Dray Tek

Vigor2860 Series

VDSL2 Security Firewall

Your reliable networking solutions partner

User's Guide

Vigor2860 Series VDSL2 Security Firewall

User's Guide

Version: 4.0

Firmware Version: V3.8.2

(For future update, please visit DrayTek web site)

Date: November 19, 2015

Copyrights

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

Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows, Windows 95, 98, Me, NT, 2000, XP, Vista, 7 and Explorer are trademarks of Microsoft Corp.
- Apple and Mac OS are registered trademarks of Apple Inc.
- Other products may be trademarks or registered trademarks of their respective manufacturers.

Safety Instructions

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

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 tore-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Be a Registered Owner

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

Firmware & Tools Updates

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

http://www.DrayTek.com

European Community Declarations

Manufacturer: DrayTek Corp.

Address: No. 26, Fu Shing Road, Hukou Township, Hsinchu Industrial Park, Hsinchu County, Taiwan 303

Product: Vigor2860 Series Router

DrayTek Corp. declares that Vigor2860 Series of routers are in compliance with the following essential requirements and other relevant provisions of R&TTE 1999/5/EC, ErP 2009/125/EC and RoHS 2011/65/EU.

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

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

This product is designed for LTE, DSL and 2.4GHz /5GHz WLAN network throughout the EC region.

Regulatory Information

Federal Communication Commission Interference Statement

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

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

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

- (1) This device may not cause harmful interference, and
- (2) This device may accept any interference received, including interference that may cause undesired operation.

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

 $\label{lem:complex} \mbox{DrayTek Vigor2860 series VDSL2/ADSL2+ routers are compliant with 47 C.F.R.\ Part\ 68.}$



More update, please visit www.draytek.com.

Table of Contents

Part I Installation	i
I-1 Introduction	1
I-1-1 Indicators and Connectors	2
I-1-1-1 For Vigor2860 / Vigor2860L	
I-1-1-2 For Vigor2860ac / Vigor2860n-plus / Vigor2860n/Vigor2860Ln I-1-1-3 For Vigor2860Vac / Vigor2860Vn-plus	
I-2 Hardware Installation	12
I-2-1 Installing Vigor Router	12
I-2-2 Installing USB Printer to Vigor Router	13
I-3 Accessing Web Page	21
I-4 Changing Password	23
I-5 Dashboard	25
I-5-1 Virtual Panel	26
I-5-2 Name with a Link	26
I-5-3 Quick Access for Common Used Menu	27
I-5-4 Topology – Switch Management	28
I-5-5 GUI Map	29
I-5-6 Web Console	29
I-5-7 Config Backup	31
I-5-8 Logout	31
I-5-9 Online Status	32
I-5-9-1 Physical Connection	
I-6 Quick Start Wizard	35
I-6-1 For WAN1 (ADSL/VDSL2)	36
I-6-2 For WAN2 (Ethernet)/(Wireless 2.4G)	42
I-6-3 For WAN3/WAN4 (USB)	57
I-6-4 For LTE WAN	59
I-7 Service Activation Wizard	61
I-8 Registering Vigor Router	64
Part II Connectivity	67
II-1 WAN	68
Web User Interface	70
II-1-1 General Setup	70
II-1-1-1 WAN1(ADSL/VDSL2)	
II-1-1-2 WAN2 (Ethernet)/(Wireless 2.4G) II-1-1-3 WAN3/WAN4 (USB)	
II-1-2 Internet Access	
II-1-2-1 Details Page for PPPoE in WAN1 (Physical Mode: VDSL2) II-1-2-2 Details Page for MPoA/Static or Dynamic IP in WAN1 (Physical Mode: VD II-1-2-3 Details Page for PPPoE/PPPoA in WAN1 (Physical Mode: ADSL)	81 SL2) 84

II-1-2-4 Details Page for MPoA/Static or Dynamic IP in WAN1 (Physical Mode: ADSL, II-1-2-5 Details Page for PPPoE in WAN2 (Physical Mode: Ethernet)	
II-1-2-6 Details Page for Static or Dynamic IP in WAN2 (Physical Mode: Ethernet)	
II-1-2-7 Details Page for PPTP/L2TP in WAN2 (Physical Mode: Ethernet)	
II-1-2-8 Details Page for Static or Dynamic IP in WAN2 (Physical Mode: Wireless 2.4	4G)
II-1-2-9 Details Page for 3G/4G USB Modem (PPP mode) in WAN3/WAN4	. 102 10E
II-1-2-10 Details Page for 3G/4G USB Modem (DHCP mode) in WAN3/WAN4	
II-1-2-11 Details Page for 3G/4G USB Modem (DHCP mode) in LTE WAN	
II-1-2-12 Details Page for IPv6 - Offline in WAN1/WAN2/WAN3/WAN4	. 111
II-1-2-13 Details Page for IPv6 - PPP in WAN1/WAN2	
II-1-2-14 Details Page for IPv6 - TSPC in WAN1/WAN2/WAN3/WAN4	
II-1-2-15 Details Page for IPv6 - AICCU in WAN1/WAN2/WAN3/WAN4 II-1-2-16 Details Page for IPv6 - DHCPv6 Client in WAN1/WAN2	
II-1-2-17 Details Page for IPv6 - Static IPv6 in WAN1/WAN2	
II-1-2-18 Details Page for IPv6 - 6in4 Static Tunnel in WAN1/WAN2	. 119
II-1-2-19 Details Page for IPv6 - 6rd in WAN1/WAN2	. 120
II-1-3 Multi-PVC/VLAN	. 122
II-1-4 WAN Budget	. 130
II-1-4-1 General Setup	. 130
II-1-4-2 Monitor Page	. 131
Application Notes	. 133
A-1 How to configure settings for IPv6 Service in Vigor2860	. 133
II-2 LAN	. 145
Web User Interface	. 147
II-2-1 General Setup	
II-2-1-1 Details Page for LAN1 - Ethernet TCP/IP and DHCP Setup	
II-2-1-2 Details Page for LAN2 ~ LAN6 and DMZ II-2-1-3 Details Page for IP Routed Subnet	
II-2-1-3 Details Page for LAN IPv6 Setup	
II-2-2 VLAN	
II-2-3 Bind IP to MAC	. 162
II-2-4 LAN Port Mirror	. 164
II-2-5 Wired 802.1x	. 165
II-2-6 Web Portal Setup	. 166
II-3 NAT	. 169
Web User Interface	. 170
II-3-1 Port Redirection	. 170
II-3-2 DMZ Host	. 174
II-3-3 Open Ports	. 177
II-3-4 Port Triggering	. 179
II-4 Applications	. 181
Web User Interface	. 183
II-4-1 Dynamic DNS	. 183
II-4-2 LAN DNS / DNS Forwarding	. 187
II-4-3 Schedule	. 190
II-4-4 RADIUS/TACACS+	. 192
II A A A Futamal DADUIC	100

