6 Prefix      Prefix Length
=====

```

```

1      FE80::250:7FFF:FE12:1010      128
2      FE80::250:7FFF:FE12:1020      128
3      FE80::250:7FFF:FE12:2080      128

> ip6 mngt status
% IPv6 Remote Management :
telnet : off,  http : off,  ping : off

```

Telnet Command: ip6 online

This command allows you to check the online status of IPv6 LAN /WAN.

`ip6 online [WAN1|WAN2|USB1|USB2]`

Syntax Description

Parameter	Description
<code>WAN1 WAN2 USB1 USB2</code>	It means the connection interface.

Example

```

> ip6 online WAN1
% WAN1 online status :
% IPv6 WAN1 Disabled
% Default Gateway : ::
% Interface : DOWN
% UpTime : 0:00:00
% IPv6 DNS Server: :: Static
% IPv6 DNS Server: :: Static
% IPv6 DNS Server: :: Static
% Tx packets = 0, Tx bytes = 0, Rx packets = 0, Rx bytes = 0
% MTU Onlink: 1280 , Config MTU : 0

```

Telnet Command: ip6 aiccu

This command allows you to view IPv6 settings for WAN interface with connection type of AICCU.

Syntax

`ip6 aiccu -i <ifno> -r`

`ip6 aiccu -i <ifno> -s`

Syntax Description

Parameter	Description
<code>-r</code>	Reset the AICCU retry account for the specified interace.
<code>ifno</code>	ifno=1, WAN1 ifno=2, WAN2 ifno=x, WANx
<code>-s</code>	Show the interface status.

Example

```

> ip6 aiccu -i 1 -r

```

```

reset AICCU Retry Account OK!

>

```

Telnet Command: ip6 ntp

This command allows you to set IPv6 settings for NTP (Network Time Protocols) server.

ip6 ntp -h

ip6 ntp -v

ip6 ntp -p [0/1]

Syntax Description

Parameter	Description
-h	It is used to display the usage of such command.
-v	It is used to show the NTP state.
-p <0/1>	It is used to specify NTP server for IPv6. 0 - Auto 1 - First Query IPv6 NTP Server.

Example

```

> ip6 ntp -p 1
% Set NTP Priority: IPv6 First

```

Telnet Command: ip6 lan

This command allows you to configure settings for IPv6 LAN.

Syntax

ip6 lan -l n [-<l:w:d:D:m:o:s> <parameter> / ...]

Syntax Description

Parameter	Description
-h	It is used to display the usage of such command.
<l:w:d:D:m:o:s><parameter>	The following lists all of the available commands with parameters.
-l n	Select LAN interface to be set. n = 1: LAN1. Default is LAN1. n = 2: LAN2 n = x: LANx
-w n	Select WAN interface to be primary. n = 0: None n = 1: WAN1 n = 2: WAN2 n = x: WANx.
-d <server>	Set the first DNS Server IP. <server>= IPv6 Address.
-D <server>	Set secondd DNS Server IP. <server>= IPv6 Address.
-m n	Set IPv6 LAN management. Default is SLAAC. n = 0: OFF n = 1: SLAAC

	n = 2: DHCPv6.
-o n	Enable Other option(O-bit) flag. (O-bit is redundant when management is DHCPv6) n= 0: Disable n= 1: Enable.
-e n:	Add an extension WAN. n = 1: WAN1 n = 2: WAN2 n = x: WANx.
-E n	Delete an extension WAN. n = 1: WAN1 n = 2: WAN2 n = x: WANx.
-b map	Set bit map(decimal) for extension WANs. map = bit 0: WAN1 map = bit 1: WAN2 map = bit n: WAN(n+1)
-f n	Disable IPv6. n = 1: Disable IPv6 n = 0: Enable IPv6.
-s n	Show IPv6 LAN setting. n = 0: show all. n = 1: LAN1, 2: LAN2, ... x: LANx, 5: DMZ. Default is show all

Example

```
> ip6 lan -l 2 -w 1 -d 2001:4860:4860::8888 -o 1 -f 0 -s 2
% Set LAN2!
% Set primary WAN1!
```

Telnet Command: ipf view

IPF users to view the version of the IP filter, to view/set the log flag, to view the running IP filter rules.

ipf view [-VcdhrtzZ]

Syntax Description

Parameter	Description
-V	It means to show the version of this IP filter.
-c	It means to show the running call filter rules.
-d	It means to show the running data filter rules.
-h	It means to show the hit-number of the filter rules.
-r	It means to show the running call and data filter rules.
-t	It means to display all the information at one time.
-z	It means to clear a filter rule's statistics.
-Z	It means to clear IP filter's gross statistics.

Example

```
> ipf view -V -c -d
ipf: IP Filter: v3.3.1 (1824)
Kernel: IP Filter: v3.3.1
```

```

Running: yes
Log Flags: 0x80947278 = nonip
Default: pass all, Logging: available

```

Telnet Command: ipf set

This command is used to set general rule for firewall.

`ipf set [Options]`

`ipf set [SET_NO] rule [RULE_NO] [Options]`

Syntax Description

Parameter	Description
<i>Options</i>	There are several options provided here, such as <code>-v</code> , <code>-c [SET_NO]</code> , <code>-d [SET_NO]</code> ,... and etc.
<i>SET_NO</i>	It means to specify the index number (from 1 to 12) of filter set.
<i>RULE_NO</i>	It means to specify the index number (from 1 to 7) of filter rule set.
<code>-v</code>	Type “-v” to view the configuration of general set.
<code>-c [SET_NO]</code>	It means to setup Call Filter, e.g., <code>-c 2</code> . The range for the index number you can type is “0” to “12” (0 means “disable”).
<code>-d [SET_NO]</code>	It means to setup Data Filter, e.g., <code>-d 3</code> . The range for the index number you can type is “0” to “12” (0 means “disable”).
<code>-l [VALUE]</code>	It means to setup Log Flag, e.g., <code>-l 2</code> Type “0” to disable the log flag. Type “1” to display the log of passed packet. Type “2” to display the log of blocked packet. Type “3” to display the log of non-matching packet.
<code>-p [VALUE]</code>	It means to setup actions for packet not matching any rule, e.g., <code>-p 1</code> Type “0” to let all the packets pass; Type “1” to block all the packets.
<code>-R [v4/v6] [Enable/Disable]</code>	Accept routing packet from WAN., e.g., <code>-R v4 0</code> : Set Accept routing packet from WAN by IPv4 is enable <code>-R v4 1</code> : Set Accept routing packet from WAN by IPv6 is disable <code>-R v6 0</code> : Set Accept routing packet from WAN by IPv4 is enable <code>-R v6 1</code> : Set Accept routing packet from WAN by IPv6 is disable
<code>-L [VALUE]</code>	Enable/Disable Strict Security Firewall, e.g., <code>-L 1</code> . 0:Disable, 1:Enable
<code>-C [VALUE]</code>	Setup the code page, e.g., <code>-C 12</code> . Type 1 - 12 as the code page number. If “0” is set, the code page setting is disabled.
<code>-M [APPE_NO]</code>	It means to configure APPE for the packets not matching with any rule, e.g., <code>-M 1</code> Type “0” to let all the packets pass; Type “1” to block all the packets.
<code>-U [URL_NO]</code>	It means to configure URL content filter for the packets not matching with any rule, e.g., <code>-U 1</code> Type “0” to let all the packets pass; Type “1” to block all the packets.
<code>-W [WEB_NO]</code>	Setup WEB Content Filter for packet not matching any rule.
<code>-D [DNS_NO]</code>	Setup DNS Filter for packet not matching any rule.

-g [VALUE]	Setup DNS Filter syslog. Type "0" to disable the function. Type "1" to enable the function.
-a [AD_SET]	It means to configure the advanced settings.
-f [VALUE]	It means to accept large incoming fragmented UDP or ICMP packets.
-E [VALUE]	It means to set the maximum count (0 ~ 60000) for session limitation.
-F [VALUE]	It means to configure the load-balance policy.
-Q [VALUE]	It means to set the QoS class.

Example

```

> ipf set -c 1 #set call filter start from set 1
Setting saved.

> ipf set -d 2 #set data filter start from set 2
Setting saved.
> ipf set -v

Call Filter: Enable (Start Filter Set = 1)
Data Filter: Enable (Start Filter Set = 2)
Log Flag   : None

Actions for packet not matching any rule:
Pass or Block   : Pass
CodePage        : ANSI(1252)-Latin I
Max Sessions Limit: 60000
Current Sessions : 0
Mac Bind IP     : Non-Strict
QOS Class       : None
APP Enforcement  : None
URL Content Filter: None
Load-Balance policy : Auto-select
-----
CodePage          : ANSI(1252)-Latin I
Window size       : 65535
Session timeout   : 1440
DrayTek Banner    : Enable
-----
Apply IP filter to VPN incoming packets      : Enable
Accept large incoming fragmented UDP or ICMP packets: Enable
-----
Strict Security Checking
[ ] APP Enforcement
>

```

Telnet Command: ipf rule

This command is used to set filter rule for firewall.

```
ipf rule s r [-<command> <parameter> | ...
```

```
ipf rule s r -v
```


Syntax Description

Parameter	Description
<i>s</i>	Such word means Filter Set, range form 1-12.
<i>r</i>	Such word means Filter Rule, range from 1-7.
<i><Command><parameter></i>	The following lists all of the available commands with parameters.
<i>-e</i>	It means to enable or disable the rule setting. 0- disable 1- enable
<i>-s o:g <obj></i>	It means to specify source IP object and IP group. o - indicates "object". g - indicates "group". obj - indicates index number of object or index number of group. Available settings range from 1-192. For example, "-s g 3" means the third source IP group profile.
<i>-s u <Address Type> <Start IP Address> <End IP Address> / <Address Mask></i>	It means to configure source IP address including address type, start IP address, end IP address and address mask. u - It means "user defined". <i>Address Type</i> - Enter the number (representing different address type). 0 - Subnet Address 1 - Single Address 2 - Any Address 3 - Range Address Example: Set Subnet Address => -s u 0 192.168.1.10 255.255.255.0 Set Single Address => -s u 1 192.168.1.10 Set Any Address => -s u 2 Set Range Address => -s u 3 192.168.1.10 192.168.1.15
<i>-d u <Address Type> <Start IP Address> <End IP Address> / <Address Mask></i>	It means to configure destination IP address including address type, start IP address, end IP address and address mask. u - It means "user defined". <i>Address Type</i> - Enter the number (representing different address type). 0 - Subnet Address 1 - Single Address 2 - Any Address 3 - Range Address Example: Set Subnet Address => -d u 0 192.168.1.10 255.255.255.0 Set Single Address => -d u 1 192.168.1.10 Set Any Address => -d u 2 Set Range Address => -d u 3 192.168.1.10 192.168.1.15
<i>-d o:g <obj></i>	It means to specify destination IP object and IP group. o - indicates "object". g - indicates "group" <obj>- indicates index number of object or index number of group. Available settings range from 1-192. For example, "-d g 1" means the first destination IP group profile.
<i>-S o:g <obj></i>	It means to specify Service Type object and IP group. o - indicates "object". g - indicates "group"

	<p><obj> - indicates index number of object or index number of group. Available settings range from 1-96. For example, “-S 0 1” means the first service type object profile.</p>
<p>-S u <protocol> <source_port__value> <destination_port_vale></p>	<p>It means to configure advanced settings for Service Type, such as protocol and port range. u - it means “user defined”. <protocol> - It means TCP(6),UDP(17), TCP/UDP(255). <source_port__value> - 1 - Port OP, range is 0-3. 0:= =, 1:!=, 2:>, 3:< 3 - Port range of the Start Port Number, range is 1-65535. 5 - Port range of the End Port Number, range is 1-65535. <destination_port_value>: 2 - Port OP, range is 0-3, 0:==, 1:!=, 2:>, 3:< 4 - Port range of the Start Port Number, range is 1-65535. 6 - Port range of the End Port Number, range is 1-65535.</p>
<p>-F <index> <log flag></p>	<p>It means the Filter action you can specify. index - Available settings contain: 0 -Pass Immediately, 1 - Block Immediately, 2 - Pass if no further match, 3 - Block if no further match. log flag - 0 means disable to save and display in Syslog; 1 means enable to save and display in Syslog.</p>
<p>-q <index> <log flag></p>	<p>It means the classification for QoS. index - Available settings contain: 1- Class 1, 2 - Class 2, 3 - Class 3, 4 - Other log flag - 0 means disable to save and display in Syslog; 1 means enable to save and display in Syslog.</p>
<p>-l <wan> <log flag></p>	<p>It means to set load balance policy. wan - Available settings contain 0 (means auto-select), 1 (means WAN1), 2 (means WAN2) and 3 (means WAN3). log flag - 0 means disable to save and display in Syslog; 1 means enable to save and display in Syslog.</p>
<p>-E<index></p>	<p>It means to enable APP Enforcement for Strict Security Checking. <index> - Available settings for APP Enforcement are: 0 - disable APP Enforcement. 1- enable APP Enforcement.</p>
<p>-a <index> <Log Flag></p>	<p>It means to specify which APP Enforcement profile will be applied. <index> - Available settings range for APP Enforcement is 0 - 32. “0” means no profile will be applied. log flag - 0 means disable to save and display in Syslog; 1 means enable to save and display in Syslog.</p>
<p>-u <index> <Log Flag></p>	<p>It means to specify which URL Content Filter profile will be applied. <index> - Available settings range from 0 - 8. “0” means no profile will be applied. log flag- 0 means disable to save and display in Syslog; 1 means enable to save and display in Syslog.</p>
<p>-w <index> <Log Flag></p>	<p>It means to specify which Web Content Filter profile will be applied.</p>

	<p><index> - Available settings range from 0 - 8. "0" means no profile will be applied.</p> <p>log flag- 0 means disable to save and display in Syslog; 1 means enable to save and display in Syslog.</p>
-n <index> <Log Flag>	<p>It means to specify which DNS Filter profile will be applied.</p> <p><index> - Available settings range from 0 - 8. "0" means no profile will be applied.</p> <p>log flag- 0 means disable to save and display in Syslog; 1 means enable to save and display in Syslog.</p>
-c <0-20>	<p>It means to set code page. Different number represents different code page.</p> <ul style="list-style-type: none"> 0. None 1. ANSI(1250)-Central Europe 2. ANSI(1251)-Cyrillic 3. ANSI(1252)-Latin I 4. ANSI(1253)-Greek 5. ANSI(1254)-Turkish 6. ANSI(1255)-Hebrew 7. ANSI(1256)-Arabic 8. ANSI(1257)-Baltic 9. ANSI(1258)-Viet Nam 10. OEM(437)-United States 11. OEM(850)-Multilingual Latin I 12. OEM(860)-Portuguese 13. OEM(861)-Icelandic 14. OEM(863)-Canadian French 15. OEM(865)-Nordic 16. ANSI/OEM(874)-Thai 17. ANSI/OEM(932)-Japanese Shift-JIS 18. ANSI/OEM(936)-Simplified Chinese GBK 19. ANSI/OEM(949)-Korean 20. ANSI/OEM(950)-Traditional Chinese Big5
-C <Windows Size> <Session_Timeout>	<p>It means to set Window size and Session timeout (Minute).</p> <p><Windows Size> - Available settings range from 1 - 65535.</p> <p><Session_Timeout> - Make the best utilization of network resources.</p>
-M <Your Comments>	Set the content of the comments for a rule.
-v	It is used to show current filter/rule settings.

Example

```

> ipf rule 2 1 -e 1 -M "Your Comments" -s "o 1" -d "o 2" -S "o 1" -F "1 1"

Setting saved.
> ipf rule 2 1 -v

Filter Set 2 Rule 1:

Status : Enable
Comments: Your
Index(1-15) in Schedule Setup: <null>, <null>, <null>, <null>

Direction : LAN -> WAN
Source IP : Object1,

```

```

Destination IP: Object2,
Service Type : TCP/UDPObject1,
Fragments : Don't Care

Pass or Block : Block Immediately
Branch to Other Filter Set: None
Max Sessions Limit : 60000
Current Sessions : 0
Mac Bind IP : Non-Strict
Qos Class : None
APP Enforcement : None
URL Content Filter : None
WEB Content Filter : None
DNS Filter : None
Load-Balance policy : Auto-select
Log : Enable

-----
CodePage : ANSI(1252)-Latin I
Window size : 65535
Session timeout : 1440
DrayTek Banner : Enable

-----
Strict Security Checking
[ ]APP Enforcement
>

```

Telnet Command: ipf flowtrack

This command is used to set and view flowtrack sessions.

`ipf flowtrack set [-re]`

`ipf flowtrack view [-fb]`

`ipf flowtrack [-i][-p][-t]`

Syntax Description

Parameter	Description
<code>-r</code>	It means to refresh the flowtrack.
<code>-e</code>	It means to enable or disable the flowtrack.
<code>-f</code>	It means to show the sessions state of flowtrack. If you do not specify any IP address, then all the session state of flowtrack will be displayed.
<code>-b</code>	It means to show all of IP sessions state.
<code>-i [IP address]</code>	It means to specify IP address (e.g., -i 192.168.2.55).
<code>-p[value]</code>	It means to type a port number (e.g., -p 1024). Available settings are 0 ~ 65535.
<code>-t [value]</code>	It means to specify a protocol (e.g., -t tcp). Available settings include: <i>tcp</i> <i>udp</i> <i>icmp</i>

Example

```
>ipf flowtrack set -r
Refresh the flowstate ok
> ipf flowtrack view -f
Start to show the flowtrack sessions state:

ORIGIN>> 192.168.1.11:59939 ->      8.8.8.8: 53 ,ifno=0
REPLY >>      8.8.8.8: 53 -> 192.168.1.11:59939 ,ifno=3
          proto=17, age=93023180(3920), flag=203
ORIGIN>> 192.168.1.11:15073 ->      8.8.8.8: 53 ,ifno=0
REPLY >>      8.8.8.8: 53 -> 192.168.1.11:15073 ,ifno=3
          proto=17, age=93025100(2000), flag=203
ORIGIN>> 192.168.1.11: 7247 ->      8.8.8.8: 53 ,ifno=0
REPLY >>      8.8.8.8: 53 -> 192.168.1.11: 7247 ,ifno=3
          proto=17, age=93020100(7000), flag=203
End to show the flowtrack sessions state
> ipf flowtrack set -e
Current flow_enable=0
> ipf flowtrack set -e
Curretn flow_enable=1
```

Telnet Command: Log

This command allows users to view log for WAN interface such as call log, IP filter log, flush log buffer, etc.

```
log [-cfhiptwx?] [-F a | c | f | w]
```

Syntax Description

Parameter	Description
-c	It means to show the latest call log.
-f	It means to show the IP filter log.
-F	It means to show the flush log buffer. a: flush all logs c: flush the call log f: flush the IP filter log w: flush the WAN log
-h	It means to show this usage help.
-p	It means to show PPP/MP log.
-t	It means to show all logs saved in the log buffer.
-w	It means to show WAN log.
-x	It means to show packet body hex dump.

Example

```
> log -w
25:36:25.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
      Client IP      = 0.0.0.0
      Your IP        = 0.0.0.0
```

```

Next server IP = 0.0.0.0
Relay agent IP = 0.0.0.0
25:36:33.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
Client IP      = 0.0.0.0
Your IP       = 0.0.0.0
Next server IP = 0.0.0.0
Relay agent IP = 0.0.0.0
25:36:41.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
Client IP      = 0.0.0.0
Your IP       = 0.0.0.0
Next server IP = 0.0.0.0
Relay agent IP = 0.0.0.0
25:36:49.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
Client IP      = 0.0.0.0
Your IP       = 0.0.0.0
Next server IP = 0.0.0.0
Relay agent IP = 0.0.0.0
25:36:57.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
Client IP      = 0.0.0.0
Your IP       = 0.0.0.0
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
```

Telnet Command: radius

This command allows you to configure detailed settings for RADIUS server

Syntax

`radius enable [0/1]`

`radius authport [port number]`

`radius client [add] [idx] -i [address] -m [mask] -p [prefix] -l [length] -s [secret]`

`radius client [del] [idx]`

`radius show`

`radius set_dot1x_phase1 -e [method_idx]`

`radius set_dot1x_phase1 -d [method_idx]`

`radius set_dot1x_phase2 -e [method_idx]`

`radius set_dot1x_phase2 -d [method_idx]`

Syntax Description

Parameter	Description
<code>enable[0/1]</code>	Enable (1) or disable (0) the RADIUS server.
<code>authport [port number]</code>	Configure the port number for authentication. Port number: Available range is from 0 to 65535. Default value is "1812".
<code>set_auth_method [method idx]</code>	Specify which method will be used for authentication. Method idx: "0" is "Only PAP"; "1" is "PAP/CHAP/MS-CHAP/MS-CHAPv2".
<code>client add</code>	Specify a client to be authenticated by RADIUS server by typing required information as follows: -i [address]: client IPv4 address(domain)

	-m [mask]: client IPv4 mask -p [prefix]: client IPv6 prefix -l [length]: client IPv6 prefix length -s [secret]: shared secret ex: radius client add 1 -i 192.168.1.1 -m 255.255.255.0 -s 123
<i>client [del] [idx]</i>	<i>del</i> - Delete related settings for selected client. <i>idx</i> - Specify the index number of client profiles.
<i>show</i>	Display the status of RADIUS server.
<i>enable_dot1x [0/1]</i>	Enable (1) or disable (0) the 802.1X Authentication function of RADIUS Server. Default is disabled.
<i>set_dot1x_phase1 [method_idx]</i>	Set the phase1 method for 802.1X authentication of RADIUS server. <i>method_idx</i> - Specify which method will be used. At present, dot1x_phase1 can only support PEAP now. So only "1" can be used for it.
<i>set_dot1x_phase2 [method_idx]</i>	Set the phase2 method for 802.1X authentication of RADIUS server. <i>method_idx</i> - Specify which method will be used. Dot1x_phase2 can only support MS-CHAPv2 now. So only "1" can be used for it.
<i>-e</i>	Set method for dot1x_phase1 or dot1x_phase2.
<i>-d</i>	Delete method for dot1x_phase1 or dot1x_phase2.

Example

```
> radius client add 1 -i 192.168.1.1 -m 255.255.255.0 -s 123
```

Telnet Command: tacacsplus set

This command allows users to configure general settings for TACACS+ server

Syntax

```
tacacspluse set [Options][Value]
```

Syntax Description

Parameter	Description
<i>enable [0-1]</i>	Disable (0)/enable(1) the TACACS+ server.
<i>IP <VALUE></i>	Set the IP address of TACACS+ server.
<i>port <VALUE></i>	Set the port number of TACACS+ server.
<i>shared_secret <VALUE></i>	Set the Shared Secret value of TACACS+ Server.

Example

```
> tacacsplus set enable 1
TACACS+ enabled!
This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.

> tacacsplus set IP 192.168.1.59
TACACS+ Server IP has been setting.
This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

```

> tacacsplus view
TACACS+ Enable:Enable.
TACACS+ Server IP:192.168.1.59
TACACS+ Server Port:49
TACACS+ Type:ASCII
TACACS+ Shared Secret:

```

Telnet Command: tacacsplus view

This command allows users to check the general settings for TACACS+ server

Syntax

tacacspluse view

Example

```

> tacacsplus view
TACACS+ Enable:Enable.
TACACS+ Server IP:192.168.1.59
TACACS+ Server Port:49
TACACS+ Type:ASCII
TACACS+ Shared Secret:

```

Telnet Command: mngt ftpport

This command allows users to set FTP port for management.

mngt ftpport [*FTP port*]

Syntax Description

Parameter	Description
<i>FTP port</i>	It means to Enter the number for FTP port. The default setting is 21.

Example

```

> mngt ftpport 21
% Set FTP server port to 21 done.

```

Telnet Command: mngt httpport

This command allows users to set HTTP port for management.

mngt httpport [*Http port*]

Syntax Description

Parameter	Description
<i>Http port</i>	It means to enter the number for HTTP port. The default setting is 80.

Example

```

> mngt httpport 80
% Set web server port to 80 done.

```

Telnet Command: mngt httpsport

This command allows users to set HTTPS port for management.

mngt httpsport [*Https port*]

Syntax Description

Parameter	Description
<i>Https port</i>	It means to Enter the number for HTTPS port. The default setting is 443.

Example

```
> mngt httpsport 443
% Set web server port to 443 done.
```

Telnet Command: mngt telnetport

This command allows users to set telnet port for management.

mngt telnetport [*Telnet port*]

Syntax Description

Parameter	Description
<i>Telnet port</i>	It means to Enter the number for telnet port. The default setting is 23.

Example

```
> mngt telnetport 23
% Set Telnet server port to 23 done.
```

Telnet Command: mngt sshport

This command allows users to set SSH port for management.

mngt sshport [*ssh port*]

Syntax Description

Parameter	Description
<i>ssh port</i>	It means to Enter the number for SSH port. The default setting is 22.

Example

```
> mngt sshport 23
% Set ssh port to 23 done.
```

Telnet Command: mngt noping

This command is used to pass or block Ping from LAN PC to the internet.

mngt noping [*on*]

mngt noping [*off*]

mngt noping [*viewlog*]

mngt noping [*clearlog*]

Syntax Description

Parameter	Description
<i>on</i>	All PING packets will be forwarded from LAN PC to Internet.
<i>off</i>	All PING packets will be blocked from LAN PC to Internet.
<i>viewlog</i>	It means to display a log of ping action, including source MAC and source IP.
<i>clearlog</i>	It means to clear the log of ping action.

Example

```
> mngt noping off  
No Ping Packet Out is OFF!!
```

Telnet Command: mngt defenseworm

This command can block specified port for passing through the router.

mngt defenseworm *[on]*

mngt defenseworm *[off]*

mngt defenseworm *[add port]*

mngt defenseworm *[del port]*

mngt defenseworm *[viewlog]*

mngt defenseworm *[clearlog]*

Syntax Description

Parameter	Description
<i>on</i>	It means to activate the function of defense worm packet out.
<i>off</i>	It means to inactivate the function of defense worm packet out.
<i>add port</i>	It means to add a new TCP port for block.
<i>del port</i>	It means to delete a TCP port for block.
<i>viewlog</i>	It means to display a log of defense worm packet, including source MAC and source IP.
<i>clearlog</i>	It means to remove the log of defense worm packet.

Example

```
> mngt defenseworm add 21
Add TCP port 21
Block TCP port list: 135, 137, 138, 139, 445, 21
> mngt defenseworm del 21
Delete TCP port 21
Block TCP port list: 135, 137, 138, 139, 445
```

Telnet Command: mngt rmtcfg

This command can allow the system administrators to login from the Internet. By default, it is not allowed.

mngt rmtcfg *[status]*

mngt rmtcfg *[enable]*

mngt rmtcfg *[disable]*

mngt rmtcfg *[http/https/ftp/telnet/ssh/tr069] [on/off]*

Syntax Description

Parameter	Description
<i>status</i>	It means to display current setting for your reference.
<i>enable</i>	It means to allow the system administrators to login from the Internet.
<i>disable</i>	It means to deny the system administrators to login from the Internet.
<i>http/https/ftp/telnet/ssh/tr069</i>	It means to specify one of the servers/protocols for enabling or disabling.
<i>on/off</i>	on - enable the function.

off - disable the function.

Example

```
> mngt rmtcfg ftp on
Enable server fail
Remote configure function has been disabled
please enable by enter mngt rmtcfg enable

> mngt rmtcfg enable
%% Remote configure function has been enabled.
> mngt rmtcfg ftp on
%% FTP server has been enabled.
```

Telnet Command: mngt lanaccess

This command allows users to manage accessing into Vigor router through LAN port.

`mngt lanaccess -e [0/1] -s [value] -i [value]`

`mngt lanaccess -f`

`mngt lanaccess -d`

`mngt lanaccess -v`

`mngt lanaccess -h`

Syntax Description

Parameter	Description
<code>-e[0/1]</code>	It means to enable/disable the function. 0-disable the function. 1-enable the function.
<code>-s[value]</code>	It means to specify service offered. Available values include: FTP, HTTP, HTTPS, TELNET, SSH, None, All
<code>-i[value]</code>	It means the interface which is allowed to access. Available values include: LAN2-LAN6, DMZ, IP Routed Subnet, None, All Note: LAN1 is always allowed for accessing into the router.
<code>-f</code>	It means to flush all of the settings.
<code>-d</code>	It means to restore the factory default settings.
<code>-v</code>	It means to view current settings.
<code>-h</code>	It means to get the usage of such command.

Example

```
> mngt lanaccess -e 1
> mngt lanaccess -s FTP,TELNET
> mngt lanaccess -i LAN3
>> mngt lanaccess -v
Current LAN Access Control Setting:
* Enable:Yes
* Service:
  - FTP:Yes
```

- HTTP:No
- HTTPS:No
- TELNET:Yes
- SSH:No
- * Subnet:
 - LAN 2: disabled
 - LAN 3: enabled
 - LAN 4: disabled
 - LAN 5: disabled
 - LAN 6: disabled
 - DMZ: disabled
 - IP Routed Subnet: disabled

Note: the settings do NOT apply to LAN1, LAN1 is always allowed to access the router

Telnet Command: mngt echoicmp

This command allows users to reject or accept PING packets from the Internet.

mngt echoicmp *[enable]*

mngt echoicmp *[disable]*

Syntax Description

Parameter	Description
<i>enable</i>	It means to accept the echo ICMP packet.
<i>disable</i>	It means to drop the echo ICMP packet.

Example

```
> mngt echoicmp enable
%% Echo ICMP packet enabled.
```

Telnet Command: mngt accesslist

This command allows you to specify that the system administrator can login from a specific host or network. A maximum of three IPs/subnet masks is allowed.

mngt accesslist *list*

mngt accesslist *add [index][ip addr][mask]*

mngt accesslist *remove [index]*

mngt accesslist *flush*

Syntax Description

Parameter	Description
<i>list</i>	It can display current setting for your reference.
<i>add</i>	It means adding a new entry.
<i>index</i>	It means to specify the number of the entry.
<i>ip addr</i>	It means to specify an IP address.
<i>mask</i>	It means to specify the subnet mask for the IP address.

<i>remove</i>	It means to delete the selected item.
<i>flush</i>	It means to remove all the settings in the access list.

Example

```
> mngt accesslist add 1 192.168.1.89 255.255.255.0
%% Set OK.
> mngt accesslist list
%% Access list :
   Index IP address      Subnet mask
=====
   1      192.168.1.89    255.255.255.0
```

Telnet Command: mngt snmp

This command allows you to configure SNMP for management.

mngt snmp [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-e <1/2>	1: Enable the SNMP function. 2: Disable the SNMP function.
-g<Community name>	It means to set the name for getting community by typing a proper character. (max. 23 characters)
-s <Community name>	It means to set community by typing a proper name. (max. 23 characters)
-m <IP address>	It means to set one host as the manager to execute SNMP function. Please type in IPv4 address to specify certain host.
-t <Community name>	It means to set trap community by typing a proper name. (max. 23 characters)
-n <IP address>	It means to set the IPv4 address of the host that will receive the trap community.
-T <seconds>	It means to set the trap timeout <0-999>.
-V	It means to list SNMP setting.

Example

```
> mngt snmp -e 1 -g draytek -s DK -m 192.168.1.1 -t trapcom -n 10.20.3.40
-T 88
SNMP Agent Turn on!!!
Get Community set to draytek
Set Community set to DK
Manager Host IP set to 192.168.1.1
Trap Community set to trapcom
Notification Host IP set to 10.20.3.40
Trap Timeout set to 88 seconds
```

Telnet Command: msubnet switch

This command is used to configure multi-subnet.

`msubnet switch [2/3/4][On/Off]`

Syntax Description

Parameter	Description
<i>2/3/4/5/6</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<i>On/Off</i>	On means turning on the subnet for the specified LAN interface. Off means turning off the subnet.

Example

```
> msynet switch 2 On
% LAN2          Subnet On!
```

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.

Telnet Command: msynet addr

This command is used to configure IP address for the specified LAN interface.

`msubnet addr [2/3/4][IP address]`

Syntax Description

Parameter	Description
<i>2/3/4/5/6</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<i>IP address</i>	Enter the private IP address for the specified LAN interface.

Example

```
> msynet addr 2 192.168.5.1
% Set LAN2 subnet IP address done !!!
```

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.

Telnet Command: msynet nmask

This command is used to configure net mask address for the specified LAN interface.

`msubnet nmask [2/3/4][IP address]`

Syntax Description

Parameter	Description
<i>2/3/4/5/6</i>	It means LAN interface. 2=LAN2 3=LAN3

	4=LAN4
<i>IP address</i>	Enter the subnet mask address for the specified LAN interface.

Example

```
> msubnet nmask 2 255.255.0.0
% Set LAN2 subnet mask done !!!

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet status

This command is used to display current status of subnet.

`msubnet status [2/3/4]`

Syntax Description

Parameter	Description
<i>2/3/4/5/6</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4

Example

```
> msubnet status 2
% LAN2      Off: 0.0.0.0/0.0.0.0, PPP Start IP: 0.0.0.60
% DHCP server: Off
% Dhcp Gateway: 0.0.0.0, Start IP: 0.0.0.10, Pool Count: 50
```

Telnet Command: msubnet dhcps

This command allows you to enable or disable DHCP server for the subnet.

`msubnet dhcps [2/3/4][On/Off]`

Syntax Description

Parameter	Description
<i>2/3/4/5/6</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<i>On/Off</i>	On means enabling the DHCP server for the specified LAN interface. Off means disabling the DHCP server.

Example

```
> msubnet dhcps 3 off
% LAN3      Subnet DHCP Server disabled!

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet nat

This command is used to configure the subnet for NAT or Routing usage.

`msubnet nat [2/3/4] [On/Off]`

Syntax Description

Parameter	Description
<i>2/3/4/5/6</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<i>On/Off</i>	On - It means the subnet will be configured for NAT usage. Off - It means the subnet will be configured for Routing usage.

Example

```
> > ms subnet nat 2 off
% LAN2 Subnet is for Routing usage!
%Note: If you have multiple WAN connections, please be reminded to setup
a Load-Balance policy so that packets from this subnet will be forwarded
to the right WAN interface!

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

Telnet Command: ms subnet gateway

This command is used to configure an IP address as the gateway used for subnet.

`msubnet gateway [2/3/4] [Gateway IP]`

Syntax Description

Parameter	Description
<i>2/3/4/5/6</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<i>Gateway IP</i>	Specify an IP address as the gateway IP.

Example

```
> ms subnet gateway 2 192.168.1.13
% Set LAN2 Dhcp Gateway IP done !!!

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

Telnet Command: ms subnet ipc nt

This command is used to defined the total number allowed for each LAN interface.

`msubnet ipc nt [2/3/4] [IP counts]`

Syntax Description

Parameter	Description
-----------	-------------

<i>2/3/4/5/6</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<i>IP counts</i>	Specify a total number of IP address allowed for each LAN interface. The available range is from 0 to 220.

Example

```
> msubnet ipcnt 2 15
This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet talk

This command is used to establish a route between two LAN interfaces.

`msubnet talk [1/2/3/4] [1/2/3/4] [On/Off]`

Syntax Description

Parameter	Description
<i>1/2/3/4</i>	It means LAN interface. 1=LAN1 2=LAN2 3=LAN3 4=LAN4
<i>On/Off</i>	On - It means to establish a link for the selected LAN with others. Off - It means to terminate the link.

Example

```
> msubnet talk 1 2 on
% Enable routing between LAN1 and LAN2!

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.

> msubnet talk
% msubnet talk <1/2/3/4> <1/2/3/4> <On/Off>
% where 1:LAN1, 2:LAN2, 3:LAN3, 4:LAN4
% Now:
%           LAN1  LAN2  LAN3  LAN4
% LAN1           V
% LAN2          V    V
% LAN3                   V
% LAN4                               V
```

Telnet Command: msubnet startip

This command is used to configure a starting IP address for DHCP.

`msubnet startip [2/3/4] [Gateway IP]`

Syntax Description

Parameter	Description
<i>2/3/4</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<i>Gateway IP</i>	Type an IP address as the starting IP address for a subnet.

Example

```
> msubnet startip 2 192.168.2.90
%Set LAN2 Dhcp Start IP done !!!

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
> msubnet startip ?
% msubnet startip <2/3/4> <Gateway IP>
% Now: LAN2 192.168.2.90; LAN3 192.168.3.10; LAN4 192.168.4.10;
```

Telnet Command: msubnet pppip

This command is used to configure a starting IP address for PPP connection.

`msubnet pppip [2/3/4] [Start IP]`

Syntax Description

Parameter	Description
<i>2/3/4</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<i>Start IP</i>	Type an IP address as the starting IP address for PPP connection.

Example

```
> msubnet pppip 2 192.168.2.250
% Set LAN2 PPP(IPCP) Start IP done !!!

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.

> msubnet pppip ?
% msubnet pppip <2/3/4> <Start IP>
% Now: LAN2 192.168.2.250; LAN3 192.168.3.200; LAN4 192.168.4.200
```

Telnet Command: msubnet nodetype

This command is used to specify the type for node which is required by DHCP option.

`msubnet nodetype [2/3/4][count]`

Syntax Description

Parameter	Description
<i>2/3/4</i>	It means LAN interface.

	2=LAN2 3=LAN3 4=LAN4
<i>count</i>	Choose the following number for specifying different node type. 1= B-node 2= P-node 4= M-node 8= H-node 0= Not specify any type for node.

Example

```
> msubnet nodetype ?
% msubnet nodetype <2/3/4> <count>
% Now: LAN2 0; LAN3 0; LAN4 0

% count: 1. B-node 2. P-node 4. M-node 8. H-node

> msubnet nodetype 2 1
% Set LAN2 Dhcp Node Type done !!!

> msubnet nodetype ?
% msubnet nodetype <2/3/4> <count>
% Now: LAN2 1; LAN3 0; LAN4 0

% count: 1. B-node 2. P-node 4. M-node 8. H-node
```

Telnet Command: msubnet primWINS

This command is used to configure primary WINS server.

msubnet primWINS *[2/3/4]* *[WINS IP]*

Syntax Description

Parameter	Description
<i>2/3/4</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<i>WINS IP</i>	Enter the IP address as the WINS IP.

Example

```
>> msubnet primWINS ?
% msubnet primWINS <2/3/4> <WINS IP>
% Now: LAN2 0.0.0.0; LAN3 0.0.0.0; LAN4 0.0.0.0
> msubnet primWINS 2 192.168.3.5
% Set LAN2 Dhcp Primary WINS IP done !!!

> msubnet primWINS ?
% msubnet primWINS <2/3/4> <WINS IP>
% Now: LAN2 192.168.3.5; LAN3 0.0.0.0; LAN4 0.0.0.0
```

Telnet Command: msubnet secWINS

This command is used to configure secondary WINS server.

```
msubnet secWINS [2/3/4] [WINS IP]
```

Syntax Description

Parameter	Description
2/3/4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
WINS IP	Enter the IP address as the WINS IP.

Example

```
> > msubnet secWINS 2 192.168.3.89
% Set LAN2 Dhcp Secondary WINS IP done !!!

> msubnet secWINS ?
% msubnet secWINS <2/3/4> <WINS IP>
% Now: LAN2 192.168.3.89; LAN3 0.0.0.0; LAN4 0.0.0.0
```

Telnet Command: msubnet tftp

This command is used to set TFTP server for multi-subnet.

`msubnet tftp [2/3/4] [TFTP server name]`

Syntax Description

Parameter	Description
<i>2/3/4/5/6</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<i>TFTP server name</i>	Type a name to indicate the TFTP server.

Example

```
> msubnet tftp ?
% msubnet tftp <2/3/4> <TFTP server name>
% Now: LAN2
      LAN3
      LAN4

> msubnet tftp 2 publish
% Set LAN2 TFTP Server Name done !!!

> msubnet tftp ?
% msubnet tftp <2/3/4> <TFTP server name>
% Now: LAN2 publish
      LAN3
      LAN4
```

Telnet Command: msubnet mtu

This command allows you to configure MTU value for LAN/IP Routed Subnet.

`msubnet mtu [interface][value]`

Syntax Description

Parameter	Description
<i>interface</i>	Available settings include LAN1-LAN4, IP_Routed_Subnet.
<i>value</i>	1000 ~ 1508 (Bytes), default: 1500 (Bytes)

Example

```
> msubnet mtu LAN1 1492%
Set LAN1 subnet mtu as 1492
> msubnet mtu ?
Usage:

>msubnet mtu <interface> <value>

<interface>: LAN1~LAN4,IP_Routed_Subnet, <value>: 1000 ~ 1496
(Bytes), de
```

```

fault: 1500 (Bytes)

e.x: >msubnet mtu LAN1 1492

Current Settings:

LAN1 MTU:          1492 (Bytes)
LAN2 MTU:          1500 (Bytes)
LAN3 MTU:          1500 (Bytes)
LAN4 MTU:          1500 (Bytes)
IP Routed Subnet MTU: 1500 (Bytes)

```

Telnet Command: object ip obj

This command is used to create an IP object profile.

`object ip obj setdefault`

`object ip obj INDEX -v`

`object ip obj INDEX -n NAME`

`object ip obj INDEX -i INTERFACE`

`object ip obj INDEX -s INVERT`

`object ip obj INDEX -a TYPE [START_IP] [END/MASK_IP]`

Syntax Description

Parameter	Description
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number of the specified object profile.
<i>-v</i>	It means to view the information of the specified object profile. Example: <code>object ip obj 1 -v</code>
<i>-n NAME</i>	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: <code>object ip obj 9 -n bruce</code>
<i>-i INTERFACE</i>	It means to define an interface for the IP object. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=3, means WAN Example: <code>object ip obj 8 -i 0</code>
<i>-s INVERT</i>	It means to set invert selection for the object profile. INVERT=0, means disabling the function. INVERT=1, means enabling the function. Example: <code>object ip obj 3 -s 1</code>
<i>-a TYPE</i>	It means to set the address type and IP for the IP object profile. TYPE=0, means Mask TYPE=1, means Single TYPE=2, means Any TYPE=3, means Rang Example: <code>object ip obj 3 -a 2</code>
<i>[START_IP]</i>	When the TYPE is set with 2, you have to type an IP address as a

	starting point and another IP address as end point. Type an IP address.
[END/MASK_IP]	Type an IP address (different with START_IP) as the end IP address.

Example

```
> object ip obj 1 -n marketing
> object ip obj 1 -a 1 192.168.1.45
> object ip obj 1 -v
IP Object Profile 1
Name      :[marketing]
Interface:[Any]
Address type:[single]
Start ip address:[192.168.1.45]
End/Mask ip address:[0.0.0.0]
Invert Selection:[0]
```

Telnet Command: object ip grp

This command is used to integrate several IP objects under an IP group profile.

object ip grp setdefault

object ip grp *INDEX* -v

object ip grp *INDEX* -n *NAME*

object ip grp *INDEX* -i *INTERFACE*

object ip grp *INDEX* -a *IP_OBJ_INDEX*

Syntax Description

Parameter	Description
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number of the specified group profile.
-v	It means to view the information of the specified group profile. Example: <i>object ip grp 1 -v</i>
-n <i>NAME</i>	It means to define a name for the IP group. NAME: Type a name with less than 15 characters. Example: <i>object ip grp 8 -n bruce</i>
-i <i>INTERFACE</i>	It means to define an interface for the IP group. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=2, means WAN Example: <i>object ip grp 3 -i 0</i>
-a <i>IP_OBJ_INDEX</i>	It means to specify IP object profiles for the group profile. Example: <i>:object ip grp 3 -a 1 2 3 4 5</i> The IP object profiles with index number 1,2,3,4 and 5 will be group under such profile.

Example

```
> object ip grp 2 -n First
IP Group Profile 2
Name      :[First]
```



```
Interface:[Any]
Included ip object index:
[0:][0]
[1:][0]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]

> object ip grp 2 -i 1
> object ip grp 2 -a 1 2
IP Group Profile 2
Name   :[First]
Interface:[Lan]
Included ip object index:
[0:][1]
[1:][2]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]
```

Telnet Command: object ipv6 obj

This command is used to create an IP object profile.

```
object ip obj setdefault
```

```
object ip obj INDEX -v
```

```
object ip obj INDEX -n NAME
```

```
object ip obj INDEX -i INTERFACE
```

```
object ip obj INDEX -s INVERT
```

```
object ip obj INDEX -a TYPE [START_IP] [END/MASK_IP]
```

Syntax Description

Parameter	Description
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number of the specified object profile.
<i>-v</i>	It means to view the information of the specified object profile. Example: <i>object ip obj 1 -v</i>
<i>-n NAME</i>	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: <i>object ip obj 9 -n bruce</i>
<i>-i INTERFACE</i>	It means to define an interface for the IP object. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=3, means WAN Example: <i>object ip obj 8 -i 0</i>
<i>-s INVERT</i>	It means to set invert selection for the object profile. INVERT=0, means disabling the function. INVERT=1, means enabling the function. Example: <i>object ip obj 3 -s 1</i>
<i>-a TYPE</i>	It means to set the address type and IP for the IP object profile. TYPE=0, means Mask TYPE=1, means Single TYPE=2, means Any TYPE=3, means Rang Example: <i>object ip obj 3 -a 2</i>
<i>[START_IP]</i>	When the TYPE is set with 2, you have to type an IP address as a starting point and another IP address as end point. Type an IP address.
<i>[END/MASK_IP]</i>	Type an IP address (different with START_IP) as the end IP address.

Example

```
> object ip obj 1 -n marketing
> object ip obj 1 -a 1 192.168.1.45
> object ip obj 1 -v
IP Object Profile 1
Name      :[marketing]
Interface:[Any]
Address type:[single]
```

```

Start ip address:[192.168.1.45]
End/Mask ip address:[0.0.0.0]
Invert Selection:[0]

```

Telnet Command: object ipv6 grp

This command is used to integrate several IP objects under an IP group profile.

object ip grp setdefault

object ip grp *INDEX* -v

object ip grp *INDEX* -n *NAME*

object ip grp *INDEX* -i *INTERFACE*

object ip grp *INDEX* -a *IP_OBJ_INDEX*

Syntax Description

Parameter	Description
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number of the specified group profile.
-v	It means to view the information of the specified group profile. Example: <i>object ip grp 1 -v</i>
-n <i>NAME</i>	It means to define a name for the IP group. NAME: Type a name with less than 15 characters. Example: <i>object ip grp 8 -n bruce</i>
-i <i>INTERFACE</i>	It means to define an interface for the IP group. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=2, means WAN Example: <i>object ip grp 3 -i 0</i>
-a <i>IP_OBJ_INDEX</i>	It means to specify IP object profiles for the group profile. Example: <i>:object ip grp 3 -a 1 2 3 4 5</i> The IP object profiles with index number 1,2,3,4 and 5 will be group under such profile.

Example

```

> object ip grp 2 -n First
IP Group Profile 2
Name      :[First]
Interface:[Any]
Included ip object index:
[0:][0]
[1:][0]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]

> object ip grp 2 -i 1
> object ip grp 2 -a 1 2

```

```

IP Group Profile 2
Name      :[First]
Interface:[Lan]
Included ip object index:
[0:][1]
[1:][2]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]

```

Telnet Command: object service obj

This command is used to create service object profile.

`object service obj setdefault`

`object service obj INDEX -v`

`object service obj INDEX -n NAME`

`object service obj INDEX -p PROTOCOL`

`object service obj INDEX -s CHK [START_P] [END_P]`

`object service obj INDEX -d CHK [START_P] [END_P]`

Syntax Description

Parameter	Description
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number of the specified service object profile.
<i>-v</i>	It means to view the information of the specified service object profile. Example: <i>object service obj 1 -v</i>
<i>-n NAME</i>	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: <i>object service obj 9 -n bruce</i>
<i>-i PROTOCOL</i>	It means to define a PROTOCOL for the service object profile. PROTOCOL =0, means any PROTOCOL =1, means ICMP PROTOCOL =2, means IGMP PROTOCOL =6, means TCP PROTOCOL =17, means UDP PROTOCOL =255, means TCP/UDP Other values mean other protocols. Example: <i>object service obj 8 -i 0</i>
<i>CHK</i>	It means the check action for the port setting. 0=equal(=), when the starting port and ending port values are the same, it indicates one port; when the starting port and ending port values are different, it indicates a range for the port and available for this service type. 1=not equal(!=), when the starting port and ending port values are the same, it indicates all the ports except the port defined here; when the starting port and ending port values are different, it indicates that all the ports except the range defined here are

	available for this service type. 2=larger(>), the port number greater than this value is available.. 3=less(<), the port number less than this value is available for this profile.
<code>-s CHK [START_P] [END_P]</code>	It means to set source port check and configure port range (1-65565) for TCP/UDP. END_P, type a port number to indicate source port. Example: <code>object service obj 3 -s 0 100 200</code>
<code>-d CHK [START_P] [END_P]</code>	It means to set destination port check and configure port range (1-65565) for TCP/UDP. END_P, type a port number to indicate destination port. Example: <code>object service obj 3 -d 1 100 200</code>

Example

```
> object service obj 1 -n limit
> object service obj 1 -p 255
> object service obj 1 -s 1 120 240
> object service obj 1 -d 1 200 220
> object service obj 1 -v
Service Object Profile 1
Name      :[limit]
Protocol  :[255]
Source port check action:[!=]
Source port range:[120~240]
Destination port check action:[!=]
Destination port range:[200~220]
```

Telnet Command: object service grp

This command is used to integrate several service objects under a service group profile.

`object service grp setdefault`

`object service grp INDEX -v`

`object service grp INDEX -n NAME`

`object service grp INDEX -a SER_OBJ_INDEX`

Syntax Description

Parameter	Description
<code>setdefault</code>	It means to return to default settings for all profiles.
<code>INDEX</code>	It means the index number of the specified group profile.
<code>-v</code>	It means to view the information of the specified group profile. Example: <code>object service grp 1 -v</code>
<code>-n NAME</code>	It means to define a name for the service group. NAME: Type a name with less than 15 characters. Example: <code>object service grp 8 -n bruce</code>
<code>-a SER_OBJ_INDEX</code>	It means to specify service object profiles for the group profile. Example: <code>:object service grp 3 -a 1 2 3 4 5</code> The service object profiles with index number 1,2,3,4 and 5 will be group under such profile.

Example

```
>object service grp 1 -n Grope_1
Service Group Profile 1
Name   :[Grope_1]
Included service object index:
[0:][0]
[1:][0]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]