II-4-4-2 Internal RADIUS	
II-4-5 LDAP /Active Directory Setup	196
II-4-6 UPnP	
II-4-7 IGMP	
II-4-8 Wake on LAN	201
II-4-9 SMS / Mail Alert Service	202
II-4-10 Bonjour	204
Application Notes	207
A-1 How to Implement the LDAP/AD Authentication for User Management? A-2 How to Configure Customized DDNS?	
II-5 Routing	214
Web User Interface	215
II-5-1 Static Route	215
II-5-2 Load-Balance /Route Policy	220
II-5-2-1 General Setup	
II-5-2-2 Diagnose	
Application Notes	er by Using
Route Policy	231
II-6 LTE	
Web User Interface	
II-6-1 General Settings	
II-6-2 SMS Inbox	
II-6-3 Send SMS	
II-6-4 Router Commands	
	246
Part III Wireless LAN	248
III-1 Wireless LAN (2.4GHz/5GHz)	249
Web User Interface	252
III-1-1 Wireless Wizard	252
III-1-2 General Setup	256
III-1-3 Security	258
III-1-4 Access Control	260
III-1-5 WPS	261
III-1-6 WDS	264
III-1-7 Advanced Setting	267
III-1-8 Station Control	270
III-1-9 AP Discovery	271
III-1-10 Station List	272

Part IV VoIP	273
IV-1 VoIP	274
Web User Interface	276
VI-1-1 VoIP Wizard	276
VI-1-2 DialPlan	278
·	
G	
VI-1-5 Status	251
Part V VPN	
V-1 VPN and Remote Access	300
Web User Interface	301
V-1-2 VPN Server Wizard	
V-1-3 Remote Access Control	
V-1-4 PPP General Setup	
V-1-5 IPsec General Setup	
·	
V-1-9 VPN Trunk Management	
V-1-10 Connection Management	
• •	
	Between Remote Office and Headquarter via IPsec342
V-2 SSL VPN	
Web User Interface	
V-2-1 General Setup	
V-2-2 SSL Web Proxy	349
V-2-3 SSL Application	
V-2-4 User Account	
V-2-5 User Group	
V-2-6 Online User Status	
V-3 Certificate Management	
Web User Interface	
V-3-1 Local Certificate	
V-3-2 Trusted CA Certificate	
V-3-3 Certificate Backup	

V-4 Central VPN Management	368
Web User Interface	369
V-4-1 General Setup	369
V-4-1-1 General Settings	
V-4-2 CPE Management	
V-4-2-1 Managed Device List	374
V-4-3 VPN Management	377
V-4-4 Log & Alert	378
Application Notes	379
A-1 CVM Application - How to manage the CPE (router) through Vigor2860 A-2 CVM Application - How to build the VPN between remote devices and series?	<i>Vigor2860</i> 383
Part VI Security VI-1 Firewall	
Web User Interface	
VI-1-1 General Setup	
VI-1-2 Filter Setup	
VI-1-3 DoS Defense	
Application Notes	
A-1 How to Configure Certain Computers Accessing to Internet	407
VI-2 Central Security Management (CSM)	411
Web User Interface	412
VI-2-1 APP Enforcement Profile	412
VI-2-2 APPE Signature Upgrade	416
VI-2-3 URL Content Filter Profile	418
VI-2-4 Web Content Filter Profile	422
VI-2-5 DNS Filter Profile	426
Application Notes	
A-1 How to Create an Account for MyVigor	t Filter / URL
Part VII Management	441
VII-1 System Maintenance	442
Web User Interface	443
VII-1-1 System Status	443
VII-1-2 TR-069	445
VII-1-3 Administrator Password	447
VII-1-4 User Password	449
VII-1-5 Login Page Greeting	452

VII-1-6 Configuration Backup	454
VII-1-7 Syslog/Mail Alert	457
VII-1-8 Time and Date	460
VII-1-9 SNMP	461
VII-1-10 Management	463
VII-1-11 Reboot System	466
VII-1-12 Firmware Upgrade	467
VII-1-13 Modem Code Upgrade	468
VII-1-14 Activation	468
VII-1-15 Internal Service User List	470
VII-2 Bandwidth Management	471
Web User Interface	473
VII-2-1 Sessions Limit	473
VII-2-2 Bandwidth Limit	475
VII-2-3 Quality of Service	477
Application Notes	484
A-1 How to Optimize the Bandwidth through QoS Technology	
VII-3 User Management	493
Web User Interface	494
VII-3-1 General Setup	494
VII-3-2 User Profile	496
VII-3-3 User Group	501
VII-3-4 User Online Status	502
Application Notes	
A-1 How to authenticate clients via User Management	
VII-4 Central AP Management (CAM)	517
Web User Interface	518
VII-4-1 Dashboard	518
VII-4-2 Status	519
VII-4-3 WLAN Profile	520
VII-4-4 AP Maintenance	524
VII-4-5 AP Map	525
VII-4-6 Traffic Graph	528
VII-4-7 Rogue AP Detection	529
VII-4-8 Event Log	532
VII-4-9 Total Traffic	532
VII-4-10 Station Number	533
VII-4-11 Load Balance	533
VII-4-12 Function Support List	534
Application Notes	535