> object service grp 1 -a 1 2
Service Group Profile 1
Name   :[Grope_1]
Included service object index:
[0:][1]
[1:][2]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]
```

Telnet Command: object kw

This command is used to create keyword profile.

object kw obj setdefault

object kw obj show PAGE

object kw obj INDEX -v

object kw obj INDEX -n NAME

object kw obj INDEX -a CONTENTS

Syntax Description

Parameter	Description
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>show PAGE</i>	It means to show the contents of the specified profile. PAGE: Enter the page number.
<i>show</i>	It means to show the contents for all of the profiles.
<i>INDEX</i>	It means the index number of the specified keyword profile.
<i>-v</i>	It means to view the information of the specified keyword profile.
<i>-n NAME</i>	It means to define a name for the keyword profile. NAME: Type a name with less than 15 characters.
<i>-a CONTENTS</i>	It means to set the contents for the keyword profile. Example: <i>object kw obj 40 -a test</i>

Example

```
> object kw obj 1 -n children
Profile 1
Name   :[children]
Content:[]
> object kw obj 1 -a gambling
Profile 1
Name   :[children]
Content:[gambling]

> object kw obj 1 -v
Profile 1
Name   :[children]
Content:[gambling]
```

Telnet Command: object fe

This command is used to create File Extension Object profile.

`object fe show`

`object fe setdefault`

`object fe obj INDEX -v`

`object fe obj INDEX -n NAME`

`object fe obj INDEX -e CATEGORY/FILE_EXTENSION`

`object fe obj INDEX -d CATEGORY/FILE_EXTENSION`

Syntax Description

Parameter	Description
<i>show</i>	It means to show the contents for all of the profiles.
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number (from 1 to 8) of the specified file extension object profile.
<i>-v</i>	It means to view the information of the specified file extension object profile.
<i>-n NAME</i>	It means to define a name for the file extension object profile. NAME: Type a name with less than 15 characters.
<i>-e</i>	It means to enable the specific CATEGORY or FILE_EXTENSION.
<i>-d</i>	It means to disable the specific CATEGORY or FILE_EXTENSION
<i>CATEGORY/FILE_EXTENSION</i>	CATEGORY: Image, Video, Audio, Java, ActiveX, Compression, Execution Example: <code>object fe obj 1 -e Image</code> FILE_EXTENSION: ".bmp", ".dib", ".gif", ".jpeg", ".jpg", ".jpg2", ".jp2", ".pct", ".pcx", ".pic", ".pict", ".png", ".tif", ".tiff", ".asf", ".avi", ".mov", ".mpe", ".mpeg", ".mpg", ".mp4", ".qt", ".rm", ".wmv", ".3gp", ".3gpp", ".3gpp2", ".3g2", ".aac", ".aiff", ".au", ".mp3", ".m4a", ".m4p", ".ogg", ".ra", ".ram", ".vox", ".wav", ".wma", ".class", ".jad", ".jar", ".jav", ".java", ".jcm", ".js", ".jse", ".jsp", ".jtk", ".alx", ".apb", ".axs", ".ocx", ".olb", ".ole",

```
".tlb", ".viv", ".vrm", ".ace", ".arj", ".bzip2", ".bz2", ".cab",  
".gz", ".gzip", ".rar", ".sit", ".zip", ".bas", ".bat", ".com",  
".exe", ".inf", ".pif", ".reg", ".scr"  
Example: object fe obj 1 -e .bmp
```

Example

```
> object fe obj 1 -n music  
> object fe obj 1 -e Audio  
> object fe obj 1 -v  
Profile Index: 1  
Profile Name:[music]  
  
-----  
-----  
Image category:  
[ ].bmp [ ].dib [ ].gif [ ].jpeg [ ].jpg [ ].jpg2 [ ].jp2 [ ].pct  
[ ].pcx [ ].pic [ ].pict [ ].png [ ].tif [ ].tiff  
-----  
-----  
Video category:  
[ ].asf [ ].avi [ ].mov [ ].mpe [ ].mpeg [ ].mpg [v].mp4 [ ].qt  
[ ].rm [v].wmv [ ].3gp [ ].3gpp [ ].3gpp2 [ ].3g2  
-----  
-----  
Audio category:  
[v].aac [v].aiff [v].au [v].mp3 [v].m4a [v].m4p [v].ogg [v].ra  
[v].ram [v].vox [v].wav [v].wma  
-----  
-----  
Java category:  
[ ].class [ ].jad [ ].jar [ ].jav [ ].java [ ].jcm [ ].js [ ].jse  
[ ].jsp [ ].jtk  
-----  
-----  
ActiveX category:  
[ ].alx [ ].apb [ ].axs [ ].ocx [ ].olb [ ].ole [ ].tlb [ ].viv  
[ ].vrm  
-----  
-----  
Compression category:  
[ ].ace [ ].arj [ ].bzip2 [ ].bz2 [ ].cab [ ].gz [ ].gzip [ ].rar  
[ ].sit [ ].zip  
-----  
-----  
Execution category:  
[ ].bas [ ].bat [ ].com [ ].exe [ ].inf [ ].pif [ ].reg [ ].scr
```


Telnet Command: port

This command allows users to set the speed for specific port of the router.

Syntax

port [1, 2, 3, 4, wan2, all] [AN, 1000F, 100F, 100H, 10F, 10H, status]

port [enable, disable][1, 2, 3, 4, all]

port status

port sniff [on, off, port, txrx, restart, status]

port 802.1x[enable, disable, status, addport, delport]

port jumbo

port wanfc

Syntax Description

Parameter	Description
1, 2, 3, 4, 5, 6, wan2, all	It means the number of LAN port and WAN port.
AN... 10H	It means the physical type for the specific port. AN: auto-negotiate. 100F: 100M Full Duplex. 100H: 100M Half Duplex. 10F: 10M Full Duplex. 10H: 10M Half Duplex.
status	It means to view the Ethernet port status.
sniff [on, off, port, txrx, restart, status]	Set the LAN Port Mirror function. On: Enable the function. Off: Disable the function. Port: Set the mirror port. E.g., port sniff p1 TXRX: Set the port number to be mirrored for transmitting/receiving the packets. E.g., port sniff txrx p2 p3 Restart: After finished the setting, use such command to activate port mirror function. Status: Display the status of LAN port mirror.
802.1x[enable, disable, status, addport, delport]	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. enable: Enable the function. disable: Disable the function. Status: Display the status of 802.1x configuration. Addport: Set the interface (LAN port 1 ~ 4) for applying 802.1x. E.g., 802.1x addport 1 Delport: Delete the interface (LAN port 1-4) with 802.1x applied. E.g., 802.1x delport 1
wanfc	It means to set WAN flow control.

Example

```
> port 1 100F
%Set Port 1 Force speed 100 Full duplex OK !!!
```

Telnet Command: portmuptime

This command allows you to set a time of keeping the session connection for specified protocol.

```
portmuptime [-<command> <parameter> | ... ]
```

Syntax Description

Parameter	Description
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-t <sec>	It means "TCP" protocol. <sec>: Type a number to set the TCP session timeout.
-u <sec>	It means "UDP" protocol. <sec>: Type a number to set the UDP session timeout.
-i <sec>	It means "IGMP" protocol. <sec>: Type a number to set the IGMP session timeout.
-w <sec>	It means "TCP WWW" protocol. <sec>: Type a number to set the TCP WWW session timeout.
-s <sec>	It means "TCP SYN" protocol. <sec>: Type a number to set the TCP SYN session timeout.
-f	It means to flush all portmaps (useful for diagnostics).
-l <List>	List all settings.

Example

```
> portmuptime -t 86400 -u 300 -i 10
> portmuptime -l
----- Current setting -----
TCP Timeout      : 86400 sec.
UDP Timeout      : 300 sec.
IGMP Timeout     : 10 sec.
TCP WWW Timeout  : 60 sec.
TCP SYN Timeout  : 60 sec.
```

Telnet Command: ppa

This command allows you to configure PPA mode.

```
ppa [-<command> <parameter> | ... ]
```

```
ppa n [-<command> <parameter> | ... ]
```

Syntax Description

Parameter	Description
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-m <mode>	Specify a mode. 1=auto 2=manual(traffic) 3=manual(qos)

	4>manual(specific hosts) 0=disable
<i>-p <proto></i>	Specify a protocol. proto - 1-TCP; 2-UDP; 3-Both.
<i>-b 1/0</i>	Enable/disable TWO-way hardware acceleration.
<i>-M enable/disable</i>	Enable/disable the multicast hardware acceleration.
<i>-v</i>	Show PPA_WAN_Table and PPA_LAN_Table for reference.
<i>-c</i>	Clean all settings.
ppa n - used in QoS or specific host	
<i>-l <rule></i>	Specify an index number of rule profile for QoS mode.
<i>-h <host></i>	Type an IP address for Specific Host mode.
<i>-s <start port></i>	Specify a starting port number for Specific Host mode.
<i>-e <end port></i>	Specify an ending port number for Specific Host mode

Example

```

> ppa -m 1 -p 1 -b 0
Set ok! The PPA mode is Auto

% You need to set the Manual mode first !

%TWO way accleration is disable

> ppa -v
% PPA mode is Auto
%PPA Protocol TCP 1, UDP 0
%PPA two way disable
%PPA time is 10
%PPA range is 192
%PPA LAN entries 0
%PPA WAN entries 0

```

Telnet Command: prn

This command allows you to view current status (interface and driver) of USB printer.

prn status

prn debug

Example

```

> prn status
Interface: USB bus 2.0
Printer: NotReady

> prn debug
conn[0] :
none
conn[1] :
none

```

```

conn[2] :
none
conn[3] :
none
LPD_data_total=0

usb1p_ptr=0
UsbPrintReady=0, UsbIsPrinting=0

```

Telnet Command: qos setup

This command allows user to set general settings for QoS.

Syntax

qos setup [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-h	Type it to display the usage of this command.
-m <mode>	It means to define which traffic the QoS control settings will apply to and enable QoS control. 0: disable. 1: in, apply to incoming traffic only. 2: out, apply to outgoing traffic only. 3: both, apply to both incoming and outgoing traffic. Default is enable (for outgoing traffic).
-i <bandwidth>	It means to set inbound bandwidth in kbps (Ethernet WAN only) The available setting is from 1 to 100000.
-o <bandwidth>	It means to set outbound bandwidth in kbps (Ethernet WAN only). The available setting is from 1 to 100000.
-r <index:ratio>	It means to set ratio for class index, in %.
-u <mode>	It means to enable bandwidth control for UDP. 0: disable 1: enable Default is disable.
-p <ratio>	It means to enable bandwidth limit ratio for UDP.
-t <mode>	It means to enable/disable Outbound TCP ACK Prioritize. 0: disable 1: enable
-V	Show all the settings.
-D	Set all to factory default (for all WANs).
[...]	It means that you can type in several commands in one line.

Example

```

> qos setup -W 2 -m 3 -i 9500 -o 8500 -r 3:20 -u 1 -p 50 -t 1

Setup WAN2 !!!!

```

```
WAN2 QoS mode is both
inbound bandwidth set to 9500
outbound bandwidth set to 8500
WAN2 class 3 ratio set to 20
WAN2 udp bandwidth control set to enable
WAN2 udp bandwidth limit ratio set to 50
WAN2 Outbound TCP ACK Prioritizel set to enable
QoS WAN2 set complete; restart QoS
>
```

Telnet Command: qos class

This command allows user to set QoS class.

Syntax

qos class -c [*no*] [-*a|e|d*] [*no*][-<command> <parameter> | ...]

Syntax Description

Parameter	Description
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-h	Type it to display the usage of this command.
-c <no>	Specify the inde number for the class. Available value for <no> contains 1, 2 and 3. The default setting is class 1.
-n <name>	It means to type a name for the class.
-a	It means to add rule for specified class.
-e <no>	It means to edit specified rule. <no>: Enter the index number for the rule.
-d <no>	It means to delete specified rule. <no>: Enter the index number for the rule.
-m <mode>	It means to enable or disable the specified rule. 0: disable, 1: enable
-l <addr>	Set the local address. <i>Addr1</i> - It means Single address. Please specify the IP address directly, for example, "-l 172.16.3.9". <i>addr1:addr2</i> - It means Range address. Please specify the IP addresses, for example, "-l 172.16.3.9: 172.16.3.50." <i>addr1:subnet</i> - It means the subnet address with start IP address. Please Enter the subnet and the IP address, for example, "-l 172.16.3.9:255.255.0.0".0 <i>any</i> - It means Any address. Simple type "-l" to specify any address for this command.
-r <addr>	Set the remote address. <i>addr1</i> - It means Single address. Please specify the IP address directly, for example, "-l 172.16.3.9". <i>addr1:addr2</i> - It means Range address. Please specify the IP addresses, for example, "-l 172.16.3.9: 172.16.3.50." <i>addr1:subnet</i> - It means the subnet address with start IP address. Please Enter the subnet and the IP address, for example, "-l 172.16.3.9:255.255.0.0".0 <i>any</i> - It means Any address. Simple type "-l" to specify any address for this command.
-p <DSCP id>	Specify the ID.
-s <Service type>	Specify the service type by typing the number. The available types are listed as below: 1:ANY 2:DNS 3:FTP 4:GRE 5:H.323 6:HTTP 7:HTTPS 8:IKE 9:IPSEC-AH 10:IPSEC-ESP 11:IRC 12:L2TP 13:NEWS 14:NFS 15:NNTP 16:PING 17:POP3 18:PPTP 19:REAL-AUDIO 20:RTSP 21:SFTP 22:SIP 23:SMTP 24:SNMP 25:SNMP-TRAPS 26:SQL-NET 27:SSH 28:SYSLOG 29:TELNET 30:TFTP

<code>-u <Service type></code>	Set a number to make user defined service type. Available number is: 1 ~ 40.
<code>-S <d/s></code>	Show the content for specified DSCP ID/Service type.
<code>-V <1/2/3></code>	Show the rule in the specified class.
<code>[..]</code>	It means that you can type in several commands in one line.

Example

```
> qos class -c 2 -n draytek -a -m 1 -l 192.168.1.50:192.168.1.80
```

Following setting will set in the class2

class 2 name set to draytek

Add a rule in class2

Class2 the 1 rule enabled

Set local address type to Range, 192.168.1.50:192.168.1.80

Telnet Command: qos type

This command allows user to configure protocol type and port number for QoS.

Syntax

`qos type [-a <service name> | -e <no> | -d <no>].`

Syntax Description

Parameter	Description
<code>-a <name></code>	It means to add rule.
<code>-e <no></code>	It means to edit user defined service type. "no" means the index number. Available numbers are 1-40.
<code>-d <no></code>	It means to delete user defined service type. "no" means the index number. Available numbers are 1-40.
<code>-n <name></code>	It means the name of the service.
<code>-t <type></code>	It means protocol type. 6: tcp(default) 17: udp 0: tcp/udp <1-254>: other
<code>-p <port></code>	It means service port. The typing format must be [start:end] (ex., 510:330).
<code>-l</code>	List user defined types. "no" means the index number. Available numbers are 1-40.

Example

```
> qos type -a draytek -t 6 -p 510:1330

service name set to draytek
service type set to 6:TCP
Port type set to Range
Service Port set to 510 ~ 1330
>
```

Telnet Command: qos voip

This command allows user to enable or disable the QoS for VoIP and RTP.

Syntax

qos voip [on/off]

Syntax Description

Parameter	Description
on/off	On - Enable the QoS for VoIP. Off - Disable th QoS for VoIP.

Example

```
> qos voip off
QoS for VoIP: Disable; SIP Port: 5060
```

Telnet Command: quit

This command can exit the telnet command screen.

Telnet Command: show lan

This command displays current status of LAN IP address settings.

Example

```
> show lan
The LAN settings:
Status  IP           Mask           DHCP Start IP  Pool Gateway
-----
[V]LAN1 192.168.1.1   255.255.255.0 V   192.168.1.10   200
192.168.1.1

[X]LAN2 192.168.2.1   255.255.255.0 V   192.168.2.90   100
192.168.2.1

[X]LAN3 192.168.3.1   255.255.255.0 V   192.168.3.10   100
192.168.3.1

[X]LAN4 192.168.4.1   255.255.255.0 V   192.168.4.10   100
192.168.4.1

[X]Route 192.168.0.1   255.255.255.0 V   0.0.0.0         0   192.168.0.1
```


Telnet Command: show dmz

This command displays current status of DMZ host.

Example

```
> show dmz
%      WAN1 DMZ mapping status:
Index  Status  WAN1 aux IP    Private IP
-----
1      Disable 0.0.0.0

%      WAN2 DMZ mapping status:
Index  Status  WAN2 aux IP    Private IP
-----
1      Disable 0.0.0.0

%      WAN3 DMZ mapping status:
Index  Status  WAN3 aux IP    Private IP
-----
1      Disable 0.0.0.0

%      WAN4 DMZ mapping status:
Index  Status  WAN4 aux IP    Private IP
-----
1      Disable 0.0.0.0
```

Telnet Command: show dns

This command displays current status of DNS setting

Example

```
> show dns
%%      Domain name server settings:
% LAN1 Primary DNS: [Not set]
% LAN1 Secondary DNS: [Not set]

% LAN2 Primary DNS: [Not set]
% LAN2 Secondary DNS: [Not set]

% LAN3 Primary DNS: [Not set]
% LAN3 Secondary DNS: [Not set]

% LAN4 Primary DNS: [Not set]
% LAN4 Secondary DNS: [Not set]
```

Telnet Command: show openport

This command displays current status of open port setting.

Example

```
> show openport
```

```

%%      Openport settings:
Index   Status  Comment           Local IP Address
*****
                        No data entry.

```

Telnet Command: show nat

This command displays current status of NAT.

Example

```

> show nat
Port Redirection Running Table:

Index  Protocol  Public Port  Private IP      Private Port
-----
1      0          0           0.0.0.0         0
2      0          0           0.0.0.0         0
3      0          0           0.0.0.0         0
4      0          0           0.0.0.0         0
5      0          0           0.0.0.0         0
6      0          0           0.0.0.0         0
7      0          0           0.0.0.0         0
8      0          0           0.0.0.0         0
9      0          0           0.0.0.0         0
10     0          0           0.0.0.0         0
11     0          0           0.0.0.0         0
12     0          0           0.0.0.0         0
13     0          0           0.0.0.0         0
14     0          0           0.0.0.0         0
15     0          0           0.0.0.0         0
16     0          0           0.0.0.0         0
17     0          0           0.0.0.0         0
18     0          0           0.0.0.0         0
19     0          0           0.0.0.0         0
20     0          0           0.0.0.0         0
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]

```

Telnet Command: show portmap

This command displays the table of NAT Active Sessions.

Example

```

> show portmap
-----
-
Private_IP:Port Pseudo_IP:Port Peer_IP:Port [Timeout/Protocol/Flag]
-----
-

```

Telnet Command: show pmtime

This command displays the reuse time of NAT session.

Level0: It is the default setting.

Level1: It will be applied when the NAT sessions are smaller than 25% of the default setting.

Level2: It will be applied when the NAT sessions are smaller than the eighth of the default setting.

Example

```
> show pmtime
Level0 TCP=86400001 UDP=300001 ICMP=10001
Level1 TCP=600000 UDP=90000 ICMP=7000
Level2 TCP=60000 UDP=30000 ICMP=5000
```

Telnet Command: show session

This command displays current status of current session.

Example

```
> show session
% Maximum Session Number: 50000
% Maximum Session Usage: 0
% Current Session Usage: 0
% Current Session Used(include waiting for free): 0
% WAN1 Current Session Usage: 0
% WAN2 Current Session Usage: 0
% WAN3 Current Session Usage: 0
% WAN4 Current Session Usage: 0
>
```

Telnet Command: show status

This command displays current status of LAN and WAN connections.

Example

```
> show status
System Uptime:1:4:49
LAN Status
Primary DNS:8.8.8.8      Secondary DNS:8.8.4.4
IP Address:192.168.1.1   Tx Rate:3266   Rx Rate:2245

WAN 1 Status: Disconnected
Enable:Yes      Line:xDSL      Name:
Mode:PPPoE      Up Time:0:00:00   IP:---      GW IP:---
TX Packets:0    TX Rate:0    RX Packets:0    RX Rate:0

WAN 2 Status: Disconnected
Enable:Yes      Line:Ethernet   Name:
Mode:---        Up Time:0:00:00   IP:---      GW IP:---
TX Packets:0    TX Rate:0    RX Packets:0    RX Rate:0

WAN 3 Status: Disconnected
Enable:Yes      Line:USB        Name:
Mode:---        Up Time:0:00:00   IP:---      GW IP:---
TX Packets:0    TX Rate:0    RX Packets:0    RX Rate:0

WAN 4 Status: Disconnected
```

```

Enable:Yes      Line:USB      Name:
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---

```

Telnet Command: show adsl

This command displays current status of ADSL.

Example

```

> show adsl
----- ATU-R Info (hw: annex A, f/w: annex A) -----
Running Mode      :          State          : TRAINING
DS Actual Rate    :          0 bps    US Actual Rate      :          0 bps
DS Attainable Rate :          0 bps    US Attainable Rate  :          0 bps
DS Path Mode      :          Fast    US Path Mode        :          Fast
DS Interleave Depth :          0    US Interleave Depth :          0
NE Current Attenuation :          0 dB    Cur SNR Margin      :          0 dB
DS actual PSD     :          0.0 dB    US actual PSD       :          0.0 dB
NE Rcvd Cells     :          0    NE Xmitted Cells    :          0
NE CRC Count      :          0    FE CRC Count        :          0
NE ES Count       :          0    FE ES Count         :          0
Xdsl Reset Times  :          0    Xdsl Link Times     :          0
ITU Version[0]    : b5004946    ITU Version[1]      : 544e0000
ADSL Firmware Version : 06-06-01-07-00-01
Power Management Mode : DSL_G997_PMS_NA
Test Mode         : DISABLE
----- ATU-C Info -----
Far Current Attenuation :          0 dB    Far SNR Margin      :          0 dB
CO ITU Version[0]      : 00000000    CO ITU Version[1]  : 00000000
DSLAM CHIPSET VENDOR  : < ----- >
>

```

Telnet Command: show statistic

This command displays statistics for WAN interface.

Syntax

show statistic

show statistic reset *[interface]*

Syntax Description

Parameter	Description
<i>reset</i>	It means to reset the transmitted/received bytes to Zero.
<i>interface</i>	It means to specify WAN1 -WAN5 interface for displaying related statistics.

Example

```

> show statistic
WAN1 total TX: 0 Bytes ,RX: 0 Bytes
WAN2 total TX: 0 Bytes ,RX: 0 Bytes
WAN3 total TX: 0 Bytes ,RX: 0 Bytes
WAN4 total TX: 0 Bytes ,RX: 0 Bytes
WAN5 total TX: 0 Bytes ,RX: 0 Bytes
WAN6 total TX: 0 Bytes ,RX: 0 Bytes
WAN7 total TX: 0 Bytes ,RX: 0 Bytes

```

```
> show statistic reset wan1
Reset WAN1 tx/rx Bytes to zero
>
```

Telnet Command: smb setting

This command is used to configure file sharing settings for SMB server.

Syntax

```
smb setting [enable/disable]
smb setting show status
smb setting set workgroup [Workgroup name]
smb setting set host [host name]
smb setting set access [LAN or LANWAN]
```

Syntax Description

Parameter	Description
<i>enable/disable</i>	Enable or disable the SMB service.
<i>show status</i>	Display current status of SMB service.
<i>Set workgroup [Workgroup name]</i>	Set a name of workgroup for SMB service.
<i>set host [host name]</i>	Set a name of the host for SMB service.
<i>set access [LAN or LANWAN]</i>	Allow to access into SMB server by LAN or borth LA N and WAN.

Example

```
> smb setting enable
SMB service is enabled.

> smb setting set access LAN
Allow SMB access from LAN only.
>
```

Telnet Command: srv dhcp badip

This command is reserved for future using.

```
srv dhcp badip
```

Example

```
> srv dhcp badip
>
```

Telnet Command: srv dhcp public

This command allows users to configure DHCP server for second subnet.

```
srv dhcp public start [IP address]
srv dhcp public cnt [IP counts]
srv dhcp public status
srv dhcp public add [MAC Addr XX-XX-XX-XX-XX-XX]
srv dhcp public del [MAC Addr XX-XX-XX-XX-XX-XX/all/ALL]
```

Syntax Description

Parameter	Description
<i>start</i>	It means the starting point of the IP address pool for the DHCP server.
<i>IP address</i>	It means to specify an IP address as the starting point in the IP address pool.
<i>cnt</i>	It means the IP count number.
<i>IP counts</i>	It means to specify the number of IP addresses in the pool. The maximum is 10.
<i>status</i>	It means the execution result of this command.
<i>add</i>	It means creating a list of hosts to be assigned.
<i>del</i>	It means removing the selected MAC address.
<i>MAC Addr</i>	It means to specify MAC Address of the host.
<i>all/ALL</i>	It means all of the MAC addresses.

Example

```
Vigor> ip route add 192.168.1.56 255.255.255.0 192.168.1.12 3 default
Vigor> srv dhcp public status
Index   MAC Address
```

Telnet Command: `srv dhcp dns1`

This command allows users to set Primary IP Address for DNS Server in LAN.

```
srv dhcp dns1 [?]
```

```
srv dhcp dns1 [DNS IP address]
```

Syntax Description

Parameter	Description
<i>?</i>	It means to display current IP address of DNS 1 for the DHCP server.
<i>DNS IP address</i>	It means the IP address that you want to use as DNS1. Note: The IP Routed Subnet DNS must be the same as NAT Subnet DNS).

Example

```
> srv dhcp dns1 168.95.1.1
% srv dhcp dns1 <DNS IP address>
% Now: 168.95.1.1
(IP Routed Subnet dns same as NAT Subnet dns)
```

Telnet Command: `srv dhcp dns2`

This command allows users to set Secondary IP Address for DNS Server in LAN.