A-T How to use AP Management Tunction (In Vigor2860) to check AP status and WLAN profile	, ,
VII-5 External Devices	
VII-5-1 All Devices	538
Part VIII Others	540
VIII-1 Objects Settings	
Web User Interface	
VIII-1-1 IP Object	
VIII-1-2 IP Group	
VIII-1-3 IPv6 Object	
VIII-1-4 IPv6 Group	
VIII-1-5 Service Type Object	549
VIII-1-6 Service Type Group	551
VIII-1-7 Keyword Object	553
VIII-1-8 Keyword Group	555
VIII-1-9 File Extension Object	556
VIII-1-10 SMS/Mail Service Object	558
VIII-1-11 Notification Object	563
Application Notes	565
A-1 How to Send a Notification to Specified Phone Number via SMS Service in L Disconnection	
VIII-2 USB Application	569
Web User Interface	570
VIII-2-1 USB General Settings	570
VIII-2-2 USB User Management	571
VIII-2-3 File Explorer	573
VIII-2-4 USB Device Status	574
VIII-2-5 Temperature Sensor	575
VIII-2-6 Modem Support List	577
VIII-2-7 SMB Client Support List	578
Application Notes	
A-1 How can I get the files from USB storage device connecting to Vigor router	? 579
Part IX Troubleshooting	582
IX-1Diagnostics	583
Web User Interface	584
IX-1-1 Dial-out Triggering	584
IX-1-2 Routing Table	585
IX-1-3 ARP Cache Table	586
IX-1-4 IPv6 Neighbour Table	587
IX-1-5 DHCP Table	587
IX-1-6 NAT Sessions Table	588

IX-1-7 DNS Cache Table	589
IX-1-8 Ping Diagnosis	590
IX-1-9 Data Flow Monitor	591
IX-1-10 Traffic Graph	593
IX-1-11 Trace Route	594
IX-1-12 Syslog Explorer	595
IX-1-13 IPv6 TSPC Status	596
IX-1-14 DSL Status	597
IX-1-15 Authentication Information	597
IX-1-16 DoS Flood Table	599
IX-2 Checking If the Hardware Status Is OK or Not	601
IX-3 Checking If the Network Connection Settings on Your Computer Is OK or Not	602
IX-4 Pinging the Router from Your Computer	605
IX-5 Checking If the ISP Settings are OK or Not	607
IX-6 Problems for 3G/4G Network Connection	608
IX-7 Backing to Factory Default Setting If Necessary	609
IX-8 Contacting DrayTek	611
Appendix I: VLAN Applications on Vigor Router	612
Part X Telnet Commands	620
Accessing Telnet of Vigor2860	621

Part I 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.

Vigor2860 series is a VDSL2 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 VPN tunnels.

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

User Management implemented on your router firmware can allow you to prevent any computer from accessing your Internet connection without a username or password. You can also allocate time budgets to your employees within office network.

With the 6-port Gigabit switch on the LAN side provides extremely high speed connectivity for the highest speed local data transfer of any server or local PCs. The tagged VLANs (IEEE802.1Q) 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 (Multiple-Private LAN Subnets).

On the Wireless-equipped models (Vigor2860n/n plus/Vn/Vn plus) each of the wireless SSIDs can also be grouped within one of the VLANs.

In addition, Vigor2860 series supports USB interface for connecting USB printer to share printing function or 3G USB modem for network connection.

Vigor2860 series provides two-level management to simplify the configuration of network connection. The user mode allows user accessing into WEB interface via simple configuration. However, if users want to have advanced configurations, they can access into WEB interface through admin mode.