```
srv dhcp dns2 [?]
```

```
srv dhcp dns2 [DNS IP address]
```

Syntax Description

Parameter	Description
-----------	-------------

?	It means to display current IP address of DNS 2 for the DHCP server.
<i>DNS IP address</i>	It means the IP address that you want to use as DNS2. Note: The IP Routed Subnet DNS must be the same as NAT Subnet DNS).

Example

```
> srv dhcp dns2 10.1.1.1
% srv dhcp dns2 <DNS IP address>
% Now: 10.1.1.1
(IP Routed Subnet dns same as NAT Subnet dns)
```


Telnet Command: `srv dhcp frcdnsmanl`

This command can force the router to invoke DNS Server IP address.

```
srv dhcp frcdnsmanl [on]
```

```
srv dhcp frcdnsmanl [off]
```

Syntax Description

Parameter	Description
<code>?</code>	It means to display the current status.
<code>on</code>	It means to use manual setting for DNS setting.
<code>Off</code>	It means to use auto settings acquired from ISP.

Example

```
> srv dhcp frcdnsmanl on
% Domain name server now is using manual settings!
> srv dhcp frcdnsmanl off
% Domain name server now is using auto settings!
```

Telnet Command: `srv dhcp gateway`

This command allows users to specify gateway address for DHCP server.

```
srv dhcp gateway [?]
```

```
srv dhcp gateway [Gateway IP]
```

Syntax Description

Parameter	Description
<code>?</code>	It means to display current gateway that you can use.
<code>Gateway IP</code>	It means to specify a gateway address used for DHCP server.

Example

```
> srv dhcp gateway 192.168.2.1
This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

Telnet Command: `srv dhcp ipcnt`

This command allows users to specify IP counts for DHCP server.

```
srv dhcp ipcnt [?]
```

```
srv dhcp ipcnt [IP counts]
```

Syntax Description

Parameter	Description
<i>?</i>	It means to display current used IP count number.
<i>IP counts</i>	It means the number that you have to specify for the DHCP server.

Example

```
> srv dhcp ipcnt ?
% srv dhcp ipcnt <IP counts>
% Now: 150
```

Telnet Command: `srv dhcp off`

This function allows users to turn off DHCP server. It needs rebooting router, please type "sys reboot" command to reboot router.

Telnet Command: `srv dhcp on`

This function allows users to turn on DHCP server. It needs rebooting router, please type "sys reboot" command to reboot router.

Telnet Command: `srv dhcp relay`

This command allows users to set DHCP relay setting.

```
srv dhcp relay servip [server ip]
```

```
srv dhcp relay subnet [index]
```

Syntax Description

Parameter	Description
<i>server ip</i>	It means the IP address that you want to used as DHCP server.
<i>Index</i>	It means subnet 1 or 2. Please type 1 or 2. The router will invoke this function according to the subnet 1 or 2 specified here.

Example

```
> srv dhcp relay servip 192.168.1.46
> srv dhcp relay subnet 2
> srv dhcp relay servip ?
% srv dhcp relay servip <server ip>
% Now: 192.168.1.46
```

Telnet Command: `srv dhcp startip`

`srv dhcp startip [?]`

`srv dhcp startip [IP address]`

Syntax Description

Parameter	Description
<code>?</code>	It means to display current used start IP address.
<code>IP address</code>	It means the IP address that you can specify for the DHCP server as the starting point.

Example

```
> srv dhcp startip 192.168.1.53
This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

Telnet Command: `srv dhcp status`

This command can display general information for the DHCP server, such as IP address, MAC address, leased time, host ID and so on.

Example

```
> srv dhcp status
DHCP server: Relay Agent
Default gateway: 192.168.1.1
Index  IP Address      MAC Address      Leased Time      HOST ID
1      192.168.1.113   00-05-5D-E4-D8-EE  17:20:08        A1000351
```

Telnet Command: `srv dhcp leasetime`

This command can set the lease time for the DHCP server.

```
srv dhcp leasetime [?]
```

```
srv dhcp leasetime [Lease Time (sec)]
```

Syntax Description

Parameter	Description
<code>?</code>	It means to display current leasetime used for the DHCP server.
<code>Lease Time (sec)</code>	It means the lease time that DHCP server can use. The unit is second.

Example

```
> srv dhcp leasetime ?
% srv dhcp leasetime <Lease Time (sec.)>
% Now: 86400
>
```

Telnet Command: `srv dhcp nodetype`

This command can set the node type for the DHCP server.

```
srv dhcp nodetype <count>
```

Syntax Description

Parameter	Description
<code>count</code>	It means to specify a type for node. 1. B-node 2. P-node 4. M-node 8. H-node

Example

```
> srv dhcp nodetype 1
> srv dhcp nodetype ?
%% srv dhcp nodetype <count>
%% 1. B-node 2. P-node 4. M-node 8. H-node
% Now: 1
```

Telnet Command: `srv dhcp primWINS`

This command can set the primary IP address for the DHCP server.

```
srv dhcp primWINS [WINS IP address]
```

```
srv dhcp primWINS clear
```

Syntax Description

Parameter	Description
<i>WINS IP address</i>	It means the IP address of primary WINS server.
<i>clear</i>	It means to remove the IP address settings of primary WINS server.

Example

```
> srv dhcp primWINS 192.168.1.88
> srv dhcp primWINS ?
%% srv dhcp primWINS <WINS IP address>
%% srv dhcp primWINS clear
% Now: 192.168.1.88
```

Telnet Command: `srv dhcp secWINS`

This command can set the secondary IP address for the DHCP server.

```
srv dhcp secWINS [WINS IP address]
```

```
srv dhcp secWINS clear
```

Syntax Description

Parameter	Description
<i>WINS IP address</i>	It means the IP address of secondary WINS server.
<i>clear</i>	It means to remove the IP address settings of second WINS server.

Example

```
> srv dhcp secWINS 192.168.1.180
> srv dhcp secWINS ?
%% srv dhcp secWINS <WINS IP address>
%% srv dhcp secWINS clear
% Now: 192.168.1.180
```

Telnet Command: `srv dhcp expired_RecycleIP`

This command can set the time to check if the IP address can be assigned again by DHCP server or not.

```
srv dhcp expRecycleIP <sec time>
```

Syntax Description

Parameter	Description
<i>sec time</i>	It means to set the time (5-300 seconds) for checking if the IP can be assigned again or not.

Example

```
Vigor> srv dhcp expRecycleIP 250
% DHCP expired_RecycleIP = 250
```

Telnet Command: `srv dhcp tftp`

This command can set the TFTP server as the DHCP server.

```
srv dhcp tftp <TFTP server name>
```

Syntax Description

Parameter	Description
<i>TFTP server name</i>	It means to Enter the name of TFTP server.

Example

```
> srv dhcp tftp TF123
> srv dhcp tftp ?
%% srv dhcp tftp <TFTP server name>
% Now: TF123
```

Telnet Command: `srv dhcp option`

This command can set the custom option for the DHCP server.

```
srv dhcp option -h
```

```
srv dhcp option -l
```

```
srv dhcp option -d [idx]
```

```
srv dhcp option -e [1 or 0] -c [option number] -v [option value]
```

```
srv dhcp option -e [1 or 0] -c [option number] -a [option value]
```

```
srv dhcp option -e [1 or 0] -c [option number] -x [option value]
```

```
srv dhcp option -u [idx unumber]
```

Syntax Description

Parameter	Description
<i>-h</i>	It means to display usage of this command.
<i>-l</i>	It means to display all the user defined DHCP options.
<i>-d[idx]</i>	It means to delete the option number by specifying its index number.
<i>-e [1 or 0]</i>	It means to enable/disable custom option feature.

	1:enable 0:disable
-c	It means to set option number. Available number ranges from 0 to 255.
-v	It means to set option number by typing string.
-a	It means to set the option value by specifying the IP address.
-x	It means to set option number with the format of Hexadecimal characters.
-u	It means to update the option value of the sepecified index.
<i>idx number</i>	It means the index number of the option value.

Example

```
>srv dhcp option -e 1 -i 2/r -c 44 -a 192.168.1.10,192.168.1.20
```

Telnet Command: `srv nat dmz`

This command allows users to set DMZ host. Before using this command, please set WAN IP Alias first.

`Srv nat dmz n m [-<command> <parameter> | ...]`

Syntax Description

Parameter	Description
<i>n</i>	It means to map selected WAN IP to certain host. 1: wan1 2: wan2
<i>m</i>	It means the index number of the DMZ host. Default setting is "1" (WAN 1). It is only available for Static IP mode. If you use other mode, you can set 1 - 8 in this field. If WAN IP alias has been configured, then the number of DMZ host can be added more.
<i>[<command> <parameter> ...]</i>	The available commands with parameters are listed below. <i>[...]</i> means that you can type in several commands in one line.
<i>-e</i>	It means to enable/disable such feature. 1:enable 0:disable
<i>-i</i>	It means to specify the private IP address of the DMZ host.
<i>-r</i>	It means to remove DMZ host setting.
<i>-v</i>	It means to display current status.

Example

```
> srv nat dmz 1 1 -i 192.168.1.96
> srv nat dmz -v
%      WAN1 DMZ mapping status:
Index  Status  WAN1 aux IP   Private IP
-----
1      Disable  0.0.0.0      192.168.1.96
```

Telnet Command: `srv nat ipsecpass`

This command allows users to enable or disable IPSec ESP tunnel passthrough and IKE source port (500) preservation.

`Srv nat ipsecpass [options]`

Syntax Description

Parameter	Description
<i>[options]</i>	The available commands with parameters are listed below.
<i>on</i>	It means to enable IPSec ESP tunnel passthrough and IKE source port (500) preservation.
<i>off</i>	It means to disable IPSec ESP tunnel passthrough and IKE source port (500) preservation.
<i>status</i>	It means to display current status for checking.

Example


```
> srv nat ipsecpass status
%% Status: IPsec ESP pass-thru and IKE src_port:500 preservation is
OFF.
```

Telnet Command: `srv nat openport`

This command allows users to set open port settings for NAT server.

`srv nat openport n m [-<command> <parameter> | ...]`

Syntax Description

Parameter	Description
<i>n</i>	It means the index number for the profiles. The range is from 1 to 20.
<i>m</i>	It means to specify the sub-item number for this profile. The range is from 1 to 10.
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-a <enable>	It means to enable or disable the open port rule profile. 0: disable 1:enable
-c <comment>	It means to Enter the description (less than 23 characters) for the defined network service.
-i <local ip>	It means to set the IP address for local computer. Local ip: Type an IP address in this field.
-w <idx>	It means to specify the public IP. 1: WAN1 Default, 2: WAN1 Alias 1, ...and so on.
-p <protocol>	Specify the transport layer protocol. Available values are TCP, UDP and ALL.
-s<start port>	It means to specify the starting port number of the service offered by the local host. The range is from 0 to 65535.
-e<end port>	It means to specify the ending port number of the service offered by the local host. The range is from 0 to 65535.
-v	It means to display current settings.
-r <remove>	It means to delete the specified open port setting. remove: Enter the index number of the profile.
-f <flush>	It means to return to factory settings for all the open ports profiles.

Example

```
> srv nat openport 1 1 -a 1 -c games -i 192.168.1.100 -w 1 -p TCP -s
23 -e 83
> srv nat openport -v
%% Status: Enable
%% Comment: games
%% Private IP address: 192.168.1.100
Index  Protocal      Start Port    End Port
*****
```

```

1.      TCP                23                83

%% Status: Disable
%% Comment:
%% Private IP address: 0.0.0.0
Index  Protocol          Start Port      End Port
*****

%% Status: Disable
%% Comment:
%% Private IP address: 0.0.0.0
Index  Protocol          Start Port      End Port
*****

>

```

Telnet Command: `srv nat portmap`

This command allows users to set port redirection table for NAT server.

```

srv nat portmap add [idx][serv name][proto][pub port][pri ip][pri port][wan1/wan2]
srv nat portmap del [idx]
srv nat portmap disable [idx]
srv nat portmap enable [idx] [proto]
srv nat portmap flush
srv nat portmap table

```

Syntax Description

Parameter	Description
<i>Add[idx]</i>	It means to add a new port redirection table with an index number. Available index number is from 1 to 10.
<i>serv name</i>	It means to type one name as service name.
<i>proto</i>	It means to specify TCP or UDP as the protocol.
<i>pub port</i>	It means to specify which port can be redirected to the specified Private IP and Port of the internal host.
<i>pri ip</i>	It means to specify the private IP address of the internal host providing the service.
<i>pri port</i>	It means to specify the private port number of the service offered by the internal host.
<i>wan1/wan2</i>	It means to specify WAN interface for the port redirection.
<i>del [idx]</i>	It means to remove the selected port redirection setting.
<i>disable [idx]</i>	It means to inactivate the selected port redirection setting.
<i>enable [idx]</i>	It means to activate the selected port redirection setting.
<i>flush</i>	It means to clear all the port mapping settings.
<i>table</i>	It means to display Port Redirection Configuration Table.

Example

```

> srv nat portmap add 1 game tcp 80 192.168.1.11 100 wan1
> srv nat portmap table

```

NAT Port Redirection Configuration Table:

Index	Service Name	Protocol	Public Port	Private IP	Private Port
1	game	6	80	192.168.1.11	100
-1					
2		0	0		-2
3		0	0		-2
4		0	0		-2
5		0	0		-2
6		0	0		-2
7		0	0		-2
8		0	0		-2
9		0	0		-2
10		0	0		-2
11		0	0		-2
12		0	0		-2
13		0	0		-2
14		0	0		-2
15		0	0		-2
16		0	0		-2
17		0	0		-2
18		0	0		-2
19		0	0		-2
20		0	0		-2

Protocol: 0 = Disable, 6 = TCP, 17 = UDP

Telnet Command: `srv nat trigger`

This command allows users to configure port triggering settings for NAT.

Syntax

`srv nat trigger setdefault`

`srv nat trigger view`

`srv nat trigger n [-<command> <parameter> | ...]`

Syntax Description

Parameter	Description
<code>setdefault</code>	Set to factory default settings.
<code>view</code>	Display all of the port triggering settings.
<code>n</code> <code><command><parameter>[...]</code>	“n” means the rule number. The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
<code>-c[XXX]</code>	Type a comment for such rule if required.
<code>-e [0/1]</code>	Enable (1) or disable (0) a rule (specified with rule number).
<code>-p [1/2/3]</code>	Specify the protocol for such trigger rule.

	1 - TCP 2 - UDP 3 - All
<code>-t</code>	Specify the port number (0-65535) for trigger.
<code>-P</code>	Specify the incoming protocol for such trigger rule.
<code>-i</code>	Specify the port number (0-65535) for incoming protocol.
<code>-d</code>	Delete the selected trigger rule.
<code>-v</code>	Display the port trigger settings for specified rule.

Example

```
> srv nat trigger 1 -c after_dinner
> srv nat trigger 1 -e 1
> srv nat trigger 1 -p 1
> srv nat trigger 1 -t 2000
> srv nat trigger 1 -P 2
> srv nat trigger 1 -i 3000
> srv nat trigger 1 -v
```

Port Trigger Rule Index:1

Status:Enable
Comment:after_dinner2000
Triggering Protocol:TCP
Triggering Port:2000
Incoming Protocol:UDP
Incoming Port:3000

Telnet Command: `srv nat status`

This command allows users to view NAT Port Redirection Running Table.

Example

```
> srv nat status
NAT Port Redirection Running Table:
```

Index	Protocol	Public Port	Private IP	Private Port
1	6	80	192.168.1.11	100
2	0	0	0.0.0.0	0
3	0	0	0.0.0.0	0
4	0	0	0.0.0.0	0
5	0	0	0.0.0.0	0
6	0	0	0.0.0.0	0
7	0	0	0.0.0.0	0
8	0	0	0.0.0.0	0
9	0	0	0.0.0.0	0
10	0	0	0.0.0.0	0
11	0	0	0.0.0.0	0
12	0	0	0.0.0.0	0
13	0	0	0.0.0.0	0

14	0	0	0.0.0.0	0
15	0	0	0.0.0.0	0
16	0	0	0.0.0.0	0
17	0	0	0.0.0.0	0
18	0	0	0.0.0.0	0
19	0	0	0.0.0.0	0
20	0	0	0.0.0.0	0
--- MORE --- ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]				

Telnet Command: `srv nat showall`

This command allows users to view a summary of NAT port redirection setting, open port and DMZ settings.

Example

```
> srv nat showall ?
Index  Proto  WAN IP:Port          Private IP:Port      Act
*****
****
R01    TCP    0.0.0.0:80          192.168.1.11:100    Y
O01    TCP    0.0.0.0:23~83       192.168.1.100:23~83 Y
D01    All    0.0.0.0             192.168.1.96        Y

R:Port Redirection, O:Open Ports, D:DMZ
```

Telnet Command: `switch -i`

This command is used to obtain the TX (transmitted) or RX (received) data for each connected switch.

Syntax

`switch -i [switch idx_no] [option]`

Syntax Description

Parameter	Description
<i>switch idx_no</i>	It means the index number of the switch profile.
<i>option</i>	The available commands with parameters are listed below. <i>cmd</i> <i>acc</i> <i>traffic [on/off/status/tx/rx]</i>
<i>cmd</i>	It means to send command to the client.
<i>acc</i>	It means to set the client authentication account and password.
<i>traffic [on/off/status/tx/rx]</i>	It means to turn on/off or display the data transmission from the client.

Example

```
> switch -i 1 traffic on
External Device NO. 1 traffic statistic function is enable
```

Telnet Command: switch status

This command is used to check the status for the auto discovery of external devices.

Example

```
> switch status
External Device auto discovery status : Disable

No Respond to External Device : Enable
```

Telnet Command: switch not_respond

This command is used to detect the external device automatically and display on this page.

Syntax

```
switch not_respond 0
```

```
switch not_respond 1
```

Syntax Description

Parameter	Description
0	Disable the option of "No Respond to External Device packets".
1	Enable the option of "No Respond to External Device packets".

Example

```
> switch not_respond 1
slave not respond!
>
```

Telnet Command: switch on

This command is used to turn on the auto discovery for external devices.

Example

```
> switch on
Enable Extrnal Device auto discovery!
```

Telnet Command: switch off

This command is used to turn off the auto discovery for external devices.

Example

```
> switch off
Disable External Device auto discovery!
```

Telnet Command: switch list

This command is used to display the connection status of the switch.

Example

```
> switch list?
```

No.	Mac	IP	status	Dur Time	Model_Name

[1]	00-50-7f-cd-07-48	192.168.1.3	On-Line	00:01:01	Vigor2920 Series

Telnet Command: switch clear

This command is used to reset the switch table and reboot the router.

switch clear *[idx]*

Syntax Description

Parameter	Description
<i>idx</i>	It means the index number of each item shown on the table. The range is from 1 to 8.
<i>-f</i>	It means to clear all of the data.

Example

```
> switch clear 1
Switch Data clear successful

> switch clear -f
Switch Data clear successful
```

Telnet Command: switch query

This command is used to enable or disable the switch query.

Example

```
> switch query on
Extern Device status query is Enable

> switch query off
Extern Device status query is Disable
```

Telnet Command: sys admin

This command is used for RD engineer to access into test mode of Vigor router.

Telnet Command: sys adminuser

This command is used to create user account. The server will authenticate the local user who wants to access into the web user interface of Vigor router.

sys adminuser *[option]*

sys adminuser edit *[index] username password*

Syntax Description

Parameter	Description
<i>option</i>	Available options includes: Local [0-1] edit [INDEX] delete [INDEX] view [INDEX]

<i>Local [0-1]</i>	0 - Disable the local user. 1 - Enable the local user.
<i>edit [INDEX] username password</i>	Edit an existed user account or create a new local user account. [INDEX] - 1 -8. There are eight profiles to be added / edited. Username - Type a new name for local user. Password - Type a password for local user.
<i>delete [INDEX]</i>	Delete a local user account.
<i>view [INDEX]</i>	Show the user account/password detail information.

Example

```
> sys adminuser Local 1
Local User has enabled!
> sys adminuser edit 1 carrie test123
Updated!
> sys adminuser view 1

Index:1
User Name:carrie
User Password:test123
```

Telnet Command: sys bonjour

This command is used to disable/enable and configure the Bonjour service.

sys bonjour [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
-e <enable>	It is used to disable/enable bonjour service (0: disable, 1: enable).
-h <enable>	It is used to disable/enable http (web) service (0: disable, 1: enable).
-t <enable>	It is used to disable/enable telnet service (0: disable, 1: enable).
-f <enable>	It is used to disable/enable FTP service (0: disable, 1: enable).
-s <enable>	It is used to disable/enable SSH service (0: disable, 1: enable).
-p <enable>	It is used to disable/enable printer service (0: disable, 1: enable).
-6 <enable>	It is used to disable/enable IPv6 (0: disable, 1: enable).

Example

```
> sys bonjour -s 1
>
```


Telnet Command: sys cfg

This command reset the router with factory default settings. When a user types this command, all the configuration will be reset to default setting.

sys cfg default

sys cfg status

Syntax Description

Parameter	Description
<i>default</i>	It means to reset current settings with default values.
<i>status</i>	It means to display current profile version and status.

Example

```
> sys cfg status
Profile version: 3.0.0   Status: 1 (0x491e5e6c)
> sys cfg default
>
```

Telnet Command: sys cmdlog

This command displays the history of the commands that you have typed.

Example

```
> sys cmdlog
% Commands Log: (The lowest index is the newest !!!)
 [1] sys cmdlog
 [2] sys cmdlog ?
 [3] sys ?
 [4] sys cfg status
 [5] sys cfg ?
```

Telnet Command: sys ftpd

This command displays current status of FTP server.

sys ftpd on

sys ftpd off

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on the FTP server of the system.
<i>off</i>	It means to turn off the FTP server of the system.

Example

```
> sys ftpd on
% sys ftpd turn on !!!
```

Telnet Command: sys domainname

This command can set and remove the domain name of the system when DHCP mode is selected for WAN.

sys domainname [wan1/wan2] [Domain Name Suffix]

sys domainname [wan1/wan2] clear

Syntax Description

Parameter	Description
<i>wan1/wan2</i>	It means to specify WAN interface for assigning a name for it.
<i>Domain Name Suffix</i>	It means the name for the domain of the system. The maximum number of characters that you can set is 40.
<i>clear</i>	It means to remove the domain name of the system.

Example

```
> sys domainname wan1 clever
> sys domainname wan2 intellegent
> sys domainname ?
% sys domainname <wan1/wan2> <Domain Name Suffix (max. 40 characters)>
% sys domainname <wan1/wan2> clear
% Now: wan1 == clever, wan2 ==intelligent
>
```

Telnet Command: sys iface

This command displays the current interface connection status (UP or Down) with IP address, MAC address and Netmask for the router.

Example

```
> sys iface
Interface 0 Ethernet:
Status: UP
IP Address: 192.168.1.1      Netmask: 0xFFFFFFFF00 (Private)
IP Address: 0.0.0.0        Netmask: 0xFFFFFFFF
MAC: 00-50-7F-00-00-00
Interface 4 Ethernet:
Status: DOWN
IP Address: 0.0.0.0        Netmask: 0x00000000
MAC: 00-50-7F-00-00-02
Interface 5 Ethernet:
Status: DOWN
IP Address: 0.0.0.0        Netmask: 0x00000000
MAC: 00-50-7F-00-00-03
Interface 6 Ethernet:
Status: DOWN
IP Address: 0.0.0.0        Netmask: 0x00000000
MAC: 00-50-7F-00-00-04
Interface 7 Ethernet:
Status: DOWN
IP Address: 0.0.0.0        Netmask: 0x00000000
MAC: 00-50-7F-00-00-05
Interface 8 Ethernet:
Status: DOWN
```

```
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-06

Interface 9 Ethernet:
Status: DOWN
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-07
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
>
```

Telnet Command: sys name

This command can set and remove the name for the router when DHCP mode is selected for WAN.

```
sys name [wan1] [ASCII string]
```

```
sys name [wan1] clear
```

Syntax Description

Parameter	Description
<i>wan1</i>	It means to specify WAN interface for assigning a name for it.
<i>ASCII string</i>	It means the name for router. The maximum character that you can set is 20.

Example

```
> sys name wan1 drayrouter
> sys name ?
% sys name <wan1/wan2> <ASCII string (max. 20 characters)>
% sys name <wan1/wan2> clear
% Now: wan1 == drayrouter, wan2 ==
```

Note: Such name can be used to recognize router's identification in SysLog dialog.

Telnet Command: sys passwd

This command allows users to set password for the administrator.