I-1-1 Indicators and Connectors

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

I-1-1-1 For Vigor2860 / Vigor2860L





ACT (Activity) Blinking Off The router is powered on and running normally. Off The router is powered off. WAN2 On Internet connection is ready. Off Blinking The data is transmitting. Oos On The QoS function is active. USB1-2 / USB On USB device is connected and ready for use. Blinking The data is transmitting. LTE On LTE device is connected and ready for use. Off LTE device is not detected, or has serious problem (e.g., no SIM card, SIM pin error, SIM deactivated, and etc.). Blinking Slowly: LTE device is in dialing up. Ouickly: The data is transmitting. DSL On The router is ready to access Internet through DSL link. Blinking Slowly: The DSL connection is ready. Ouickly: The connection is training. WCF On The Web Content Filter is active. (It is enabled from Firewall >> General Setup). VPN On The VPN tunnel is active. Off VPN services are disabled Blinking Traffic is passing through VPN tunnel. Dos On The DoS function is active. Blinking It will blink while detecting an attack. LED on Connector Left Off The port is connected. Blinking The data is transmitting. Right On The port is connected with 10010Mbps. Left On The port is connected with 10010Mbps	LED		Status	Explanation	
Off The router is powered off. WAN2 On Internet connection is ready. Off Internet connection is not ready. Blinking The data is transmitting. QoS On The QoS function is active. USB1-2 / USB On USB device is connected and ready for use. Blinking The data is transmitting. LTE On LTE device is connected and ready for use. Off LTE device is not detected, or has serious problem (e.g., no SIM card, SIM pin error, SIM deactivated, and etc.). Blinking Slowly: LTE device is in dialing up. Quickly: The data is transmitting. DSL On The router is ready to access Internet through DSL link. Blinking Slowly: The DSL connection is ready. Quickly: The connection is training. WCF On The Web Content Filter is active. (It is enabled from Firewall >> General Setup). VPN On The VPN tunnel is active. Off VPN services are disabled Blinking Traffic is passing through VPN tunnel. DoS On The DoS function is active. Blinking It will blink while detecting an attack. LED on Connector WAN2 (Giga) Right On The port is connected. Blinking The data is transmitting. Right On The port is connected with 10/100Mbps. LED Off The port is connected with 10/100Mbps					
WAN2 On Internet connection is ready. Off Internet connection is not ready. Blinking The data is transmitting. Oos On The QoS function is active. USB1-2 / USB On USB device is connected and ready for use. Blinking The data is transmitting. LTE On LTE device is connected and ready for use. Off LTE device is not detected, or has serious problem (e.g., no SIM card, SIM pin error, SIM deactivated, and etc.). Blinking Slowly: LTE device is in dialing up. Quickly: The data is transmitting. DSL On The router is ready to access Internet through DSL link. Blinking Slowly: The DSL connection is ready. Quickly: The connection is training. WCF On The Web Content Filter is active. (It is enabled from Firewall >> General Setup). VPN On The VPN tunnel is active. Off VPN services are disabled Blinking Traffic is passing through VPN tunnel. Dos On The DoS function is active. Blinking It will blink while detecting an attack. LED on Connector WAN2 (Giga) Right On The port is connected. Blinking The data is transmitting. Right On The port is connected with 1000Mbps. Left On The port is connected with 10/100Mbps				i y	
Off Internet connection is not ready. Blinking The data is transmitting. Oos On The QoS function is active. USB1-2 / USB On USB device is connected and ready for use. Blinking The data is transmitting. LTE On LTE device is connected and ready for use. Off LTE device is not detected, or has serious problem (e.g., no SIM card, SIM pin error, SIM deactivated, and etc.). Blinking Slowly: LTE device is in dialing up. Quickly: The data is transmitting. DSL On The router is ready to access Internet through DSL link. Blinking Slowly: The DSL connection is ready. Quickly: The connection is training. WCF On The Web Content Filter is active. (It is enabled from Firewall >> General Setup). VPN On The VPN tunnel is active. Off VPN services are disabled Blinking Traffic is passing through VPN tunnel. Dos On The DoS function is active. Blinking It will blink while detecting an attack. LED on Connector WAN2 LEFT On The port is connected. Off The port is disconnected. Blinking The data is transmitting. Right On The port is connected with 1000Mbps. LED Off The port is connected with 100100Mbps. Left On The port is connected with 100100Mbps.	WAND				
Blinking The data is transmitting. QoS On The QoS function is active. USB1-2 / USB On USB device is connected and ready for use. Blinking The data is transmitting. LTE On LTE device is connected and ready for use. Off LTE device is not detected, or has serious problem (e.g., no SIM card, SIM pin error, SIM deactivated, and etc.). Blinking Slowly: LTE device is in dialing up. Quickly: The data is transmitting. DSL On The router is ready to access Internet through DSL link. Blinking Slowly: The DSL connection is ready. Quickly: The connection is training. WCF On The Web Content Filter is active. (It is enabled from Firewall >> General Setup). VPN On The VPN tunnel is active. Off VPN services are disabled Blinking Traffic is passing through VPN tunnel. DoS On The DoS function is active. Blinking It will blink while detecting an attack. LED on Connector WAN2 (Giga) Eliking The data is transmitting. Right On The port is connected with 1000Mbps. Left On The port is connected with 100100Mbps Left On The port is connected.	VVAIVZ			, , , , , , , , , , , , , , , , , , ,	
USB1~2 / USB				, , , , , , , , , , , , , , , , , , ,	
USB1-2 / USB On Blinking The data is transmitting. LTE On LTE device is connected and ready for use. Off LTE device is not detected, or has serious problem (e.g., no SIM card, SIM pin error, SIM deactivated, and etc.). Blinking Slowly: LTE device is in dialing up. Quickly: The data is transmitting. DSL On The router is ready to access Internet through DSL link. Blinking Slowly: The DSL connection is ready. Quickly: The connection is training. WCF On The Web Content Filter is active. (It is enabled from Firewall >> General Setup). VPN On The VPN tunnel is active. Off VPN services are disabled Blinking Traffic is passing through VPN tunnel. DOS On The DoS function is active. Blinking It will blink while detecting an attack. LED on Connector WAN2 (Giga) Right Con The port is connected with 1000Mbps. Left On The port is connected with 10/100Mbps Left Con The port is connected with 10/100Mbps	200			Ü	
Blinking The data is transmitting. LTE On LTE device is connected and ready for use. Off LTE device is not detected, or has serious problem (e.g., no SIM card, SIM pin error, SIM deactivated, and etc.). Blinking Slowly: LTE device is in dialing up. Quickly: The data is transmitting. On The router is ready to access Internet through DSL link. Blinking Slowly: The DSL connection is ready. Quickly: The connection is training. WCF On The Web Content Filter is active. (It is enabled from Firewall >> General Setup). VPN On The VPN tunnel is active. Off VPN services are disabled Blinking Traffic is passing through VPN tunnel. DoS On The DoS function is active. Blinking It will blink while detecting an attack. LED on Connector WAN2 (Giga) Left On The port is connected. Blinking The data is transmitting. Right On The port is connected with 1000Mbps. Left On The port is connected with 10/100Mbps Left On The port is connected.					
Description	USB1~2	/ USB		,	