```
sys passwd [ASCII string]
```

Syntax Description

Parameter	Description
<i>ASCII string</i>	It means the password for administrator. The maximum character that you can set is 23.

Example

```
> sys passwd admin123
>
```

Telnet Command: sys reboot

This command allows users to restart the router immediately.

Example

```
> sys reboot
>
```

Telnet Command: sys autoreboot

This command allows users to restart the router automatically within a certain time.

`sys autoreboot [on/off/hour(s)]`

Syntax Description

Parameter	Description
<i>on/off</i>	On - It means to enable the function of auto-reboot. Off - It means to disable the function of auto-reboot.
<i>hours</i>	It means to set the time schedule for router reboot. For example, if you type "2" in this field, the router will reboot with an interval of two hours.

Example

```
> sys autoreboot on
autoreboot is ON
> sys autoreboot 2
autoreboot is ON
autoreboot time is 2 hour(s)
```

Telnet Command: sys commit

This command allows users to save current settings to FLASH. Usually, current settings will be saved in SRAM. Yet, this command will save the file to FLASH.

Example

```
> sys commit
>
```

Telnet Command: sys tftpd

This command can turn on TFTP server for upgrading the firmware.

Example

```
> sys tftpd
% TFTP server enabled !!!
```

Telnet Command: sys cc

This command can display current country code and wireless region of this device.

Example

```
> sys cc
Country Code      : 0x 0 [International]
Wireless Region Code: 0x30
>
```

Telnet Command: sys version

This command can display current version for the system.

Example

```
> sys version
Router Model: Vigor2762Vn+   Version: 3.7.4.1 English
Profile version: 3.0.0     Status: 1 (0x49165e6c)
Router IP: 192.168.1.1     Netmask: 255.255.255.0
Firmware Build Date/Time: Mar 20 2014 14:09:50
Router Name: drayrouter
Revision: 40055 2860_374
VDSL2 Firmware Version: 05-04-08-00-00-06
```

Telnet Command: sys qrybuf

This command can display the system memory status and leakage list.

Example

```
> sys qrybuf
System Memory Status and Leakage List

Buf sk_buff ( 200B), used#: 1647, cached#: 30
Buf KMC4088 (4088B), used#: 0, cached#: 8
Buf KMC2552 (2552B), used#: 1641, cached#: 42
Buf KMC1016 (1016B), used#: 7, cached#: 1
Buf KMC504 ( 504B), used#: 8, cached#: 8
Buf KMC248 ( 248B), used#: 26, cached#: 22
Buf KMC120 ( 120B), used#: 67, cached#: 61
Buf KMC56 ( 56B), used#: 20, cached#: 44
Buf KMC24 ( 24B), used#: 58, cached#: 70
Dynamic memory: 13107200B; 4573168B used; 190480B/0B in level 1/2
cache.

FLOWTRACK Memory Status
# of free = 12000
# of maximum = 0
# of flowstate = 12000
# of lost by siganture = 0
# of lost by list = 0
```

Telnet Command: sys pollbuf

This command can turn on or turn off polling buffer for the router.

```
sys pollbuf [on]
```

```
sys pollbuf [off]
```

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on pulling buffer.
<i>off</i>	It means to turn off pulling buffer.

Example

```

> sys pollbuf on
% Buffer polling is on!

> sys pollbuf off
% Buffer polling is off!

```

Telnet Command: sys britask

This command can improve triple play quality.

sys britask *[on]*

sys britask *[off]*

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on the bridge task for improving the triple play quality.
<i>off</i>	It means to turn off the bridge task.

Example

```

> sys britask on
% bridge task is ON, now

```

Telnet Command: sys tr069

This command can set CPE settings for applying in VigorACS.

sys tr069 get *[parm] [option]*

sys tr069 set *[parm] [value]*

sys tr069 getnoti *[parm]*

sys tr069 setnoti *[parm] [value]*

sys tr069 log

sys tr069 debug *[on/off]*

sys tr069 save

sys tr069 inform *[event code]*

sys tr069 port *[port num]*

sys tr069 cert_auth *[on/off]*

Syntax Description

Parameter	Description
<i>get [parm] [option]</i>	It means to get parameters for tr-069. option=<nextlevel>: only gets nextlevel for GetParameterNames.
<i>set [parm] [value]</i>	It means to set parameters for tr-069.
<i>getnoti [parm]</i>	It means to get parameter notification value.
<i>setnoti [parm] [value]</i>	It means to set parameter notification value.
<i>log</i>	It means to display the TR-069 log.
<i>debug [on/off]</i>	on: turn on the function of sending debug message to syslog. off: turn off the function of sending debug message to syslog.

<i>save</i>	It means to save the parameters to the flash memory of the router.
<i>Inform [event code]</i>	It means to inform parameters for tr069 with different event codes. [event code] includes: 0-"0 BOOTSTRAP", 1-"1 BOOT", 2-"2 PERIODIC", 3-"3 SCHEDULED", 4-"4 VALUE CHANGE", 5-"5 KICKED", 6-"6 CONNECTION REQUEST", 7-"7 TRANSFER COMPLETE", 8-"8 DIAGNOSTICS COMPLETE", 9-"M Reboot"
<i>port [port num]</i>	It means to change tr069 listen port number.
<i>cert_auth [on/off]</i>	on: turn on certificate-based authentication. off: turn off certificate-based authentication.

Example

```

> sys tr069 get Int. nextlevel
Total number of parameter is 24
Total content length of parameter is 915
InternetGatewayDevice.LANDeviceNumberOfEntries
InternetGatewayDevice.WANDeviceNumberOfEntries
InternetGatewayDevice.DeviceInfo.
InternetGatewayDevice.ManagementServer.
InternetGatewayDevice.Time.
InternetGatewayDevice.Layer3Forwarding.
InternetGatewayDevice.LANDevice.
InternetGatewayDevice.WANDevice.
InternetGatewayDevice.Services.
InternetGatewayDevice.X_00507F_InternetAcc.
InternetGatewayDevice.X_00507F_LAN.
InternetGatewayDevice.X_00507F_NAT.
InternetGatewayDevice.X_00507F_Firewall.
InternetGatewayDevice.X_00507F_Bandwidth.
InternetGatewayDevice.X_00507F_Applications.
InternetGatewayDevice.X_00507F_VPN.
InternetGatewayDevice.X_00507F_VoIP.
InternetGatewayDevice.X_00507F_WirelessLAN.
InternetGatewayDevice.X_00507F_System.
InternetGatewayDevice.X_00507F_Status.

InternetGatewayDevice.X_00507F_Diagnostics.
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
```

Telnet Command: sys sip_alg

This command can turn on/off SIP ALG (Application Layer Gateway) for traversal.

```
sys sip_alg [1]
```

```
sys sip_alg [0]
```


Syntax Description

Parameter	Description
<i>1</i>	It means to turn on SIP ALG.
<i>0</i>	It means to turn off SIP ALG.

Example

```
> sys sip_alg ?
usage: sys sip_alg [value]
 0 - disable SIP ALG
 1 - enable SIP ALG
current SIP ALG is disabled
```

Telnet Command: sys license

This command can process the system license.

Syntax

```
sys license licmsg
sys license licauth
sys license regser
sys license licera
sys license licifno
sys license lic_wiz [set/reg/qry]
sys license dev_chg
sys license dev_key
```

Syntax Description

Parameter	Description
<i>licmsg</i>	It means to display license message.
<i>licauth</i>	It means the license authentication time setting.
<i>regser</i>	It means the license register server setting.
<i>licera</i>	It means to erase license setting.
<i>licifno</i>	It means license and signature download interface setting.
<i>lic_wiz</i> [<i>set/reg/qry</i>]	It means the license wizard setting. qry: query service support status set [idx] [trial] [service type] [sp_id] [start_date] [License Key] reg: register service in portal
<i>dev_chg</i>	It means to change the device key.
<i>dev_key</i>	It means to show device key.

Example

```
> sys license licifno

License and Signature download interface setting:
```

```
licifno [AUTO/WAN#]
```

```
Ex: licifno wan1
```

```
Download interface is "auto-selected" now.
```

Telnet Command: sys diag_log

This command is used for RD debug.

```
sys diag_log [status| enable| disable| flush| lineno [w] | level [x] | feature [on/off] [y]/  
log]
```

Syntax Description

Parameter	Description
<i>status</i>	It means to show the status of diagnostic log.
<i>enable</i>	It means to enable the function of diag_log.
<i>disable</i>	It means to disenable the function of diag_log.
<i>flush</i>	It means the flush log buffer.
<i>lineno [w]</i>	It means the total lines for displaying message. w - Available value ranges from 100 to 50000.
<i>level[x]</i>	It determines the level of data displayed. x - Available value ranges from 0 to 12. The larger the number is, the detailed the data is displayed.
<i>feature [on/off][y]</i>	It is used to specify the function of the log. Supported features include SYS and DSL (Case-Insensitive). Default setting is "on" for "DSL".
<i>voip_feature [on/off][vf_name]</i>	It means VoIP feature. Type on to enable the feature or type off to disable the feature. vf_name: available settings include DRVTAPI, DRVMMC, DRVMP, DRVFXO, DRVHAL, PSMPHONE, PSMSUPP, PSM, FXO, PSMISDN, DTMFPSER, CALLERID (Case-Insensitive).
<i>log</i>	It means the dump log buffer.

Example

```
> sys diag_log status  
Status:  
diag_log is Enabled.  
lineno : 10000.  
level : 3.  
Enabled feature: SYS DSL  
> sys diag_log log  
0:00:02 [DSL] Current modem firmware: AnnexA_548006_544401  
0:00:02 [DSL] Modem firmware feature: 5, ADSL_A, VDSL2  
0:00:02 [DSL] xtseCfg=04 00 04 00 0c 01 00 07  
0:00:02 [DSL] don't have last showtime mode!! set next mode to VDSL!!  
0:00:02 [DSL] Status has changed: Stopped(0) -> FwWait(3)  
0:00:02 [DSL] Status has changed: FwWait(3) -> Starting(1)  
0:00:02 [DSL] Status has changed: Starting(1) -> Running(2)  
0:00:02 [DSL] Status was switched: firmwareReady(3) to Init(5)  
0:00:02 [DSL] Status was switched: Init(5) to Restart(10)  
0:00:02 [DSL] Status was switched: Restart(10) to
```

```

FirmwareRequest(1)
0:00:02 [DSL] Line state has changed: 00000000 -> 000000FF
0:00:02 [DSL] Entering VDSL2 mode
0:00:03 [DSL] modem code: [05-04-08-00-00-06]
0:00:05 [DSL] Status was switched: FirmwareRequest(1) to
firmwareReady(3)
0:00:05 [DSL] Status was switched: firmwareReady(3) to Init(5)
0:00:05 [DSL] >> nXtseA=0d, nXtseB=00, nXtseV=07, nFwFeatures=5
0:00:05 [DSL] >> nHsToneGroupMode=0, nHsToneGroup=106,
nToneSet=43, nCamState
=2
0:00:05 [DSL] Line state has changed: 000000FF -> 00000100
0:00:05 [DSL] Line state has changed: 00000100 -> 00000200
0:00:05 [DSL] Status was switched: Init(5) to Train(6)

```

Telnet Command: sys daylightsave

This command is used to configure daylight save setting.

Syntax

sys daylightsave [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
[<command><parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-v	Display the daylight saving settings.
-r	Set to factory default setting.
-e [1/0]	Enable (1) / disable (0) daylight saving.
-t [0/1/2]	Specify the saving type for daylight setting. 0 - Default 1 - Time range 2 - Yearly
-s <year> <month> <day> <hour>	Set the detailed settings of the starting day for time range type. year - must be the year after 2013. month - 1 - 12 day - 1 - 31 hour - 0 - 23 e.g., sys daylightsave -s 2014 3 10 12
-d <year> <month> <day> <hour>	Set the detailed settings of the ending day for time range type. year - After 2013. month - 1 - 12 day - 1 - 31 hour - 0 - 23 e.g., sys daylightsave -d 2014 9 10 12
-y <month> <th weekday> <day in week> <hour>	Set the detailed settings of the starting day for yearly type. month - 1 - 12 th weekday - 1 - 5, 9: last week day in week - 0:Sun, 1:Mon, 2:Tue, 3:Wed, 4:Thu, 5: Fri, 6:Sat hour - 0 - 23 e.g., sys daylightsave -y 9 1 0 14

<pre>-z <month> <th weekday> <day in week> <hour></pre>	<p>Set the detailed settings of the ending day for yearly type.</p> <p>month - 1 ~ 12</p> <p>th weekday - 1 ~ 5, 9: last week</p> <p>day in week - 0:Sun, 1:Mon, 2:Tue, 3:Wed, 4:Thu, 5: Fri, 6:Sat</p> <p>hour - 0 ~ 23</p> <p>e.g, sys daylightsave -z 3 1 6 14</p>
---	---

Example

```
> sys daylightsave -y 9 1 0 14
% Start: Yearly on Sep 1th Sun 14:00
```

Telnet Command: sys dnsCacheTbl

This command is used to configure TTL settings which will be displayed in DNS Cache table.

Syntax

```
sys dnsCacheTbl [<command><parameter>|...]
```

Syntax Description

Parameter	Description
<i>[<command><parameter> ...]</i>	The available commands with parameters are listed below. <i>[...]</i> means that you can type in several commands in one line.
<i>-l</i>	Display DNS IPv4 entry in the DNS cache table.
<i>-s</i>	Display DNS IPv6 entry in the DNS cache table.
<i>-v</i>	Display the TTL limit value in the DNS cache table.
<i>-t <0/n ></i>	Set the TTL limit value in the DNS cache table. 0- No limit N - Greater than or equal to 5.
<i>-c</i>	Clear the DNS cache table.

Example

```
> sys dnsCacheTbl -l
%DNS Cache Table List
> sys dnsCacheTbl -t 65
% Set TTL limit: 65 seconds.
% When TTL larger than 65s , delete the DNS entry in the router's DNS cache
tabl
e.
>
```

Telnet Command: sys syslog

This command is used to configure

Syntax

```
sys syslog -a <enable> [-<command> <parameter> | ... ]
```

Syntax Description

Parameter	Description
-----------	-------------

<code>[<command><parameter>/...]</code>	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
<code>-a <1/0></code>	Enable (1) or disable (0) Syslog Access Setup.
<code>-s <1/0></code>	Enable (1) or disable (0) Syslog Save to Syslog Server.
<code>-i <IP address></code>	Define the IP address of the Syslog server.
<code>-d <port number></code>	Define the port number (1 - 65535) as the destination port.
<code>-u <1/0></code>	Enable (1) or disable (0) Syslog Save to USB Disk.
<code>-m <1/0></code>	Enable (1) or disable (0) Mail Syslog.
<code>-f <1/0></code>	Enable (1) or disable (0) Firewall Log.
<code>-v <1/0></code>	Enable (1) or disable (0) VPN Log.
<code>-e <1/0></code>	Enable (1) or disable (0) User Access Log.
<code>-c <1/0></code>	Enable (1) or disable (0) Call Log.
<code>-w <1/0></code>	Enable (1) or disable (0) WAN Log.
<code>-r <1/0></code>	Enable (1) or disable (0) Router/DSL Information.
<code>-t <1/0></code>	Enable (1) or disable (0) AlertLog Setup.
<code>-o <port number></code>	Define the port number (1 - 65535) for AlertLog.

Example

```
> sys syslog -a 1 -s 1 -i 192.168.1.25 -d 514
>
```

Telnet Command: sys time

This command is used to configure system time and date.

Syntax

`sys time server [domain]`

`sys time inquire`

`sys time show`

`sys time zone [index]`

Syntax Description

Parameter	Description
<i>domain</i>	Enter the domain name of the time server. The maximum length is 39 characters.
<i>index</i>	Different number means different time zone. 1 - GMT-12:00 Eniwetok, Kwajalein 2 - GMT-11:00 Midway Island, Samoa 3 - GMT-10:00 Hawaii 4 - GMT-09:00 Alaska 5 - GMT-08:00 Pacific Time (US & Canada) 6 - GMT-08:00 Tijuana 7 - GMT-07:00 Mountain Time (US & Canada) 8 - GMT-07:00 Arizona 9 - GMT-06:00 Central Time (US & Canada) 10 - GMT-06:00 Saskatchewan 11 - GMT-06:00 Mexico City, Tegucigalpa 12 - GMT-05:00 Eastern Time (US & Canada) 13 - GMT-05:00 Indiana (East) 14 - GMT-05:00 Bogota, Lima, Quito 15 - GMT-04:00 Atlantic Time (Canada)

-
- 16 - GMT-04:00 Caracas, La Paz
 - 17 - GMT-04:00 Santiago
 - 18 - GMT-03:30 Newfoundland
 - 19 - GMT-03:00 Brasilia
 - 20 - GMT-03:00 Buenos Aires, Georgetown
 - 21 - GMT-02:00 Mid-Atlantic
 - 22 - GMT-01:00 Azores, Cape Verde Is.
 - 23 - GMT Greenwich Mean Time : Dublin
 - 24 - GMT Edinburgh, Lisbon, London
 - 25 - GMT Casablanca, Monrovia
 - 26 - GMT+01:00 Belgrade, Bratislava
 - 27 - GMT+01:00 Budapest, Ljubljana, Prague
 - 28 - GMT+01:00 Sarajevo, Skopje, Sofija
 - 29 - GMT+01:00 Warsaw, Zagreb
 - 30 - GMT+01:00 Brussels, Copenhagen
 - 31 - GMT+01:00 Madrid, Paris, Vilnius
 - 32 - GMT+01:00 Amsterdam, Berlin, Bern
 - 33 - GMT+01:00 Rome, Stockholm, Vienna
 - 34 - GMT+02:00 Bucharest
 - 35 - GMT+02:00 Cairo
 - 36 - GMT+02:00 Helsinki, Riga, Tallinn
 - 37 - GMT+02:00 Athens, Istanbul, Minsk
 - 38 - GMT+02:00 Jerusalem
 - 39 - GMT+02:00 Harare, Pretoria
 - 40 - GMT+03:00 Volgograd
 - 41 - GMT+03:00 Baghdad, Kuwait, Riyadh
 - 42 - GMT+03:00 Nairobi
 - 43 - GMT+03:00 Moscow, St. Petersburg
 - 44 - GMT+03:30 Tehran
 - 45 - GMT+04:00 Abu Dhabi, Muscat
 - 46 - GMT+04:00 Baku, Tbilisi
 - 47 - GMT+04:30 Kabul
 - 48 - GMT+05:00 Ekaterinburg
 - 49 - GMT+05:00 Islamabad, Karachi, Tashkent
 - 50 - GMT+05:30 Bombay, Calcutta
 - 51 - GMT+05:30 Madras, New Delhi
 - 52 - GMT+06:00 Astana, Almaty, Dhaka
 - 53 - GMT+06:00 Colombo
 - 54 - GMT+07:00 Bangkok, Hanoi, Jakarta
 - 55 - GMT+08:00 Beijing, Chongqing
 - 56 - GMT+08:00 Hong Kong, Urumqi
 - 57 - GMT+08:00 Singapore
 - 58 - GMT+08:00 Taipei
 - 59 - GMT+08:00 Perth
 - 60 - GMT+09:00 Seoul
 - 61 - GMT+09:00 Osaka, Sapporo, Tokyo
 - 62 - GMT+09:00 Yakutsk
 - 63 - GMT+09:30 Darwin
 - 64 - GMT+09:30 Adelaide
 - 65 - GMT+10:00 Canberra, Melbourne, Sydney
 - 66 - GMT+10:00 Brisbane
 - 67 - GMT+10:00 Hobart
 - 68 - GMT+10:00 Vladivostok
 - 69 - GMT+10:00 Guam, Port Moresby
 - 70 - GMT+11:00 Magadan, Solomon Is.
 - 71 - GMT+11:00 New Caledonia
 - 72 - GMT+12:00 Fiji, Kamchatka, Marshall Is.
 - 73 - GMT+12:00 Auckland, Wellington
-

Example

```

> sys time zone 8
Set Time Zone OK

> sys time show
***** System Time *****

```

```
Current System Time: [2000 Jan 01 Sat 02:09:29]
Time Server: [pool.ntp.org]
Time Zone Index: [8]. GMT-07:00
*****
```

Telnet Command: sys eap_tls

This command is used to disable or enable EAP-TLS.

You might have to enable EAP-TLS compatibility to avoid compatibility issues with some operating systems. But, please note that enabling EAP-TLS compatibility will lower down the connection security level.

Syntax

```
sys eap_tls set [0/1]
```

Syntax Description

Parameter	Description
0	Disable EAP-TLS compatibility!
1	Enable EAP-TLS compatibility!

Example

```
> sys eap_tls set 1
Enable EAP_TLS compatibility!
```

Telnet Command: testmail

This command is used to display current settings for sending test mail.

Example

```
> testmail
Send out test mail
Mail Alert:[Disable]
SMTP_Server:[0.0.0.0]
Mail to:[]
Return-Path:[]
```

Telnet Command: upnp off

This command can close UPnP function.

Example

```
>upnp off
UPNP say bye-bye
```

Telnet Command: upnp on

This command can enable UPnP function.

Example

```
>upnp on
```

```
UPNP start.
```

Telnet Command: upnp nat

This command can display IGD NAT status.

Example

```
> upnp nat ?
***** IGD NAT Status *****

((0))
InternalClient >>192.168.1.10<<, RemoteHost >>0.0.0.0<<
InternalPort >>21<<, ExternalPort >>21<<
PortMapProtocol >>TCP<<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
Ftp Example [MICROSOFT]
((1))
InternalClient >>0.0.0.0<<, RemoteHost >>0.0.0.0<<
InternalPort >>0<<, ExternalPort >>0<<
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
0<<

--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
```

Telnet Command: upnp service

This command can display the information of the UPnP service. UPnP service must be enabled first.

Example

```
> upnp on
UPNP start.

> upnp service
>>>> SERVICE TABLE1 <<<<<
  serviceType urn:schemas-microsoft-com:service:OSInfo:1
  serviceId   urn:microsoft-com:serviceId:OSInfo1
  SCPDURL     /upnp/OSInfo.xml
  controlURL  /OSInfo1
  eventURL    /OSInfoEvent1
  UDN         uuid:774e9bbe-7386-4128-b627-001daa843464

>>>> SERVICE TABLE2 <<<<<
  serviceType
urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1
  serviceId   urn:upnp-org:serviceId:WANCommonIFC1
  SCPDURL     /upnp/WComIFCX.xml
```



```

controlURL /upnp?control=WANCommonIFC1
eventURL   /upnp?event=WANCommonIFC1
UDN        uuid:2608d902-03e2-46a5-9968-4a54ca499148
.
.
.

```

Telnet Command: upnp subscribe

This command can show all UPnP services subscribed.

Example

```

> upnp on
UPNP start.
> upnp subscribe
Vigor> upnp subscribe
>>>> (1) serviceType urn:schemas-microsoft-com:service:OSInfo:1

----- Subscribtion1 -----

sid = 7a2bbdd0-0047-4fc8-b870-4597b34da7fb

eventKey =1, ToSendEventKey = 1

expireTime =6926

active =1

DeliveryURLs
=<http://192.168.1.113:2869/upnp/eventing/twtnpnsiun>

>>>> (2) serviceType
urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1

----- Subscribtion1 -----

sid = d9cd47a5-d9c9-4d3d-8043-d03a82f27983

eventKey =1, ToSendEventKey = 1
.
.
.

```

Telnet Command: upnp tmpvs

This command can display current status of temp Virtual Server of your router.

Example

```

Vigor> upnp tmpvs
***** Temp virtual server status *****

((0))
real_addr >>192.168.1.10<<, pseudo_addr >>172.16.3.229<<

```

```

real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>TCP<<
time >>0<<

((1))
real_addr >>0.0.0.0<<, pseudo_addr >>0.0.0.0<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>0<<
time >>0<<
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
```

Telnet Command: upnp wan

This command is used to specify WAN interface to apply UPnP.

```
upnp wan [n]
```

Syntax Description

Parameter	Description
<i>n</i>	It means to specify WAN interface to apply UPnP. n=0, it means to auto-select WAN interface. n=1, WAN1 n=2, WAN2

Example

```
> upnp wan 1
use wan1 now.
```

Telnet Command: usb list

This command is use to display the information about the brand name and model name of the USB modems which are supported by Vigor router.

Example

```
> usb list ?
Brand      Module                Standard
-----
Aiko       Aiko 83D              3.5G          Y
BandRich   Bandlux C170          3.5G          Y
BandRich   Bandlux C270          3.5G          Y
BandRich   Bandlux C321          3.5G          Y
BandRich   Bandlux C330          3.5G          Y
BandRich   Bandlux C331          3.5G          Y
BandRich   Bandlux C502          3.5G          Y
Huawei     Huawei E169u          3.5G          Y
Huawei     Huawei E220           3.5G          Y
Huawei     Huawei E303D          3.5G          Y
Huawei     Huawei E392           3.5G          Y
Huawei     Huawei E398           3.5G          Y
```

Sony Ericcs	Sony Ericsson MD30	3.5G	Y
TP-LINK	TP-LINK MA180	3.5G	Y
TP-LINK	TP-LINK MA260	3.5G	Y
Vodafone	Vodafone K3765-Z	3.5G	Y
Vodafone	Vodafone K4605	3.5G	Y
ZTE	ZTE MF626	3.5G	Y
ZTE	ZTE MF627 plus	3.5G	Y
ZTE	ZTE MF633	3.5G	Y
ZTE	ZTE MF636	3.5G	Y
SpinCom	SpinCom GPRS Modem	3.5G	Y

- MORE - ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] -

Telnet Command: usb user

This command is used to set profiles for FTP/SMB users.

Syntax Description

`usb user add [Index] [Username] [Password] [Permission] [Home path]`

`usb user rm [Index]`

`usb user enable [Index]`

`usb user disable [Index]`

`usb user list`

Syntax Description

Parameter	Description
<i>add</i>	Add a new user profile.
<i>Rm</i>	Delete an existed user profile.
<i>enable</i>	Enable a user profile.
<i>disable</i>	Disable a user profile.
<i>list</i>	Display all of the user profile.
<i>index</i>	It means the index number of the user profile. There are 16 profiles allowed to be configured. So the range of such option is 1 ~ 16.
<i>Username</i>	Type a text (maximum 11 characters) as the username for the user profile.
<i>Password</i>	Type a text (maximum 11 characters) as the password for the user profile.
<i>Permission</i>	Specify the action (RWDLCR) permitted. If one of the actions is not allowed, simple type "-" instead. R - Read File. W - Write File. D - Delete File. L - List directory. C - Create directory. R - Remove selected directory.
<i>Home path</i>	Set the path (maximum 159 characters) for the USB user profile.

Example

```
> usb user add 1 root 1234 R-DLCR /usr
```

Telnet Command: `vigbrg set`

This command is to configure specified WAN as bridge mode.

Syntax Description

```
vigbrg set -v [IP version] -w [WAN_idx] -l [LAN_idx] -e [0/1] -f [0/1]
```

Syntax Description

Parameter	Description
<code>-v [IP version]</code>	Indicate the IP version for the IP address. 4 - IPv4. 6 - IPv6.
<code>-w [WAN_idx]</code>	WAN_idx - Indicate the WAN interface. 1 - WAN1 2 - WAN2 3 - WAN3 4 - WAN4
<code>-l [LAN_idx]</code>	LAN_idx - Indicate the LAN interface. 1 - LAN1 2 - LAN2 3 - LAN3 4 - LAN4
<code>e [0/1]</code>	Enable (1) or disable (0) the Vigor Bridge for WAN or/and LAN.
<code>f [0/1]</code>	Enable (1) or disable (0) the firewall functions.

Example

```
> vigbrg set -v 4 -w 1 -l 1 -e 1  
[WAN1] IPv4 bridge is enable. Set subnet[LAN1]
```

Telnet Command: `vigbrg status`

This command can show whether the Vigor Bridge Function is enabled or disabled.

Example

```
> vigbrg status  
%Vigor Bridge Function is enable!  
  