Off LTE device is not detected, or has serious problem (e.g., no SIM card, SIM pin error, SIM deactivated, and etc.). Blinking Slowly: LTE device is in dialing up. Quickly: The data is transmitting. DSL On The router is ready to access Internet through DSL link. Blinking Slowly: The DSL connection is ready. Quickly: The connection is training. WCF On The Web Content Filter is active. (It is enabled from Firewall >> General Setup). VPN On The VPN tunnel is active. Off VPN services are disabled Blinking Traffic is passing through VPN tunnel. DOS On The DoS function is active. Blinking It will blink while detecting an attack. LED on Connector WAN2 (Giga) Left On The port is connected. WAN2 (Giga) Right On The port is connected with 1000Mbps. LED Off The port is connected with 10/100Mbps The port is connected. The port is connected with 10/100Mbps The port is connected.				Č .	
(e.g., no SIM card, SIM pin error, SIM deactivated, and etc.). Blinking Slowly: LTE device is in dialing up. Ouickly: The data is transmitting. DSL On The router is ready to access Internet through DSL link. Blinking Slowly: The DSL connection is ready. Ouickly: The connection is training. WCF On The Web Content Filter is active. (It is enabled from Firewall >> General Setup). VPN On The VPN tunnel is active. Off VPN services are disabled Blinking Traffic is passing through VPN tunnel. DoS On The DoS function is active. Blinking It will blink while detecting an attack. LED on Connector WAN2 (Giga) Left On The port is connected. Blinking The data is transmitting. Right On The port is connected with 1000Mbps. Left On The port is connected with 10/100Mbps Left On The port is connected.	LTE			,	
Blinking Slowly: LTE device is in dialing up. Ouickly: The data is transmitting. DSL On The router is ready to access Internet through DSL link. Blinking Slowly: The DSL connection is ready. Ouickly: The connection is training. WCF On The Web Content Filter is active. (It is enabled from Firewall >> General Setup). VPN On The VPN tunnel is active. Off VPN services are disabled Blinking Traffic is passing through VPN tunnel. DoS On The DoS function is active. Blinking It will blink while detecting an attack. LED on Connector WAN2 (Giga) Left On The port is connected. Blinking The data is transmitting. Right On The port is connected with 1000Mbps. LED Off The port is connected with 10/100Mbps Left On The port is connected.			Off		
Blinking Slowly: LTE device is in dialing up.				, 0	
Ouickly: The data is transmitting. DSL On The router is ready to access Internet through DSL link. Blinking Slowly: The DSL connection is ready. Ouickly: The connection is training. WCF On The Web Content Filter is active. (It is enabled from Firewall >> General Setup). VPN On The VPN tunnel is active. Off VPN services are disabled Blinking Traffic is passing through VPN tunnel. DoS On The DoS function is active. Blinking It will blink while detecting an attack. LED on Connector WAN2 (Giga) Left On The port is connected. WAN2 (Giga) Right On The port is connected with 1000Mbps. LED Off The port is connected with 10/100Mbps Left On The port is connected. Left On The port is connected with 10/100Mbps Left On The port is connected.			DUSTS	,	
DSL On The router is ready to access Internet through DSL link. Blinking Slowly: The DSL connection is ready. Quickly: The connection is training. WCF On The Web Content Filter is active. (It is enabled from Firewall >> General Setup). VPN On The VPN tunnel is active. Off VPN services are disabled Blinking Traffic is passing through VPN tunnel. DoS On The DoS function is active. Blinking It will blink while detecting an attack. LED on Connector WAN2 (Giga) Left On The port is connected. WAN2 (Giga) Right On The port is connected with 1000Mbps. LED Off The port is connected with 10/100Mbps Left On The port is connected.			Blinking	• • • • • • • • • • • • • • • • • • • •	
Blinking Slowly: The DSL connection is ready. Quickly: The connection is training. WCF On The Web Content Filter is active. (It is enabled from Firewall >> General Setup). VPN On The VPN tunnel is active. Off VPN services are disabled Blinking Traffic is passing through VPN tunnel. DOS On The DoS function is active. Blinking It will blink while detecting an attack. LED on Connector WAN2 (Giga) Left On The port is connected. WAN2 (Giga) Right On The port is connected with 1000Mbps. LED Off The port is connected with 10/100Mbps LED Off The port is connected. The port is connected with 10/100Mbps The port is connected.	DOL			,	
Ouickly: The connection is training.	DSL			, ,	
WCF On The Web Content Filter is active. (It is enabled from Firewall >> General Setup). VPN On The VPN tunnel is active. Off VPN services are disabled Blinking Traffic is passing through VPN tunnel. DoS On The DoS function is active. Blinking It will blink while detecting an attack. LED on Connector WAN2 (Giga) Left On The port is connected. WAN2 (Giga) Right On The port is connected with 1000Mbps. LED Off The port is connected with 10/100Mbps LED Off The port is connected. The port is connected with 10/100Mbps The port is connected.			Blinking		
Firewall >> General Setup). VPN	MOE				
VPN On The VPN tunnel is active. Off VPN services are disabled Blinking Traffic is passing through VPN tunnel. Dos On The DoS function is active. Blinking It will blink while detecting an attack. LED on Connector WAN2 (Giga) Left On The port is connected. WAN2 (Giga) Right On The port is connected with 1000Mbps. LED Off The port is connected with 10/100Mbps Left On The port is connected.	WCF		On		
Off VPN services are disabled Blinking Traffic is passing through VPN tunnel. DoS On The DoS function is active. Blinking It will blink while detecting an attack. LED on Connector WAN2 (Giga) Left On The port is connected. WAN2 (Giga) Right On The port is connected with 1000Mbps. LED Off The port is connected with 10/100Mbps Left On The port is connected.	VDN		0::	• • • • • • • • • • • • • • • • • • • •	
Blinking Traffic is passing through VPN tunnel. DoS On The DoS function is active. Blinking It will blink while detecting an attack. LED on Connector WAN2 (Giga) Left On The port is connected. WED Off The port is disconnected. Blinking The data is transmitting. Right On The port is connected with 1000Mbps. LED Off The port is connected with 10/100Mbps Left On The port is connected.	VPN				
DoS On The DoS function is active. Blinking It will blink while detecting an attack. LED on Connector Left On The port is connected. WAN2 (Giga) Right On The port is disconnected. Right On The port is connected with 1000Mbps. LED Off The port is connected with 10/100Mbps LED The port is connected.					
Blinking It will blink while detecting an attack. LED on Connector UAN2 (Giga) Left On The port is connected. Blinking The data is transmitting. Right On The port is connected with 1000Mbps. LED Off The port is connected with 10/100Mbps Left On The port is connected.				· · · ·	
LED on Connector WAN2 (Giga) Left LED On Off The port is connected. Right LED On Off The port is connected with 1000Mbps. LED Off The port is connected with 10/100Mbps. LED Off The port is connected with 10/100Mbps. Left On The port is connected.	DoS				
WAN2 (Giga) Left LED Off The port is connected. Blinking The data is transmitting. Right On The port is connected with 1000Mbps. LED Off The port is connected with 10/100Mbps Left On The port is connected.			·	It will blink while detecting an attack.	
WAN2 (Giga) LED Off The port is disconnected. Blinking The data is transmitting. Right On The port is connected with 1000Mbps. LED Off The port is connected with 10/100Mbps Left On The port is connected.	LED on Connector				
(Giga) Blinking The data is transmitting. Right On The port is connected with 1000Mbps. LED Off The port is connected with 10/100Mbps Left On The port is connected.		Left	On	The port is connected.	
Right On The port is connected with 1000Mbps. LED Off The port is connected with 10/100Mbps Left On The port is connected.		LED	Off	The port is disconnected.	
LED Off The port is connected with 10/100Mbps Left On The port is connected.	(Giga)		Blinking	The data is transmitting.	
Left On The port is connected.		Right	On	The port is connected with 1000Mbps.	
Left On The port is connected.			Off		
			On	·	
	GigaL		Off	The port is disconnected.	

AN		Blinking	The data is transmitting.
1~6	Right	On	The port is connected with 1000Mbps.
	LED	Off	The port is connected with 10/100Mbps









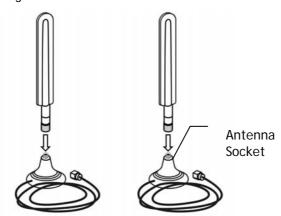
Switch on Rear Side

(Available for Vigor2860L)

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.
USB1~2 / USB	Connecter for a USB device (for 3G/4G USB Modem or printer).
VDSL/ADSL	Connecter for accessing the Internet.
WAN2	Connecter for local network devices or modem for accessing Internet.
GigaLAN (1-6)	Connecters for local network devices.
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.
SIM Card Slot	Connector for a SIM card.

Notifications for Antenna Installation (for Viogr2860L)

Magnetic antenna must be installed on the antenna socket before connecting to Vigor router.



There are two mounting holes for installing antennas with sockets on Vigor router. Please install them as shown below.



Note, if only one antenna shall be installed, please use the mounting hole (major signal transmitted hole) near to the SIM card slot.

While installing the SIM card into the card slot, note that back plate of the SIM card slot must be removed first and the direction of card notch must be on the left side.



I-1-1-2 For Vigor2860ac / Vigor2860n-plus / Vigor2860n/Vigor2860Ln



LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
WAN2	On	Internet connection is ready.
	Off	Internet connection is not ready.
	Blinking	The data is transmitting.
QoS	On	The QoS function is active.
USB	On	USB device is connected and ready for use.
	Blinking	The data is transmitting.
LTE	On	LTE device is connected and ready for use.
	Off	LTE device is not detected, or has serious problem (e.g., no SIM card, SIM pin error, SIM deactivated, and etc.).
	Blinking	Slowly: LTE device is in dialing up.
		Quickly: The data is transmitting.
DSL	On	The router is ready to access Internet through DSL link.
	Blinking	Slowly: The DSL connection is ready. Quickly: The connection is training.
WCF	On	The Web Content Filter is active. (It is enabled from Firewall >> General Setup).
2.4G/5G/WLAN	On	2.4G/5G: Wireless access point with bandwidth of 2.4GHz/5GHz is ready. WLAN: Wireless access point is ready.
	Blinking	It will blink slowly while wireless traffic goes through. ACT and WLAN LEDs blink quickly and simultaneously when WPS is working, and will return to normal condition after two minutes. (You need to setup WPS

			within 2 minutes.)	
VPN		On	The VPN tunnel is active.	
		Off	VPN services are disabled.	
		Blinking	Traffic is passing through VPN tunnel.	
DoS		On	The DoS function is active.	
		Blinking	It will blink while detecting an attack.	
LED on	LED on Connector			
	Left LED	On	The port is connected.	
WAN2		Off	The port is disconnected.	
(Giga)		Blinking	The data is transmitting.	
	Right	On	The port is connected with 1000Mbps.	
	LED	Off	The port is connected with 10/100Mbps	
GigaLA N 1~6	Left LED	On	The port is connected.	
		Off	The port is disconnected.	
		Blinking	The data is transmitting.	
	Right	On	The port is connected with 1000Mbps.	
	LED	Off	The port is connected with 10/100Mbps	













Switch on Rear Side

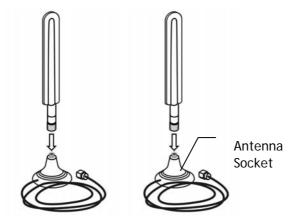
(Available for Vigor2860Ln)

Interface	Description
Wireless LAN ON/OFF/WPS	For Vigor2860n :
	 Press the button and release it within 2 seconds. When the wireless function is ready, the green LED will be on.
	 Press the button and release it within 2 seconds to turn off the WLAN function. When the wireless function is not ready, the