%Wan1 management is disable!
```

Telnet Command: vigbrg cfgip

This command allows users to transfer a bridge modem into ADSL router by accessing into and adjusting specified IP address. Users can access into Web UI of the router to manage the router through the IP address configured here.

vigbrg cfgip *[IP Address]*

Syntax Description

Parameter	Description
<i>IP Address</i>	It means to type an IP address for users to manage the router.

Example

```
> vigbrg cfgip 192.168.1.15
> vigbrg cfgip ?
% Vigor Bridge Config IP,
% Now: 192.168.1.15
```

Telnet Command: vigbrg wanstatus

This command can display the existed WAN connection status for the modem (change from ADSL router into bridge modem), including index number, MAC address, Stamp Time, PVC, VLAN port for Vigor Bridge Function..

Example

```
> vigbrg wanstatus
Vigor Bridge: Running
WAN mac table:
Index  MAC Address          Stamp Time      PVC      VLan
  Port
```

Telnet Command: vigbrg wlanstatus

This command can display the existed WLAN connection status for the modem (change from router into bridge modem), including index number, MAC address, Stamp Time, PVC, VLAN port for Vigor Bridge Function.

Example

```
> vigbrg wlanstatus
Vigor Bridge: Running
WAN mac table:
Index  MAC Address          Stamp Time      PVC      VLan   Port
```

Telnet Command: vlan group

This command allows you to set VLAN group. You can set four VLAN groups. Please run *vlan restart* command after you change any settings.

Syntax

vlan group *id [set/set_ex] [p1/p2/p3/p4/s1/s2/s3/s4]*

Syntax Description

Parameter	Description
<i>id</i>	It means the group 0 to 7 for VLAN.

<i>set</i>	It indicates each port can join more than one VLAN group.
<i>set_ex</i>	It indicates each port can join one VLAN group at one time.
<i>p1/p2/p3/p4</i>	It indicates LAN port 1 to LAN port 4. To group LAN1, LAN2, LAN3 and/or LAN4 under one VLAN group, please Enter the port number(s) you want.
<i>s1/s2/s3/s4</i>	It is only available for WALN models.

Example

```
> vlan group 3 set p1 s3 s4
VLAN  p1  p2  p3  p4  s1  s2  s3  s4
-----
   3   V                V   V
>
```

Telnet Command: vlan off

This command allows you to disable VLAN function.

Syntax

vlan off

Example

```
> vlan off
VLAN is Disable!
Force subnet LAN2/3/4 to be disabled!!
```

Telnet Command: vlan on

This command allows you to enable VLAN function.

Syntax

vlan on

Example

```
> vlan on
VLAN is Enable!
```

Telnet Command: vlan pri

This command is used to define the priority for each VLAN profile setting.

Syntax

vlan pri *n pri_no*

Syntax Description

Parameter	Description
<i>n</i>	It means VLAN ID number. n=VLAN ID number (from 0 to 7).
<i>pri_no</i>	It means the priority of VLAN profile. pri_no=0 -7 (from none to highest priority).

Example

```
> vlan pri 1 2
VLAN1: Priority=2
```

Telnet Command: vlan restart

This command can make VLAN settings restarted with newest configuration.

Syntax

vlan restart

Example

```
> vlan restart ?
VLAN restarts!!!
```

Telnet Command: vlan status

This command display current status for VLAN.

Syntax

vlan status

Example

```
> vlan status
VLAN is Enable :
-----
VLAN Enable VID Pri p1 p2 p3 p4 s1 s2 s3 s4 subnet
-----
0 OFF 0 0
1 OFF 0 2
2 OFF 0 0
3 OFF 0 0 V V V 1:LAN1
4 OFF 0 0
5 OFF 0 0
6 OFF 0 0
7 OFF 0 0
-----
Note: they are only untag for s1/s2/s3/s4, but they can join tag vlan
with lan
ports.
Permit untagged device in P1 to access router: ON.
```

Telnet Command: vlan subnet

This command is used to configure the LAN interface used by the VLAN group.

Syntax

vlan subnet group_id [1/2/3/4]

Syntax Description

Parameter	Description
-----------	-------------

[1/2/3/4]

It means interfaces, LAN1 ~ LAN4.

Example

```
> vlan subnet group_id 2
% Vlan Group-0 using LAN2      !

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

Telnet Command: vlan submode

This command changes the VLAN encapsulation mechanisms in the LAN driver.

Syntax

vlan submode [on/off/status]

Syntax Description

Parameter	Description
<i>on</i>	It means to enable the promiscuous mode.
<i>off</i>	It means to enable the normal mode.
<i>status</i>	It means to display if submode is normal mode or promiscuous mode.

Example

```
> vlan submode status
% vlan subnet mode : normal mode
> vlan submode on
% vlan subnet mode modified to promiscuous mode.
> vlan submode status
% vlan subnet mode : promiscuous mode
```

Telnet Command: vlan tagged

This command is used to enable or disable the incoming of untagged packets.

Syntax

vlan tagged [n] [on/off]

vlan tagged [unlimited] [on/off]

vlan tagged [p1_untag] [on/off]

Syntax Description

Parameter	Description
<i>n</i>	It means VLAN channel. The range is from 0 to 7.
<i>on/off</i>	It means to enable/disable the tagged VLAN.
[<i>unlimited</i>] [<i>on/off</i>]	unlimited on: It allows the incoming of untagged packets even all VLAN are tagged.

	unlimited off: It does not allow the incoming of untagged packets.
<i>[p1_untag] [on/off]</i>	P1_untag on: It allows the incoming of untagged packets from LAN port 1. P1_untag off: It does not allow the incoming of untagged packets from LAN port 1.

Example

```
> vlan tagged unlimited on
unlimited mode is ON
```

Telnet Command: vlan vid

This command is used to configure VID number for each VLAN channel.

Syntax

vlan vid n vid_no

Syntax Description

Parameter	Description
<i>n</i>	It means VLAN channel. The range is from 0 to 7.
<i>vid_no</i>	It means the value of VLAN ID. Enter the value as the VLAN ID number. The range is from 0 to 4095.

Example

```
> vlan vid 1 4095
VLAN1, vid=4095
```

Telnet Command: vlan sysvid

This command is used to modify and show the scope (reserved 78) of the VLAN IDs used internally by the system.

Syntax

vlan sysvid [show | n]

Syntax Description

Parameter	Description
<i>show</i>	It means to show the scope of VLAN ID used internally.
<i>n</i>	It means the value to be set as VLAN ID. The range is from 0 to 4018.

Example

```
> vlan sysvid 100
You have set system VLAN ID to range: 100 ~ 177,
We recommend that you reboot the system now.

> vlan sysvid 200
You have set system VLAN ID to range: 200 ~ 263,
We recommend that you reboot the system now.
```

```
> vlan sysvid show
The system VLAN ID is in range: 200 ~ 263
```

Telnet Command: vpn l2lset

This command allows users to set advanced parameters for LAN to LAN function.

```
vpn l2lset [list index] peerid [peerid]
vpn l2lset [list index] localid [localid]
vpn l2lset [list index]main [auto/proposal index]
vpn l2lset [list index] aggressive [g1/g2]
vpn l2lset [list index]pfs [on/off]
vpn l2lset [list index] phase1[lifetime]
vpn l2lset [list index] phase2[lifetime]
```

Syntax Description

Parameter	Description
<i>list index</i>	It means the index number of L2L (LAN to LAN) profile.
<i>peerid</i>	It means the peer identity for aggressive mode.
<i>localid</i>	It means the local identity for aggressive mode.
<i>main</i>	It means to choose proposal for main mode.
<i>auto index</i>	It means to choose default proposals.
<i>proposal index</i>	It means to choose specified proposal.
<i>aggressive</i>	It means the chosen DH group for aggressive mode
<i>pfs</i>	It means "perfect forward secrete".
<i>on/off</i>	It means to turn on or off the PFS function.
<i>phase1</i>	It means phase 1 of IKE.
<i>lifetime</i>	It means the lifetime value (in second) for phase 1 and phase 2.
<i>phase2</i>	It means phase 2 of IKE.

Example

```
> VPN l2lset 1 peerid 10226
```

Telnet Command: vpn dinset

This command allows users to configure setting for remote dial-in VPN profile.

```
vpn dinset <list index>
vpn dinset <list index> <on/off>
vpn dinset <list index> motp <on/off>
vpn dinset <list index> pin_secret <pin> <secret>
```

Syntax Description

Parameter	Description
< <i>list index</i> >	It means the index number of the profile.
< <i>on/off</i> >	It means to enable or disable the profile.

	on - Enable. off - Disable.
<i>motp <on/off></i>	It means to enable or disable the authentication with mOTP function. on - Enable. off - Disable.
<i>pin_secret<pin> <secret></i>	It means to set PIN code with secret. <i><pin></i> - Enter the code for authentication (e.g, 1234). <i><secret></i> - Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6)

Example

```

> vpn dinset 1

Dial-in profile index 1

Profile Name: ???
Status: Deactive

Mobile OTP: Disabled

Password:

Idle Timeout: 300 sec

> vpn dinset 1 on
% set profile active

> vpn dinset 1 motp on
% Enable Mobile OTP mode!>
> vpn dinset 1 pin_secret 1234 e759bb6f0e94c7ab4fe6
> vpn dinset 1

Dial-in profile index 1

Profile Name: ???
Status: Active

Mobile OTP: Enabled

PIN: 1234

Secret: e759bb6f0e94c7ab4fe6

Idle Timeout: 300 sec

```

Telnet Command: **vpn subnet**

This command allows users to specify a subnet selection for the specified remote dial-in VPN profile.

```
vpn subnet [index] [1/2/3/4/5/6]
```

Syntax Description

Parameter	Description
<index>	It means the index number of the VPN profile.
<1/2/3/4/5/6>	1 - it means LAN1 2 - it means LAN2. 3 - it means LAN3 4 - it means LAN4. 5 - it means LAN51 6 - it means LAN6.

Example

```
> vpn subnet 1 2
>
```

Telnet Command: vpn setup

This command allows users to setup VPN for different types.

Command of PPTP Dial-Out

```
vpn setup <index> <name> pptp_out <ip> <usr> <pwd> <nip> <nmask>
```

Command of IPsec Dial-Out

```
vpn setup <index> <name> ipsec_out <ip> <key> <nip> <nmask>
```

Command of L2Tp Dial-Out

```
vpn setup <index> <name> l2tp_out <ip> <usr> <pwd> <nip> <nmask>
```

Command of Dial-In

```
vpn setup <index> <name> dialin <ip> <usr> <pwd> <key> <nip> <nmask>
```

Syntax Description

Parameter	Description
For PPTP Dial-Out	
<index>	It means the index number of the profile.
<name>	It means the name of the profile.
<ip>	It means the IP address to dial to.
<usr> <pwd>	It means the user and the password required for the PPTP connection.
<nip> <nmask>	It means the remote network IP and the mask. e.g., vpn setup 1 name1 pptp_out 1.2.3.4 vigor 1234 192.168.1.0 255.255.255.0
For IPsec Dial-Out	
<index>	It means the index number of the profile.
<name>	It means the name of the profile.
<ip>	It means the IP address to dial to.
<key>	It means the value of IPsec Pre-Shared Key.
<nip> <nmask>	It means the remote network IP and the mask. e.g., vpn setup 1 name1 ipsec_out 1.2.3.4 1234 192.168.1.0

	255.255.255.0
For L2TP Dial-Out	
<index>	It means the index number of the profile.
<name>	It means the name of the profile.
<ip>	It means the IP address to dial to.
<usr> <pwd>	It means the user and the password required for the L2TP connection.
<nip> <nmask>	It means the remote network IP and the mask. e.g.,, vpn setup 1 name1 l2tp_out 1.2.3.4 vigor 1234 192.168.1.0 255.255.255.0
For Dial-In	
<index>	It means the index number of the profile.
<name>	It means the name of the profile.
<ip>	It means the IP address allowed to dial in.
<usr> <pwd>	It means the user and the password required for the PPTP/L2TP connection.
<key>	It means the value of IPsec Pre-Shared Key.
<nip> <nmask>	It means the remote network IP and the mask. e.g., vpn setup 1 name1 dialin 1.2.3.4 vigor 1234 abc 192.168.1.0 255.255.255.0

Example

```
> vpn setup 1 name1 dialin 1.2.3.4 vigor 1234 abc 192.168.1.0
255.255.255.0
% Profile Change Log ...

% Profile Index : 1
% Profile Name : name1
% Username : vigor
% Password : 1234
% Pre-share Key : abc
% Call Direction : Dial-In
% Type of Server : ISDN PPTP IPsec L2TP
% Dial from : 1.2.3.4
% Remote Network IP : 192.168.1.0
% Remote Network Mask : 255.255.255.0
>
```

Telnet Command: vpn option

This command allows users to configure settings for LAN to LAN profile.

vpn option <index> <cmd1>=<param1> [<cmd2>=<para2> | ...]

Syntax Description

Parameter	Description
<index>	It means the index number of the profile.

	Available index numbers: 1 - 32
For Common Settings	
<i><index></i>	It means the index number of the profile.
<i>pname</i>	It means the name of the profile.
<i>ena</i>	It means to enable or disable the profile. on - Enable off - Disable
<i>thr</i>	It means the way that VPN connection passes through. Available settings are w1f, w1o, w2f, and w2o. w1f - WAN1 First. w1o - WAN1 Only. w2f - WAN2 First. w2o - WAN2 Only.
<i>nnpkt</i>	It means the NetBios Naming Packet. on - Enable the function to pass the packet. off - Disable the function to block the packet.
<i>dir</i>	It means the call direction. Available settings are b, o and i. b - Both o - Dial-Out i - Dial-In.
<i>idle=[value]</i>	It means Always on and Idle Time out. Available values include: -1 - it means always on for dial-out. 0 - it means always on for dial-in. Other numbers (e.g., idle=200, idle=300, idle=500) mean the router will be idle after the interval (seconds) configured here.
<i>palive</i>	It means to enable PING to keep alive. -1 - disable the function. 1,2,3,4 - Enable the function and PING IP 1.2.3.4 to keep alive.
For Dial-Out Settings	
<i>ctype</i>	It means "Type of Server I am calling". "ctype=t" means PPTP. "ctype=s" means IPSec. "ctype= l" means L2TP(IPSec Policy None). "ctype= l1" means L2TP(IPSec Policy Nice to Have). "ctype= l2" means L2TP(IPSec Policy Must).
<i>dialto</i>	It means Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89).
<i>ltype</i>	It means Link Type. "ltype=0" means "Disable". "ltype=1" means "64kbps". "ltype=2" means "128kbps". "ltype=3" means "BOD".
<i>oname</i>	It means Dial-Out Username. "oname=admin" means to set Username = admin.
<i>opwd</i>	It means Dial-Out Password "opwd=1234" means to set Password = 1234.
<i>pauth</i>	It means PPP Authentication.

	<p>“pauth=pc” means to set PPP Authentication = PAP&CHAP. “pauth=p” means to set PPP Authentication = PAP Only</p>
<i>ovj</i>	<p>It means VJ Compression. “ovj=on/off” means to enable/disable VJ Compression.</p>
<i>okey</i>	<p>It means IKE Pre-Shared Key. “okey=abcd” means to set IKE Pre-Shared Key = abcd.</p>
<i>ometh</i>	<p>It means IPSec Security Method. “ometh=ah/” means AH. “ometh=espd/espda/” means ESP DES without/with Authentication. “ometh=esp3/esp3a/” means ESP 3DES without/with Authentication. “ometh=espa/espaa” means ESP AES without/with Authentication.</p>
<i>sch</i>	<p>It means Index(1-15) in Schedule Setup. sch=1,3,5,7 Set schedule 1->3->5->7</p>
<i>rca1lb</i>	<p>It means Require Remote to Callback. “rca1lb=on/off” means to enable/disable Set Require Remote to Callback.</p>
<i>ikeid</i>	<p>It means IKE Local ID. “ikeid=vigor” means Set Local ID = vigor.</p>
For Dial-In Settings	
<i>itype</i>	<p>It means Allowed Dial-In Type. Available settings include: “itype=t” means PPTP. “itype=s” means IPSec. “itype=L1” means L2TP (None). “itype=L1” means L2TP(Nice to Have). “itype=L2” means L2TP(Must).</p>
<i>peer</i>	<p>It means specify Peer VPN Server IP for Remote VPN Gateway. Type “203.12.23.48” means to allow VPN dial-in with IP address of 203.12.23.48. Type “off” means any remote IP is allowed to dial in.</p>
<i>peerid</i>	<p>It means the peer ID for Remote VPN Gateway. Type “draytek” means the word is used as local ID.</p>
<i>iname</i>	<p>It means Dial-in Username. “iname=admin” means to set username as “admin”.</p>
<i>ipwd</i>	<p>It means Dial-in Password. “ipwd=1234” means to set password as “1234”.</p>
<i>ivj</i>	<p>It means VJ Compression. “ivj=on/off” means to enable /disable VJ Compression.</p>
<i>ikey</i>	<p>It means IKE Pre-Shared Key. “ikey=abcd” means to set IKE Pre-Shared Key = abcd.</p>
<i>imeth</i>	<p>It means IPSec Security Method “imeth=h” means “Allow AH”. “imeth=d” means “Allow DES”. “imeth=3” means “Allow 3DES”. “imeth=a” means “Allow AES”.</p>
For TCP/IP Settings	
<i>mywip</i>	<p>It means My WAN IP.</p>

	“mywip=1.2.3.4” means to set My WAN IP as “1.2.3.4”.
<i>rgip</i>	It means Remote Gateway IP. “rgip=1.2.3.4” means to set Remote Gateway IP as “1.2.3.4”.
<i>rnip</i>	It means Remote Network IP. “rnip=1.2.3.0” means to set Remote Network IP as “1.2.3.0”.
<i>rnmask</i>	It means Remote Network Mask. “rnmask=255.255.255.0” means to set Remote Network Mask as “255.255.255.0”.
<i>rip</i>	It means RIP Direction. “rip=d” means to set RIP Direction as “Disable”. “rip=t” means to set RIP Direction as “TX”. “rip=r” means to set RIP Direction as “RX”. “rip=b” means to set RIP Direction as “Both”.
<i>mode</i>	It means the option of “From first subnet to remote network, you have to do”. “mode=r” means to set Route mode. “mode=n” means to set NAT mode.
<i>droute</i>	It means to Change default route to this VPN tunnel (Only single WAN supports this). droute=on/off means to enable/disable the function.

Example

```
> vpn option 1 idle=250
% Change Log..

% Idle Timeout = 250
```

Telnet Command: vpn mroute

This command allows users to list, add or delete static routes for a certain LAN to LAN VPN profile.

vpn mroute <index> list

vpn mroute <index> add <network ip>/<mask>

vpn mroute <index> del <network ip>/<mask>

Syntax Description

Parameter	Description
<i>list</i>	It means to display all of the route settings.
<i>add</i>	It means to add a new route.
<i>del</i>	It means to delete specified route.
<index>	It means the index number of the profile. Available index numbers: 1 - 32
<network ip>/<mask>	Enter the IP address with the network mask address.

Example

```
> vpn mroute 1 add 192.168.5.0/24
```



```
% 192.168.5.0/24
% Add new route 192.168.5.0/24 to profile 1
```

Telnet Command: vpn list

This command allows users to view LAN to LAN VPN profiles.

```
vpn list <index> all
vpn list <index>com
vpn list <index>out
vpn list <index> in
vpn list <index>net
```

Syntax Description

Parameter	Description
<i>all</i>	It means to list configuration of the specified profile.
<i>com</i>	It means to list common settings of the specified profile.
<i>out</i>	It means to list dial-out settings of the specified profile.
<i>in</i>	It means to list dial-in settings of the specified profile.
<i>net</i>	It means to list Network Settings of the specified profile.
<i><index></i>	It means the index number of the profile. Available index numbers: 1 ~ 32

Example

```
> vpn list 32 all
% Common Settings

% Profile Name           : ???
% Profile Status        : Disable
% Netbios Naming Packet : Pass
% Call Direction        : Both
% Idle Timeout          : 300
% PING to keep alive    : off

% Dial-out Settings

% Type of Server         : PPTP
% Link Type:             : 64k bps
% Username               : ???
% Password               :
% PPP Authentication     : PAP/CHAP
% VJ Compression        : on
% Pre-Shared Key        :
% IPSec Security Method : AH
% Schedule               : 0,0,0,0
% Remote Callback       : off
% Provide ISDN Number   : off
% IKE phase 1 mode      : Main mode
% IKE Local ID          :
```

```

% Dial-In Settings

--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
> vpn list 1 com
% Common Settings

% Profile Name           : ???
% Profile Status        : Disable
% Netbios Naming Packet : Pass
% Call Direction        : Both
% Idle Timeout          : 300
% PING to keep alive    : off
>

```

Telnet Command: vpn remote

This command allows users to enable or disable *PPTP/IPSec/L2TP* VPN service.

vpn remote [*PPTP/IPSec/L2TP*] [*on/off*]

Syntax Description

Parameter	Description
<i>PPTP/IPSec/L2TP</i>	There are four types to be selected.
<i>on/off</i>	on - enable VPN remote setting. off - disable VPN remote setting.

Example

```

> vpn remote PPTP on
Set PPTP VPN Service : On

Please restart the router!!

```

Telnet Command: vpn 2ndsubnet

This command allows users to enable second subnet IP as VPN server IP.

vpn 2ndsubnet *on*

vpn 2ndsubnet *off*

Syntax Description

Parameter	Description
<i>on/off</i>	It means to enable or disable second subnet.

Example

```

> vpn 2ndsubnet on
%Enable second subnet IP as VPN server IP!