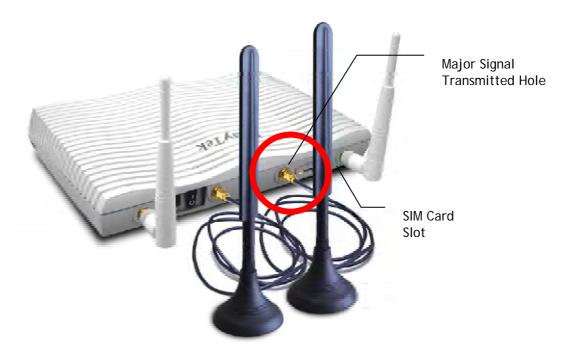
	LED will be off.
	For Vigor2860ac/Vigor2860n-plus/Vigor2860Ln:
	Wireless band will be switched /changed according to the button
	pressed and released. For example,
	2.4G (On) and 5G (On) - in default.
	2.4G (Off) and 5G (On) - pressed and released the button once.
	 2.4G (On) and 5G (Off) - pressed and released the button twice.
	 2.4G (Off) and 5G (Off) - pressed and released the button three times.
	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.
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.
USB1~2 / USB	Connecter for a USB device (for 3G/4G USB Modem or printer or
0301~27 030	thermometer).
VDSL/ADSL	Connecter for accessing the Internet.
WAN2 (Giga)	Connecter for local network devices or modem for accessing Internet.
GigaLAN (1-6)	Connecters for local network devices.
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.
SIM Card Slot	Connector for a SIM card.

Notifications for Antenna Installation (for Vigor2860Ln)

Both magnetic antennas must be installed on the antenna socket before connecting to Vigor router.



There are two mounting holes for installing antennas with sockets on Vigor router. Please install them as shown below.

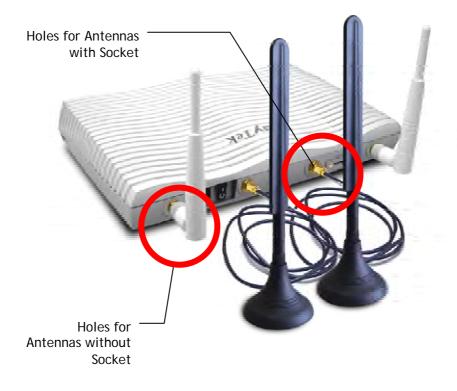


Note, if only one antenna shall be installed, please use the mounting hole (major signal transmitted hole) near to the SIM card slot.

While installing the SIM card into the card slot, note that back plate of the SIM card slot must be removed first and the direction of card notch must be on the left side.

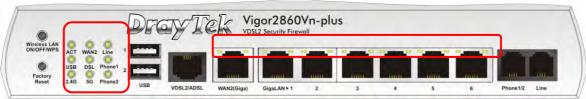


There are two types of antennas provided for Vigor2860Ln, which must be installed in different locations carefully and correctly. Wrong installation might cause bad signal of wireless connection. Therefore, pay attention to the installation of antennas by referring to the following illustration.



I-1-1-3 For Vigor2860Vac / Vigor2860Vn-plus





LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running normally.
		Off	The router is powered off.
WAN2		On	Internet connection is ready.
		Off	Internet connection is not ready.
		Blinking	The data is transmitting.
Line		On	A PSTN phone call comes (in and out). However, when the phone call is disconnected, the LED will be off.
		Off	There is no PSTN phone call.
USB		On	USB device is connected and ready for use.
		Blinking	The data is transmitting.
DSL		On	The router is ready to access Internet through DSL link.
		Blinking	Slowly: The DSL connection is ready.
			Quickly: The connection is training.
Phone1	/Phone2	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.
2.4G/50	C)	On	Wireless access point with bandwidth of 2.4GHz/5GHz is ready.
		Blinking	It will blink slowly while wireless traffic goes through. ACT and WLAN LEDs blink quickly and simultaneously when WPS is working, and will return to normal condition after two minutes. (You need to setup WPS within 2 minutes.)
LED on	Connecto	or	
	Left LED	On	The port is connected.
WAN2		Off	The port is disconnected.
(Giga)		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps
GigaL	Left	On	The port is connected.
	LED	Off	The port is disconnected.
AN		Blinking	The data is transmitting.
1~6	Right	On	The port is connected with 1000Mbps.
	LED	Off	The port is connected with 10/100Mbps







Interface	Description	
Wireless LAN ON/OFF/WPS	Wireless band will be switched /changed according to the button pressed and released. For example,	
	• 2.4G (On) and 5G (On) - in default.	
	 2.4G (Off) and 5G (On) - pressed and released the button once. 	
	 2.4G (On) and 5G (Off) - pressed and released the button twice. 	
	 2.4G (Off) and 5G (Off) - pressed and released the button three times. 	
	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.	
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.	
USB	Connecter for a USB device (for 3G/4G USB Modem or printer).	
VDSL/ADSL	Connecter for accessing the Internet.	
WAN2 (Giga)	Connecter for local network devices or modem for accessing Internet.	
GigaLAN (1-6)	Connecters for local network devices.	
Phone 1/2	Connecter for analog phone(s).	
Line	Connector for PSTN life line.	
PWR	Connecter for a power adapter.	
ON/OFF	Power Switch.	