```

Telnet Command: vpn trunk

This command allows users to configure VPN Backup, VPN load balance, GRE over IPsec, and Binding tunnel policy.

vpn trunk show_usable

vpn trunk backup <add/del> <name> <Member#1> <Member#2>

vpn trunk backup more_syslog <ON/OFF>

vpn trunk backup ERD <name> <Normal/Recover/Resume><second>

vpn trunk lb <add/del> <name> <Member#1> <Member#2>

vpn trunk lb more_syslog <ON/OFF>

vpn trunk lb algorithm <name> <RR>

vpn trunk lb algorithm <name><W-RR><Auto> <AccordingRatio> <Member1:Member2>

vpn trunk lb algorithm <name><Fastest>

vpn trunk bind usage <BindIndex>

vpn trunk bind show <LoadBalanceName>

vpn trunk bind reset_default

vpn trunk bind more_syslog <ON/OFF>

vpn trunk bind set <BindIndex> <ACT> <TrunkName> <Member> <SrcIp:A-B> <DstIp:A-B> <DstPort:A-B> <Proto> <Frag>

vpn trunk bind insert <After_BindIndex> <ACT> <TrunkName> <Member> <SrcIp:A-B> <DstIp:A-B> <DstPort:A-B> <Proto> <Frag>

vpn trunk SetGre show <Dialout_Index>

vpn trunk SetGre

<Active/In-active><Dialout_Index><GRE_MyIP><GRE_PeerIP><Logical_Traffic>

vpn trunk An_Gre GreIPsecAnalyze <ON/OFF>

Syntax Description

Parameter	Description
<i>show_usable</i>	Display a list of LAN to LAN dial out profiles.
<i>backup <add/del> <name> <Member#1> <Member#2></i>	Set multiple VPN tunnels (LAN to LAN profiles) as backup tunnel. add/del - Add or delete a profile for used in VPN Trunk. name - Specify the name of the VPN trunk. Member#1 - Indicate the first LAN to LAN profile. Member#2 - Indicate the second LAN to LAN profile.
<i>backup more_syslog <ON/OFF></i> <i>lb more_syslog <ON/OFF></i> <i>bind more_syslog <ON/OFF></i>	These commands are used for RD debug.
<i>backup ERD <name> <Normal/Recover/Resume><second></i>	ERD means Environment Recovers Detection. name - Specify the name of the VPN trunk. Normal - Indicate the Normal mode. All dial-out VPN TRUNK backup profiles will be activated alternatively. Recover - Indicate the duration of VPN backup operation. Resume - When VPN connection breaks down or disconnects, Member 1 will be the top priority for the system to do VPN connection. Second - "0" means to dial each six seconds automatically. "60 - 2147483647" means to early handle for less than 30 seconds within

	designated time.
<i>lb <add/del> <name> <Member#1> <Member#2></i>	It means to create VPN trunk with load balance. add/del - Add or delete a profile for used in VPN Trunk. name - Specify the name of the VPN trunk. Member#1 - Indicate the first LAN to LAN profile. Member#2 - Indicate the second LAN to LAN profile.
<i>lb algorithm <name> <RR/W-RR/Fastest></i>	Set multiple VPN tunnels for using as traffic load balance tunnel. Such command is to configure the algorithm (with round robin mode) of Load Balance. name - Specify the name of the VPN trunk. RR - It means round robin mode. All of the dial-out profiles will be taken turns equally.
<i>lb algorithm <name><W-RR><Auto> <AccordingRatio> <Member1:Member2></i>	Such command is to configure the algorithm (with round robin mode) of Load Balance. name - Specify the name of the VPN trunk. W-RR - It means weighted round robin mod based on speed ratio. <ul style="list-style-type: none"> ● <i>Auto</i> - the speed must be based on Lay2. ● <i>AccordingRatio</i> - the speed must be based on given ratio. Member#1 - Indicate the first LAN to LAN profile. Member#2 - Indicate the second LAN to LAN profile.
<i>lb algorithm <name><Fastest></i>	Such command is to configure the algorithm (with fastest mode) of Load Balance. Most of traffics will be led to the channel with the fastest connection. name - Specify the name of the VPN trunk.
<i>bind usage <BindIndex></i>	Display detailed information for VPN Load Balance Tunnel Bind. BindIndex - Indicate the index number of the tunnel bind.
<i>bind show <LoadBalanceName></i>	Display the bind information for VPN Load Balance profile. LoadBalanceName - Enter the name of VPN Load Balance profile
<i>bind reset_default</i>	Reset the bind tunnel for VPN load balance to factory reset settings.
<i>bind set <BindIndex> <ACT> <TrunkName> <Member> <SrcIp:A-B> <DstI p:A-B> <DstPort:A-B> <Proto> <Frag></i>	Set the binding tunnel policy. BindIndex - Indicate the index number (1 - 64) for the tunnel to be bound. <pre>vpn trunk bind set 1 y vpnlb 1 192.168.10.1~192.168.10.2 192.168.99.1~192.168.99.254 1~65535 0 OFF</pre> ACT - Specify the action. "y" means active; "n" means inactive or delete. TrunkName - TrunkName - Specify the name of the VPN trunk created by using "vpn trunk lb" command. Member - Specify the index number of the LAN to LAN (dial-out) profile to be bound. SrcIp:A-B - Specify the source IP range (e.g., 192.168.10.0-192.168.10.255. DstI p:A-B - Specify the destination IP range (e.g., 192.168.1.0-192.168.1.255. DstPort:A-B - Specify the destination port range (1-65535). Proto - Specify the protocol. <ul style="list-style-type: none"> 0 - any 1 - ICMP 2 - IGMP 6 - TCP 17 - UDP 255 - TCP/UDP

	Frag - "ON" means to bind the fragmented packet; "OFF" means not to care. It is the default setting.
<pre>bind insert <After_BindIndex> <ACT> <TrunkName> <Member> <SrcIp:A-B> <DstIp:A-B> <DstPort:A-B> <Proto> <Frag></pre>	<p>It is used to insert additional load balance policy into an existing policy.</p> <p>After_BindIndex - Specify an index number that new additional policy should be inserted before. See the following example:</p> <pre>vpn trunk bind insert 1 y vpnlb 2 192.168.10.3~192.168.10.200 192.168.99.200~192.168.99.200 80~80 TCP OFF</pre> <p>ACT - Specify the action. "y" means active; "n" means inactive or delete.</p> <p>TrunkName - Specify the name of the VPN trunk.</p> <p>Member - Specify the index number of the LAN to LAN (dial-out) profile to be bound.</p> <p>SrcIp:A-B - Specify the source IP range (e.g., 192.168.10.0-192.168.10.255).</p> <p>DstIp:A-B - Specify the destination IP range (e.g., 192.168.1.0-192.168.1.255).</p> <p>DstPort:A-B - Specify the destination port range (1-65535).</p> <p>Proto - Specify the protocol.</p> <ul style="list-style-type: none"> 0 - any 1 - ICMP 2 - IGMP 6 - TCP 17 - UDP 255 - TCP/UDP <p>Frag - "ON" means to bind the fragmented packet; "OFF" means not to care. It is the default setting.</p>
<pre>SetGre show <Dialout_Index></pre>	<p>Display the GRE over IPsec settings in specified LAN to LAN profile.</p> <p>Dialout_Index - Index number of the LAN to LAN (dial-out) profile.</p>
<pre>SetGre <Active/In-active><Dialout_Index><GRE_MyIP><GRE_PeerIP><Logical_Traffic></pre>	<p>Active/In-active - Specify the action. "y" means active; "n" means inactive.</p> <p>Dialout_Index - Index number of the LAN to LAN (dial-out) profile.</p> <p>GRE_MyIP - Enter the virtual IP for router itself for verified by peer.</p> <p>GRE_PeerIP - Enter the virtual IP of peer host for verified by router.</p> <p>Logical_Traffic - Specify the action for RFC2890. "y" means active; "n" means inactive.</p>
<pre>An_Gre GreIPsecAnalyze <ON/OFF></pre>	<p>These commands are used for RD debug.</p>

Example

```
> vpn setup 1 name1 pptp_out 1.2.3.4 vigor 1234 192.168.1.0 255.255.255.0
% Profile Change Log ...

% Profile Index : 1
% Profile Name : name1j
% Username : vigor
% Password : 1234
% Call Direction : Dial-Out
% Type of Server : PPTP
% Dial to : 1.2.3.4
% Remote Network IP : 192.168.1.0
% Remote Network Mask : 255.255.255.0
> vpn setup 2 market pptp_out 5.6.7.8 vigor 5678 192.168.1.31 255.255.255.0
% Profile Change Log ...

% Profile Index : 2
% Profile Name : market
```

```

% Username : vigor
% Password : 5678
% Call Direction : Dial-Out
% Type of Server : PPTP
% Dial to : 5.6.7.8
% Remote NETwork IP : 192.168.1.31
% Remote NETwork Mask : 255.255.255.0
> vpn trunk lb add comp 1 2
%% Combination VPN Load Balance profile list :
<Index> < Name > < Member1(Active)Type > <
Member2(Active)Type >
1 comp 1(YES)PPTP 2(YES)P
PTP

%% Note: <Active: NO> The LAN-to-LAN Profile is disable or under Dial-In(Call
Di
rection) at present.
=====

% Setting OK.
> vpn trunk bind set 1 y comp 2 192.168.10.1~192.168.10.2
192.168.99.1~192.168.99.254 1~65535 0 OFF
% VPN Load Balance Tunnel Bind Table Index[1] detail:
=====
Action = ACTIVE
Trunk Profile(000) Name= comp
Binding Dial Out Index = 2
Binding Src IP = 192.168.10.1 ~ 192.168.10.2
Binding Dest IP = 192.168.99.1 ~ 192.168.99.254
Binding Dest Port = 1 ~ 65535
Binding Fragmented = NO
Binding Protocol = ANY Protocol
>

```

Telnet Command: vpn NetBios

This command allows users to enable or disable NetBios for Remote Access User Accounts or LAN-to-LAN Profile.

vpn NetBios set <H2I/L2I> <index> <Block/Pass>

Syntax Description

Parameter	Description
<H2I/L2I>	H2I means Remote Access User Accounts. L2I means LAN-to-LAN Profile. Specify which one will be applied by NetBios.
<index>	The index number of the profile.
<Block/Pass>	Pass - 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, set it block data transmission of Netbios Naming Packet inside the tunnel.

Example

```

> vpn NetBios set H2I 1 Pass
% Remote Dial In Profile Index [1] :
% NetBios Block/Pass: [PASS]

```

Telnet Command: vpn mss

This command allows users to configure the maximum segment size (MSS) for different TCP types.

vpn mss show

vpn mss default

vpn mss set <connection type> <TCP maximum segment size range>

Syntax Description

Parameter	Description
<i>show</i>	It means to display current setting status.
<i>default</i>	TCP maximum segment size for all the VPN connection will be set as 1360 bytes.
<i>set</i>	Use it to specify the connection type and value of MSS.
<connection type>	1-4 represent various type. 1 - PPTP 2 - L2TP 3 - IPSec 4 - L2TP over IPSec
<TCP maximum segment size range>	Each type has different segment size range. PPTP - 1 ~ 1412 L2TP - 1 ~ 1408 IPSec - 1 ~ 1381 L2TP over IPSec - 1 ~ 1361

Example

```
>vpn mss set 1 1400
% VPN TCP maximum segment size (MSS) :
  PPTP = 1400
  L2TP = 1360
  IPSec = 1360
  L2TP over IPSec = 1360
>vpn mss show
VPN TCP maximum segment size (MSS) :
PPTP = 1400
L2TP = 1360
IPSec = 1360
L2TP over IPSec = 1360
```

Telnet Command: vpn ike

This command is used to display IKE memory status and leakage list.

vpn ike -q

Example

```
> vpn ike -q
IKE Memory Status and Leakage List
```

```
# of free L-Buffer=95, minimum=94, leak=1
# of free M-Buffer=529, minimum=529 leak=3
# of free S-Buffer=1199, minimum=1198, leak=1
# of free Msgid-Buffer=1024, minimum=1024
```

Telnet Command: vpn Multicast

This command allows users to pass or block the multi-cast packet via VPN.

```
vpn Multicast set <H2I/L2I> <index> <Block/Pass>
```

Syntax Description

Parameter	Description
<H2I/L2I>	H2I means Host to LAN (Remote Access User Accounts). L2I means LAN-to-LAN Profile.
<index>	The index number of the profile.
<Block/Pass>	Set Block/Pass the Multicast Packets. The default is Block.

Example

```
> vpn Multicast set L2I 1 Pass
% Lan to Lan Profile Index [1] :
% Status Block/Pass: [PASS]
```

Telnet Command: vpn pass2nd

This command allows users to determine if the packets coming from the second subnet passing through current used VPN tunnel.

```
vpn pass2nd[on]
```

```
vpn pass2nd [off]
```

Syntax Description

Parameter	Description
on/off	on - the packets can pass through NAT. off - the packets cannot pass through NAT.

Example

```
> vpn pass2nd on
% 2nd subnet is allowed to pass VPN tunnel!
```

Telnet Command: vpn pass2nat

This command allows users to determine if the packets passing through by NAT or not when the VPN tunnel disconnects.

```
vpn pass2nat [on]
```

```
vpn pass2nat [off]
```

Syntax Description

Parameter	Description
<i>on/off</i>	on - the packets can pass through NAT. off - the packets cannot pass through NAT.

Example

```
> vpn pass2nat on
% Packets would go through by NAT when VPN disconnect!!
```

Telnet Command: vpn sameSubnet

This command allows users to build VPN between clients via virtual subnet.

```
vpn sameSubnet -i [value]
vpn sameSubnet -E [0/1]
vpn sameSubnet -e[value]
vpn sameSubnet -I [xxx.xxx.xxx.xxx]
vpn sameSubnet -o [add/del]
vpn sameSubnet -v
```

Syntax Description

Parameter	Description
<i>-i [value]</i>	Specify the index number of VPN profile.
<i>-E [0/1]]</i>	Enable or disable the IPsec with the same subnet. 1 - enable. 0 - disable.
<i>-e [value]</i>	Translate specified LAN to virtual subnet. 1 - LAN1 2 - LAN2 3 - LAN3 ...
<i>-I [xxx.xxx.xxx.xxx]</i>	Set the virtual subnet (e.g., 172.16.3.250).
<i>-v</i>	Display current status of virtual subnet.

Example

```
> vpn sameS -i 1 -e 1 -E 1 -e 1 -I 10.10.10.0 -o add
> vpn sameS -v
IPsec with the same subnet:
VPN profile 1 enable,
% translated LAN1 to Virtual subnet: 10.10.10.0
```

Telnet Command: wan ppp_mru

This command allows users to adjust the size of PPP LCP MRU. It is used for specific network.

```
wan ppp_mru <WAN interface number> <MRU size >
```

Syntax Description

Parameter	Description
<WAN interface number>	Type a number to represent the physical interface. For Vigor130, the number is 1 (which means WAN1).
<MRU size >	It means the number of PPP LCP MRU. The available range is from 1400 to 1600.

Example

```
>wan ppp_mru 1 ?
% Now: 1492

> wan ppp_mru 1 1490
>
> wan ppp_mru 1 ?
% Now: 1490

> wan ppp_mru 1 1492
> wan ppp_mru 1 ?
% Now: 1492
```

Telnet Command: wan mtu/wan mtu2

This command allows users to adjust the size of MTU/MTU2 for WAN.

wan mtu *[value]*

wan mtu2 *[value]*

Syntax Description

Parameter	Description
<i>value</i>	It means the number of MTU for PPP. The available range is from 1000 to 1500. For Static IP/DHCP, the maximum number will be 1500. For PPPoE, the maximum number will be 1492. For PPTP/L2TP, the maximum number will be 1460.

Example

```
> wan mtu 1100
> wan mtu ?
Static IP/DHCP (Max MSS: 1500)
PPPoE(Max MSS: 1492)
PPTP/L2TP(Max MSS: 1460)
% wan ppp_mss <MSS size: 1000 ~ 1500>
% Now: 1100
```

Telnet Command: wan DF_check

This command allows you to enable or disable the function of DF (Don't fragment)

wan DF_check *[on]*

wan DF_check *[off]*

Syntax Description

Parameter	Description
<i>on/off</i>	It means to enable or disable DF.

Example

```
> wan DF_check on
%DF bit check enable!
```

Telnet Command: wan disable

This command allows you to disable WAN connection.

Example

```
> wan disable WAN
%WAN disabled.
```

Telnet Command: wan enable

This command allows you to enable WAN connection.

Example

```
> wan enable WAN
%WAN1 enabled.
```

Telnet Command: wan forward

This command allows you to enable or disable the function of WAN forwarding. The packets are allowed to be transmitted between different WANs.

`wan forward [on]`

`wan forward [off]`

Syntax Description

Parameter	Description
<i>on/off</i>	It means to enable or disable WAN forward.

Example

```
> wan forward ?
%WAN forwarding is Disable!

> wan forward on
%WAN forwarding is enable!
```

Telnet Command: wan status

This command allows you to display the status of WAN connection, including connection mode, TX/RX packets, DNS settings and IP address.

Example

```
> wan status
WAN1: Offline, stall=N
Mode: ---, Up Time=00:00:00
IP=---, GW IP=---
TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0
Primary DNS=0.0.0.0, Secondary DNS=0.0.0.0
```

```

PVC_WAN3: Offline, stall=N
Mode: ---, Up Time=00:00:00
IP=---, GW IP=---
TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0

PVC_WAN4: Offline, stall=N
Mode: ---, Up Time=00:00:00
IP=---, GW IP=---
TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0

PVC_WAN5: Offline, stall=N
Mode: ---, Up Time=00:00:00
IP=---, GW IP=---
TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0

```

Telnet Command: wan detect

This command allows you to Ping a specified IP to detect the WAN connection (static IP or PPPoE mode).

```
wan detect [wan1][on/off/always_on]
```

```
wan detect [wan1]target [ip addr]
```

```
wan detect [wan1]ttl [1-255]
```

```
wan detect status
```

Syntax Description

Parameter	Description
<i>on</i>	It means to enable ping detection. The IP address of the target shall be set.
<i>off</i>	It means to enable ARP detection (default).
<i>always_on</i>	disable link detect, always connected(only support static IP)
<i>target</i>	It means to set the ping target.
<i>ip addr</i>	It means the IP address used for detection. Type an IP address in this field.
<i>ttl</i>	It means to set the ping TTL value (work as trace route) If you do not set any value for ttl here or just type 0 here, the system will use default setting (255) as the ttl value.
<i>status</i>	It means to show the current status.

Example

```

> wan detect status
WAN1: always on
WAN2: off
WAN3: off
WAN4: off
WAN5: off
> wan detect wan1 target 192.168.1.78
Set OK

```

```

> wan detect wan1 on
Set OK

> wan detect status
WAN1: on, Target=192.168.1.78, TTL=255
WAN2: off
WAN3: off
WAN4: off
WAN5: off
>

```

Telnet Command: wan lb

This command allows you to Enable/Disable for each WAN to join auto load balance member.

wan lb [wan1/wan2/...] on

wan lb [wan1/wan2/...] off

Syntax Description

Parameter	Description
<i>wan1/wan2</i>	It means to specify which WAN will be applied with load balance.
<i>on</i>	It means to make WAN interface as the member of load balance.
<i>off</i>	It means to cancel WAN interface as the member of load balance.

Example

```

> wan lb status
WAN1: on
WAN2: on
WAN3: on
WAN4: on
WAN5: on
WAN6: on
WAN7: on

```

Telnet Command: wan mvlan

This command allows you to configure multi-VLAN for WAN and LAN. It supports pure bridge mode (modem mode) between Ethernet WAN and LAN port 2~4.

wan mvlan [pvc_no/status/save/enable/disable] [on/off/clear/tag tag_no] [service type/vlan priority] [px ...] [Keep Tag]

Syntax Description

Parameter	Description
<i>pvc_no</i>	It means index number of PVC. There are 10 PVC, 0(Channel-1) to 9(Channel-9) allowed to be configured. However, only 2 to 9 are available for configuration.
<i>status</i>	It means to display the whole Bridge status.
<i>save</i>	It means to save the configuration into flash of Vigor router.
<i>enable/disable</i>	It means to enable/disable the Multi-VLAN function.
<i>on/off</i>	It means to turn on/off bridge mode for the specific channel.

<i>clear</i>	It means to turn off/clear the port.
<i>tag tag_no</i>	It means to tag a number for the VLAN. -1: No need to add tag number. 1-4095: Available setting numbers used as tagged number.
<i>service type</i>	It means to specify the service type for VLAN. 0: Normal. 1: IGMP.
<i>vlan priority</i>	It means to specify the priority for the VALN setting. Range is from 0 to 7.
<i>px</i>	It means LAN port. Available setting number is from 2 to 4. Port number 1 is locked for NAT usage.
<i>Keep Tag</i>	It means Multi-VLAN packets will keep their VLAN headers to LAN.

Example

PVC 7 will map to LAN port 2/3/4 in bridge mode; service type is Normal. No tag added.

```
> wan mvlan 7 on p2 p3 p4
PVC Bridge p1 p2 p3 p4 p5 p6 Service Type Tag Priority Keep Tag
-----
7 ON 0 0 1 1 0 0 Normal 0(OFF) 0 OFF
>
```

Telnet Command: wan multifno

This command allows you to specify a channel (in Multi-PVC/VLAN) to make bridge connection to a specified WAN interface.

wan multifno [channel #] [WAN interface #]

wan multifno status

Syntax Description

Parameter	Description
<i>channel #</i>	There are 4 (?) channels including VLAN and PVC. Available settings are: 1=Channel 1 3=Channel 3 4=Channel 4 5=Channel 5
<i>WAN interface #</i>	Type a number to indicate the WAN interface. 1=WAN1
<i>status</i>	It means to display current bridge status.

Example

```
> wan multifno 5 1
% Configured channel 5 uplink to WAN1
> wan multifno status
% Channel 3 uplink ifno: 3
% Channel 4 uplink ifno: 3
% Channel 5 uplink ifno: 3
```

```

% Channel 6 uplink ifno: 3
% Channel 7 uplink ifno: 3
>

```

Telnet Command: wan vlan

This command allows you to tag packets on WAN VLAN with specified number.

Syntax

```

wan vlan wan [#] adsl tag [value]
wan vlan wan [#] adsl [enable/disable]
wan vlan wan [#] adsl pri[value]
wan vlan wan [#] vdsl tag [value]
wan vlan wan [#] vdsl [enable/disable]
wan vlan wan [#] vdsl pri[value]
wan vlan stat

```

Syntax Description

Parameter	Description
#	It means the number of WAN interface. 1: means WAN1 2: means WAN2.
value	It means the number to be tagged on packets. The range of the value is between 32 ~ 4095.
enable/disable	It means to enable or disable the WAN interface for VLAN.
pri[value]	It means to set priority of data transmission via 802.1q. The range of the value is between 0 ~ 7.
stat	It means to display the table of WAN VLAN status.

Example

```

> wan vlan stat
%Interface      Pri      Tag      Enabled
%=====
% WAN1 (ADSL)   0        0
% WAN1 (VDSL)   0        0
%WAN2           0        0

```

Telnet Command: wan budget

This command allows you determine the data *traffic volume* for each WAN interface respectively to prevent from overcharges for data transmission by the ISP.

Syntax

```

wan budget wan [#] rdate [day] [hour]
wan budget wan [#] [enable/disable]
wan budget wan [#] thres [budget limit (MB)]
wan budget wan [#] gthres [budget limit (GB)]
wan budget wan [#] mode [monthly/periodic/none]

```

wan budget wan [#] psday [th day in periodic]
 wan budget wan [#] action [action bitmap]
 wan budget status

Syntax Description

Parameter	Description
<i>wan[#]</i>	Specify the WAN interface.
<i>rdate</i>	Specify the WAN budget refresh time. day - Available settings are from 1 to 30. hour - Available settings are from 1 to 23. E.g., wan budget wan 1 rdate 5 10 If monthly mode is selected: WAN budget will be refreshed on 5th day at 10:00 in each month If periodic mode is selected: WAN budget will be refreshed every 5 days and 10 hours
<i>enable/disable</i>	enable - Enable the function of wan budget. disable - Disable the function of wan budget.
<i>thres [budget limit (MB)]</i>	Specify the maximum value for WAN budget limit. (Unit: MB) budget limit - Type a number.
<i>gthres [budget limit (GB)]</i>	Specify the maximum value of wan budget limit. (Unit: GB) budget limit - Type a number.
<i>mode</i> <i>[monthly periodic none]</i>	Specify the calculation mode (monthly, periodically, or none) for WAN budget.
<i>psday [th day in periodic]</i>	It is used only when mode is set with "periodic". Specify the order of "today" in the cycle. E.g., wan budget wan 5 psday → It means "today" is the 5 th day in the billing cycle.
<i>action [action bitmap]</i>	Determine the action to be performed when it reaches the WAN budget limit. <i>action bitmap</i> - Type a total number of actions to be executed. Different numbers represent different actions. 1: shutdown wan 2: send mail alert 4: send sms alert For example, if you type "5" (5=1+4), the system will send SMS alert when WAN shutdown is detected.
<i>status</i>	Display current configuration status of WAN budget.

Example

```
> wan budget wan 1 action 5
% WAN 1 budget action set to 5
> wan budget wan 1 gthres 10
% WAN 1 budget limit set to 10 GB
```

Telnet Command: wan detect_mtu

This command allows you to run a WAN MTU Discovery. The user can specify an IPv4 target to ping and find the suitable MTU size of the WAN interface.

Syntax

wan detect_mtu -w [number] -i [Host/IP address] -s [base_size] -d [decrease_size] (-c [count])

Syntax Description

Parameter	Description
-----------	-------------

<i>-w [number]</i>	Specify the WAN interface. Value: Enter the number of WAN interface. 1: WAN1; 2:WAN2....and etc.
<i>-l [Host/IP address]</i>	Specify the IPv4 target to detect. If can be an IPv4 address or domain name. Host/IP address: Enter the IP address/domain name of the target.
<i>-s [base_size]</i>	Set the MTU size base for Discovery. base_size: Available setting is 1000 ~ 1500.
<i>-d [decrease size]</i>	Set the MTU size to decrease between detections. decrease size: Available setting is 1 ~ 100.
<i>-c [count]</i>	Set the maximum times of ping failure during a Discovery. count: Available settings are 1 ~ 10. Default value is 3.

Example

```
> wan detect_mtu -w 2 -i 8.8.8.8 -s 1500 -d 30 -c 10
detecting mtu size:1500!!!

mtu size:1470!!!
```

Telnet Command: wan detect_mtu6

This command allows you to run a WAN MTU Discovery. The user can specify an IPv6 target to ping and find the suitable MTU size of the WAN interface.

Syntax

wan detect_mtu6 -w *[number]* -i *[IPv6 address]* -s *[base_size]*

Syntax Description

Parameter	Description
<i>-w [number]</i>	Specify the WAN interface number: Enter the number of WAN interface. 1: WAN1; 2:WAN2....and etc.
<i>-l [IPv6 address]</i>	Specify the IPv6 target to detect. It must be an IPv6 IP address. IPv6 address: Enter the IPv6 address of the target.
<i>-s [base_size]</i>	Specify the size of MTU. base_size: Available setting is 1000 ~ 1500.

Example

```
> wan detect_mtu6 -w 1 -i 2404:6800:4008:c06::5e -s 1500
>
```

Telnet Command: wptl

This command is used to specify an URL for accessing into or display a message when a wireless user connects to Internet through this router.

Syntax

wptl -p *<profile>* [*-l <lan>*] [*-s <ssid>*] [*-m <message>* | *-u <url>* | *-f <url>*] [*-e* | *-d*]

Syntax Description

Parameter	Description
<i>profile</i>	It means to specify one of the SSID profiles for configuration. The range is from 1 to 4.
<i>-l <lan></i>	It means to specify the LAN interface for applying the function. lan1 and lan2: -l 1,2

<code>-s <ssid></code>	It means to specify the WLAN interface (SSID1 ~ SSID4) for applying the function.
<code>-m <message></code>	Redirect to message.
<code>-u <url></code>	Redirect to url.
<code>-f <url></code>	Redirect to url and force the user to click on the button to proceed.
<code>-e</code>	Enable the profile.
<code>-d</code>	Disable the profile.
<code>-i</code>	Display the content of the profile.
<code>-c</code>	Reset all of the settings.
<code>-x <0/1/2></code>	Change the priority of the profile. 0:none 1:wptl 2:usermgt
<code>-h<0/1></code>	Disable(0)/enable(1) redirection of HTTPS.

Example

```
> wptl -e -p 1 -l 1,2 -s 1 -u http://www.draytek.com
Profile 1 enable ... [OK]
Applied LAN interfaces ... [OK]
Applied WLAN interfaces ... [OK]
Redirect to URL mode ... [OK]
>
```

Telnet Command: wl acl

This command allows the user to configure wireless access control settings.

Syntax

```
wl acl enable [ssid1 ssid2 ssid3 ssid4]
wl acl disable [ssid1 ssid2 ssid3 ssid4]
wl acl add [MAC] [ssid1 ssid2 ssid3 ssid4] [isolate]
wl acl del [MAC]
wl acl mode [ssid1 ssid2 ssid3 ssid4] [white/black]
wl acl show
wl acl showmode
wl acl clean
```

Syntax Description

Parameter	Description
<code>enable [ssid1 ssid2 ssid3 ssid4]</code>	It means to enable the settings for SSID1, SSID2, SSID3 and SSID4.
<code>disable [ssid1 ssid2 ssid3 ssid4]</code>	It means to disable the settings for SSID1, SSID2, SSID3 and SSID4.
<code>add [MAC] [ssid1 ssid2 ssid3 ssid4] [isolate]</code>	It means to associate a MAC address to certain SSID interfaces' access control settings. The isolate setting will limit the wireless client's network capabilities to accessing the wireless LAN only.

	[MAC] format: xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx or xx.xx.xx.xx.xx.xx
<i>del [MAC]</i>	It means to delete a MAC address entry defined in the access control list.
<i>mode [ssid1 ssid2 ssid3 ssid4] [white/black]</i>	It means to set white/black list for each SSID.
<i>wl acl show</i>	It means to show access control status.
<i>wl acl showmode</i>	It means to show the mode for each SSID.
<i>wl acl clean</i>	It means to clean all access control setting.

Example

```

> > wl acl showmode
ssid1: none
ssid2: none
ssid3: none
ssid4: none
> wl acl add 00-50-70-ff-12-70
Set Done !!
> wl acl add 00-50-70-ff-12-70 ssid1 ssid2 isolate
Set Done !!
> wl acl show
-----Enable Mac Address Filter-----
ssid1: dis  ssid2: dis  ssid3: dis  ssid4: dis
-----MAC Address Filter-----
Index  Attribute      MAC Address      Associated SSIDs
  0                00:50:70:ff:12:70  ssid1 ssid2 ssid3 ssid4
  1                s                00:50:70:ff:12:70  ssid1 ssid2

s: Isolate the station from LAN
>

```

Telnet Command: wl config

This command allows users to configure general settings and security settings for wireless connection.

wl config mode *[value]*

wl config mode show

wl config channel *[number]*

wl config preamble *[enable]*

wl config txburst *[enable]*

wl config ssid *[ssid_num enable ssid_name [hidden_ssid]]*

wl config security *[SSID_NUMBER] [mode]*

wl config ratectl *[ssid_num enable upload download]*

wl config isolate *[ssid_num lan member]*

Syntax Description

Parameter	Description
-----------	-------------

<i>mode[value]</i>	It means to select connection mode for wireless connection. Available settings are: "11bgn", "11gn", "11n", "11bg", "11g", or "11b".
<i>mode show</i>	It means to display what the current wireless mode is.
<i>channel [number]</i>	It means the channel of frequency of the wireless LAN. The available settings are 0,1,2,3,4,5,6,7,8,9,10,11,12 and 13. number=0, means Auto number=1, means Channel 1 number=13, means Channel 13.
<i>preamble [enable]</i>	It means to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. 0: disable to use long preamble. 1: enable to use long preamble.
<i>txburst [enable]</i>	It means to enhance the performance in data transmission about 40%* more (by enabling Tx Burst). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. 0: disable the function. 1: enable the funciton.
<i>ssid[ssid_num enable ssid_name [hidden_ssid]]</i>	It means to set the name of the SSID, hide the SSID if required. <i>ssid_num</i> : Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. <i>ssid_name</i> : Give a name for the specified SSID. <i>hidden_ssid</i> : Type 0 to hide the SSID or 1 to display the SSID
<i>Security [SSID_NUMBER] [mode][key][index]</i>	It means to configure security settings for the wireless connection. <i>SSID_NUMBER</i> : Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. <i>mode</i> : Available settings are: disable: No security. wpa1x: WPA/802.1x Only wpa21x: WPA2/802.1x Only wpamix1x: Mixed (WPA+WPA2/802.1x only) wep1x: WEP/802.1x Only wpapsk: WPA/PSK wpa2psk: WPA2/PSK wpamixpsk: Mixed (WPA+WPA2)/PSK wep: WEP <i>key, index</i> : Moreover, you have to add keys for <i>wpapsk</i> , <i>wpa2psk</i> , <i>wpamixpsk</i> and <i>wep</i> , and specify index number of schedule profiles to be followed by the wireless connection. WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8-63 ASCII text string or 64 Hexadecimal digit format.
<i>ratectl [ssid_num enable upload download]</i>	It means to set the rate control for the specified SSID. <i>ssid_num</i> : Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. <i>enable</i> : It means to enable the function of the rate control for the specified SSID. 0: disable and 1:enable. <i>upload</i> : It means to configure the rate control for data upload. The unit is kbps. <i>download</i> : It means to configure the rate control for data download. The unit is kbps.

<i>isolate [ssid_num lan member]</i>	It means to isolate the wireless connection for LAN and/or Member. <i>lan</i> - It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other. <i>member</i> - It can make the wireless clients (stations) with the same SSID not accessing for each other.
--------------------------------------	--

Example

```
> wl config mode 11bgn
Current mode is 11bgn
% <Note> Please restart wireless after you set the channel
> wl config channel 13
Current channel is 13
% <Note> Please restart wireless after you set the channel.
> wl config preamble 1
Long preamble is enabled
% <Note> Please restart wireless after you set the parameters.
> wl config ssid 1 enable dray
SSID Enable Hide_SSID Name
1 1 0 dray
% <Note> Please restart wireless after you set the parameters.
> wl config security 1 wpa1x
%% Configured Wlan Security Setting:
% SSID1
%% Mode: wpa1x
%% Wireless card must be reset for configurations to take effect
%% (Telnet Command: wl restart)
```

Telnet Command: wl set

This command allows users to configure basic wireless settings.

`wl set [SSID] [CHAN[En]]`

`wl set txburst [enable]`

Syntax Description

Parameter	Description
<i>SSID</i>	It means to Enter the SSID for the router. The maximum character that you can use is 32.
<i>CHAN[En]</i>	It means to specify required channel for the router. <i>CHAN</i> : The range for the number is between 1 - 13. <i>En</i> : type <i>on</i> to enable the function; type <i>off</i> to disable the function.
<i>txburst [enable]</i>	It means to enhance the performance in data transmission about 40%* more (by enabling Tx Burst). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. 0: disable the function. 1: enable the function.

Example

```
> wl set MKT 2 on
% New Wlan Setting is:
% SSID=MKT
```

```
% Chan=2
% Wl is Enable
```

Telnet Command: **wl act**

This command allows users to activate wireless settings.

`wl act [En]`

Syntax Description

Parameter	Description
<i>En</i>	It means to enable or disable the function of VPN isolation. 0: diable 1: enable

Example

```
> wl act on
% Set Wlan to Enable.
```

Telnet Command: **wl iso_vpn**

This command allows users to activate the function of VPN isolation.

`wl iso_vpn [ssid] [En]`

Syntax Description

Parameter	Description
<i>ssid</i>	It means the number of SSID. 1: SSID1 2: SSID2 3: SSID3 4: SSID4
<i>En</i>	It means to enable or disable the function of VPN isolation. 0: disable 1: enable

Example

```
> wl iso_vpn 1 on
% ssid: 1 isolate vpn on :1
```

Telnet Command: **wl wpa**

This command allows you to configure WPA wireless settings.

`wl wpa 1/2/3`

Syntax Description

Parameter	Description
<i>wl wpa</i>	Type 1/2/3 to represent different WPA modes. 1 - means WPA+WPA2 2 - means WPA2 Only 3 - means WPA Only

Example

```
> wl wpa 1
>
```

Telnet Command: wl wmm

This command allows users to set WMM for wireless connection. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs).

```
wl wmm ap QueIdx Aifsn Cwmin Cwmax Txop ACM
wl wmm bss QueIdx Aifsn Cwmin Cwmax Txop ACM
wl wmm ack Que0_Ack Que1_Ack Que2_Ack Que3_Ack
wl wmm enable SSID0 SSID1 SSID2 SSID3
wl wmm apsd value
wl wmm show
```

Syntax Description

Parameter	Description
<i>ap</i>	It means to set WMM for access point.
<i>bss</i>	It means to set WMM for wireless clients.
<i>ack</i>	It means to map to the Ack policy settings of AP WMM.
<i>enable</i>	It means to enable the WMM for each SSID. 0: disable 1: enable
<i>Apsd [value]</i>	It means to enable / disable the ASPD(automatic power-save delivery) function. 0: disable 1: enable
<i>show</i>	It displays current status of WMM.
<i>QueIdx</i>	It means the number of the queue which the WMM settings will be applied to. There are four queues, best effort, background, voice, and video.
<i>Aifsn</i>	It controls how long the client waits for each data transmission.
<i>Cwmin/ Cwmax</i>	CWMin means contention Window-Min and CWMax means contention Window-Max. Specify the value ranging from 1 to 15.
<i>Txop</i>	It means transmission opportunity. Specify the value ranging from 0 to 65535.
<i>ACM</i>	It can restrict stations from using specific category class if it is enabled. 0: disable 1: enable

Example

```
> wl wmm ap 0 3 4 6 0 0
  QueIdx=0: APAifsn=3,APCwmin=4,APCwmax=6, APTxop=0, APACM=0
> wl wmm enable 1 0 1 0
  WMM_SSID0 =1, WMM_SSID1 =0,WMM_SSID2 =1,WMM_SSID3 =0
> wl wmm show
  Enable WMM: SSID0 =1, SSID1 =0,SSID2 =1,SSID3 =0
```

```

APSD=0
QueIdx=0: APAifsn=3,APCwmin=4,APCwmax=6, APTxop=0,APACM=0
QueIdx=1: APAifsn=7,APCwmin=4,APCwmax=10, APTxop=0,APACM=0
QueIdx=2: APAifsn=1,APCwmin=3,APCwmax=4, APTxop=94,APACM=0
QueIdx=3: APAifsn=1,APCwmin=2,APCwmax=3, APTxop=47,APACM=0
QueIdx=0: BSSAifsn=3,BSSCwmin=4,BSSCwmax=10, BSSTxop=0,BSSACM=0
QueIdx=1: BSSAifsn=7,BSSCwmin=4,BSSCwmax=10, BSSTxop=0,BSSACM=0
QueIdx=2: BSSAifsn=2,BSSCwmin=3,BSSCwmax=4, BSSTxop=94,BSSACM=0
QueIdx=3: BSSAifsn=2,BSSCwmin=2,BSSCwmax=3, BSSTxop=47,BSSACM=0
AckPolicy[0]=0: AckPolicy[1]=0,AckPolicy[2]=0,AckPolicy[3]=0

```

Telnet Command: wl ht

This command allows you to configure wireless settings.

wl ht bw value

wl ht gi value

wl ht badecline value

wl ht autoba value

wl ht rdg value

wl ht msdu value

wl ht txpower value

wl ht antenna value

wl ht greenfield value

Syntax Description

Parameter	Description
<i>wl ht bw value</i>	The value you can type is 0 (for BW_20) and 1 (for BW_40).
<i>wl ht gi value</i>	The value you can type is 0 (for GI_800) and 1 (for GI_4001)
<i>wl ht badecline value</i>	The value you can type is 0 (for disabling) and 1 (for enabling).
<i>wl ht autoba value</i>	The value you can type is 0 (for disabling) and 1 (for enabling).
<i>wl ht rdg value</i>	The value you can type is 0 (for disabling) and 1 (for enabling).
<i>wl ht msdu value</i>	The value you can type is 0 (for disabling) and 1 (for enabling).
<i>wl ht txpower value</i>	The value you can type ranges from 1 - 6 (level).
<i>wl ht antenna value</i>	The value you can type ranges from 0-3. 0: 2T3R 1: 2T2R 2: 1T2R 3: 1T1R
<i>wl ht greenfield value</i>	The value you can type is 0 (for mixed mode) and 1 (for green field).

Example

```

> wl ht bw value 1
BW=0
<Note> Please restart wireless after you set new parameters.
> wl restart

```



```
Wireless restart.....
```

Telnet Command: wl restart

This command allows you to restart wireless setting.

Example

```
> wl restart  
Wireless restart.....
```

Telnet Command: wl wds

This command allows you to configure WDS settings.

Syntax

`wl wds mode [value]`

`wl wds security [value]`

`wl wds ap [value]`

`wl wds hello [value]`

`wl wds status`

`wl wds show`

`wl wds mac [value]`

`wl wds flush`

Syntax Description

Parameter	Description
<code>mode [value]</code>	It means to specify connection mode for WDS. [value]: Available settings are : d: Disable b: Bridge r: Repeater
<code>security [value]</code>	It means to configure security mode with encrypted keys for WDS. <i>mode</i> : Available settings are: disable: No security. wep: WEP wpapsk [key]: WPA/PSK wpa2psk [key]: WPA2/PSK <i>key</i> : Moreover, you have to add keys for <i>wpapsk</i> , <i>wpa2psk</i> , and <i>wep</i> , and specify index number of schedule profiles to be followed by the wireless connection. WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8-63 ASCII text string or 64 Hexadecimal digit format. e.g., <code>wl dual wds security disable</code> <code>wl dual wds security wep 12345</code> <code>wl dual wds security wpa2psk 12345678</code>
<code>ap [value]</code>	It means to enable or disable the AP function. Value: 1 - enable the function. 0 - disable the function.

<i>hello [value]</i>	It means to send hello message to remote end (peer). Value: 1 - enable the function. 0 - disable the function.
<i>status</i>	It means to display WDS link status for 2.4GHz connection.
<i>show</i>	It means to display current WDS settings.
<i>mac add [index addr]</i>	add [index addr] - Add the peer MAC entry in Repeater/Bridge WDS MAC table.
<i>mac clear/disable/enable [index/all]</i>	clear/disable/enable [index/all]- Clear, disable, enable the specified or all MAC entries in Repeater/Bridge WDS MAC table. e.g, <i>wl dual wds mac enable 1</i>
<i>flush</i>	It means to reset all WDS setting.

Example

```
> wl wds status
Please enable WDS hello function first.

> wl wds hello 1
% <Note> Please restart router after you set the parameters.

> wl wds status
```

Telnet Command: wl btnctl

This command allows you to enable or disable wireless button control.

wl btnctl [value]

Syntax Description

Parameter	Description
<i>value</i>	0: disable 1: enable

Example

```
> wl btnctl 1
Enable wireless button control
Current wireless button control is on
>
```

Telnet Command: wl iwpriv

This command is reserved for RD debug. Do not use them.

Telnet Command: wl set8021x

This command allows you to configure the external or internal server used by Vigor router for wireless authentication.

Syntax

wl set8021x -t [0/1]

wl set8021x -v

Syntax Description

Parameter	Description
-t	Specify the type (external or internal) of wireless authentication server. 0 - Indicate the external RADIUS server. 1- Indicate the local 802.1x server.
-v	View the settings of 802.1x.

Example

```
> wl set8021x -t 1
% <Note> Please restart wireless after you set the parameters.
> wl set8021x -v
802.1X type is : Local 802.1X
>
```

Telnet Command: wol

This command allows you to set the white list of WAN IP addresses/Subnets, that the magic packet from these IP addresses/Subnets will be eligible to pass through NAT and wake up the LAN client. You also need to set NAT rule for LAN client.

Syntax

wol up *[MAC Address]/[IP Address]*

wol fromWan *[on/off/any]*

wol fromWan_Setting *[idx][ip address][mask]*

Syntax Description

Parameter	Description
<i>MAC Address</i>	It means the MAC address of the host.
<i>IP address</i>	It means the LAN IP address of the host. If you want to wake up LAN host by using IP address, be sure that that IP address has been bound with the MAC address (IP BindMAC).
<i>on/off/any</i>	It means to enable or disable the function of WOL from WAN. on: enable off: disable any: It means any source IP address can pass through NAT and wake up the LAN client. This command will allow the user to choose whether WoL packets can be passed from the Internet to the LAN network from a specific WAN interface.
<i>[idx][ip address] [mask]</i>	It means the index number (from 1 to 4). These commands will allow the user to configure the LAN clients that the user may wake up from the Internet through the use of the WoL packet. <i>ip address</i> - It means the WAN IP address. <i>mask</i> - It means the mask of the IP address.

Example

```
> wol fromWan on
> wol fromWan_Setting 1 192.168.1.45 255.255.255.0
>
```

Telnet Command: user

The command is used to create new user account profiles.

Syntax

User set [-a|-b|-c|-d|-e|-l|-o|-q|-r|-s|-u]

user edit [PROFILE_IDX] [-a|-d|-e|-f|-i|-m|-n|-p|-q|-r|-s|-t|-u|-v|-w|-x|-A|-H|-T|-P|-I]

user account [USER_NAME] [-d|-q|-r|-t|-w]

user setdefault

Syntax Description

Parameter	Description
<i>set</i>	It means to configure general setup for the user management.
<i>edit</i>	It means to modify the selected user profile.
<i>account</i>	It means to set user account.
<i>User Set</i>	
<i>-a</i> [Profile idx][User name][IP_Address]	It means to pass an IP Address. <i>Profile idx</i> - Enter the index number of the selected profile. <i>User name</i> - Enter the user name that you want it to pass. <i>IP_Address</i> - Enter the IP address that you want it to pass.
<i>-c</i> [user name] <i>-c all</i>	Clear the user record. <i>user name</i> - Enter the user name that you want to get clear corresponding record. <i>all</i> - all of the records will be removed.
<i>-d</i>	Disable User management function.
<i>-e</i>	Enable User management function.
<i>-l all</i> <i>-l userl</i> <i>-l ip</i>	Show online user. <i>all</i> - all of the users will be displayed on the screen. <i>user name</i> - Enter the user name that you want to view on the screen. <i>ip</i> - Enter the IP address that you want to view on the screen.
<i>-o</i>	It means to show user account information. e.g., <i>-o</i>
<i>-q</i>	It means to trigger the alert tool to do authentication.
<i>-r</i> [user name all]	Remove the user record. <i>user name</i> - Enter the name of the user profile. <i>all</i> - all of the user profile settings will be removed.
<i>-s</i>	It means to set login service. 0:HTTPS 1:HTTP e.g., <i>-s 1</i>
<i>-buser</i> [user name] <i>-b ip</i> [ip address]	Block specifies user or IP address. <i>user name</i> - Enter the user name that you want to block. <i>ip address</i> -- Enter the IP address that you want to block.
<i>-u user</i> [user name] <i>-u ip</i> [ip address]	Unblock specifies user or IP address. <i>user name</i> - Enter the user name that you want to unblock. <i>ip address</i> -- Enter the IP address that you want to unblock.

<i>User edit</i>	
<i>PROFILE_IDX</i>	Enter the index number of the profile that you want to edit.
<i>-a [Param]</i>	Enable/Disable Internal RADIUS server. 0:Disable 1:Enable
<i>-d</i>	Disable User profile function.
<i>-e</i>	Enable User profile function.
<i>-f [Param]</i>	Enable/Disable Local 802.1X user. 0:Disable 1:Enable
<i>-l [Param]</i>	Set the idle time. 0:Unlimited, MAX:255. e.g., <i>-l 60</i>
<i>-m [Param]</i>	Set the maximum login user number. 0:Unlimited, MAX:2000.
<i>-n [Param]</i>	It means to set a user name for a profile. e.g., <i>-n fortest</i>
<i>-p [Param]</i>	It means to configure user password. e.g., <i>-p 60fortest</i>
<i>-q [Param]</i>	It means to set time quota (1 - 65535) of the user profile. e.g., <i>-q 200</i>
<i>-r [Param]</i>	It means to set data quota (1 - 65535) of the user profile. e.g., <i>-r 1000</i>
<i>-s [Param]</i>	It means to set schedule index . “sch_idx” could be 1 to 15.
<i>-t [Param]</i>	It means to enable /disable time quota limitation for user profile. 0:Disable 1:Enable
<i>-u [Param]</i>	It means to enable /disable data quota limitation for user profile. 0:Disable 1:Enable
<i>-v</i>	It means to view user profile(s).
<i>-w [Param]</i>	It means to specify the data quota unit (MB/GB). e.g., <i>-w MB</i>
<i>-x [Param]</i>	It means to set external server authentication 0: None 2: Radius 3: TACACS+ e.g., <i>-x 2</i>
<i>-l [Param]</i>	It means to set log type. 0: None 1: Login 2: Event 3: All
<i>-P [Param]</i>	It means to set pop browser tracking window. 0:Disable 1:Enable
<i>-T [Param]</i>	It means to set Authentication by Telnet. 0:Disable

	1:Enable
<i>-H [Param]</i>	It means to set Authentication by web page. 0:Disable 1:Enable
<i>-A [Param]</i>	It means to set Authentication by Alert Tool. 0:Disable 1:Enable
<i>User account</i>	
<i>USER_NAME</i>	It means to type a name of the user account.
<i>-d [Param]</i>	It means to enable /disable data quota limitation for user account. 0:Disable 1:Enable
<i>-q [Param]</i>	It means to set account time quota. e.g., <i>-q 200</i>
<i>-r [Param]</i>	It means to set account data quota. e.g., <i>-r 1000</i>
<i>-t [Param]</i>	It means to enable /disable time quota limitation for user account. 0:Disable 1:Enable
<i>-w [Param]</i>	It means to set data quota unit (MB/GB).
<i>setdefault</i>	Setup all of the user profiles to factory default configuration.

Example

```
>user account admin -d 0 -q 200 -r 1000 -t 1 -w MB
Disable the [admin] data quota limited
```

Telnet Command: appqos

The command is used to configure QoS for APP..

Syntax

appqos view

appqos enable[0/1]

appqos traceable [-v | -e AP_INDEX CLASS | -d AP_INDEX]

appqos untraceable

Syntax Description

Parameter	Description
<i>view</i>	It means to display current status of APP QoS.
<i>enable[0/1]</i>	It means to enable or disable the function of APP QoS.
<i>traceable/ untraceable</i>	The APPs are divided into traceable and untraceable based on their properties.
<i>-v</i>	It means to view the content of all traceable APs. Use “appqos traceable -v” to display all of the traceable APS with speficed index number. Use “appqos untraceable -v” to display all of the untraceable APS with speficed index number.

<i>-e</i>	It means to enable QoS for application(s) and assign QoS class.
<i>AP_INDEX</i>	Each index number represents one application. Index number: 50, 51, 52, 53, 54, 58, 60, 62, 63, 64, 65, 66, 68 are used for 13 traceable APPs. Index number: 0-49, 55-59, 61, 67, 69, and 70-123 are used for 125 untraceable AP.
<i>CLASS</i>	Specifies the QoS class of the application, from 1 to 4 1:Class 1, 2:Class 2, 3:Class 3, 4:Other Class
<i>-d</i>	It means to disable QoS for application(s).

Example

```
> appqos enable 1

APP QoS set to Enable.
> appqos traceable -e 68 2

TELNET: ENABLED, QoS Class 2.
```

Telnet Command: nand bad /nand usage

“NAND usage” is used to display NAND Flash usage; “nand bad” is used to display NAND Flash bad blocks.

nand bad

nand usage

Example

```
>nand usage
Show NAND Flash Usage:
Partition      Total          Used           Available      Use%
cfg            4194304        7920           4186384        0%
bin_web       33554432      11869493      21684939       35%
cfg-bak       4194304        7920           4186384        0%
bin_web-bak  33554432      11869493      21684939       35%
> nand bad
Show NAND Flash Bad Blocks:
Block  Address      Partition
1020   0x07f80000   unused
1021   0x07fa0000   unused
1022   0x07fc0000   unused
1023   0x07fe0000   unused
```