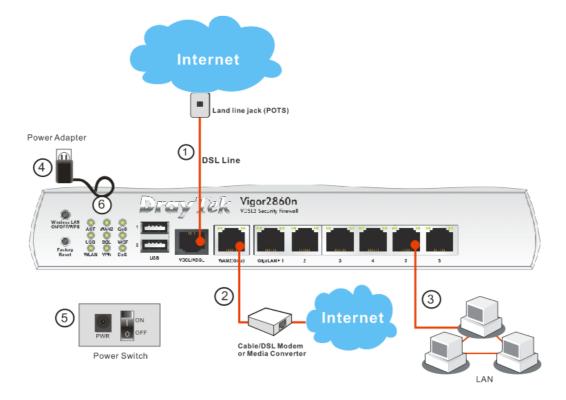
I-2 Hardware Installation

I-2-1 Installing Vigor Router

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

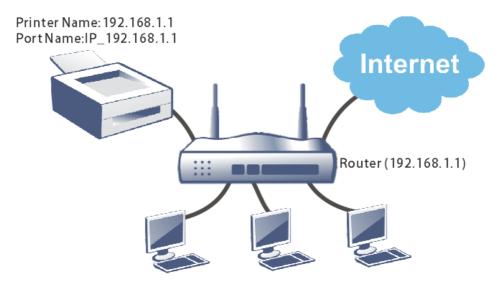
- 1. Connect the DSL interface to the land line jack with a DSL line cable.
- 2. Connect the cable Modem/DSL Modem/Media Converter to the WAN port of router with Ethernet cable (RJ-45).
- 3. Connect one end of an Ethernet cable (RJ-45) to one of the LAN ports of the router and the other end of the cable (RJ-45) into the Ethernet port on your computer.
- 4. Connect one end of the power adapter to the router's power port on the rear panel, and the other side into a wall outlet.
- 5. Power on the device by pressing down the power switch on the rear panel.
- 6. The system starts to initiate. After completing the system test, the ACT LED will light up and start blinking.

(For the hardware connection, we take "n" model as an example.)



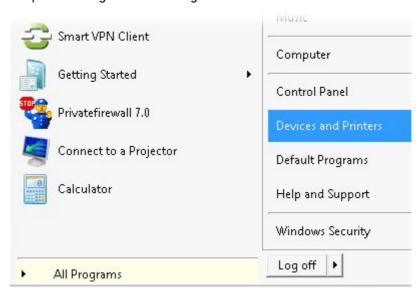
I-2-2 Installing USB Printer to Vigor Router

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).

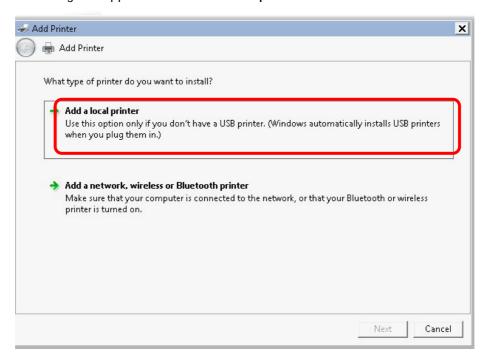
- 1. Connect the printer with the router through USB/parallel port.
- 2. Open All Programs>>Getting Started>>Devices and Printers.



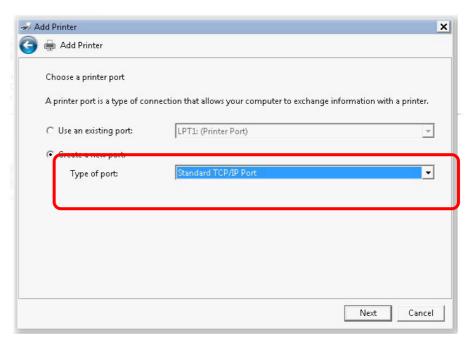
3. Click Add a printer.



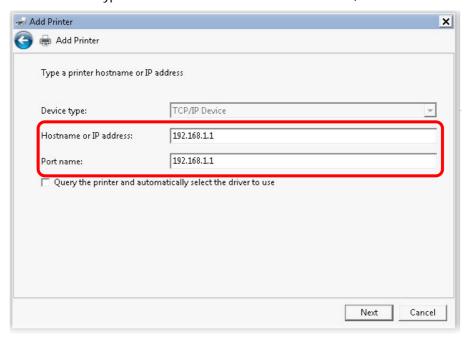
4. A dialog will appear. Click Add a local printer and click Next.



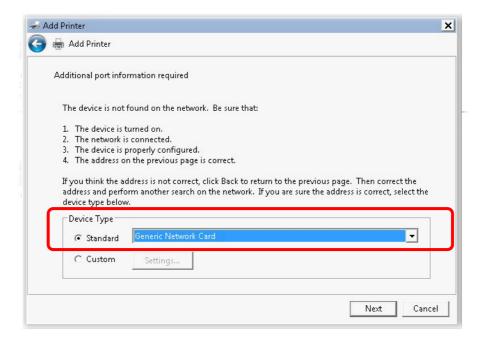
5. In this dialog, choose Create a new port. In the field of Type of port, use the drop down list to select Standard TCP/IP Port. Then, click Next.



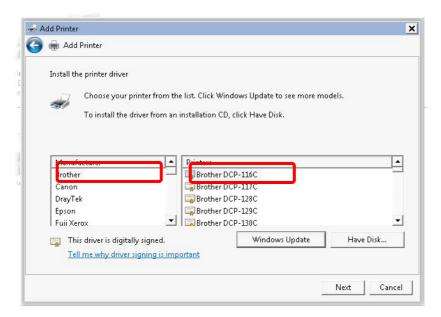
6. In the following dialog, type 192.168.1.1 (router's LAN IP) in the field of Hostname or IP Address and type 192.168.1.1 as the Port name. Then, click Next.



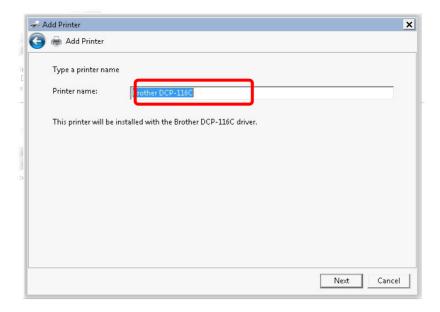
7. Click Standard and choose Generic Network Card.



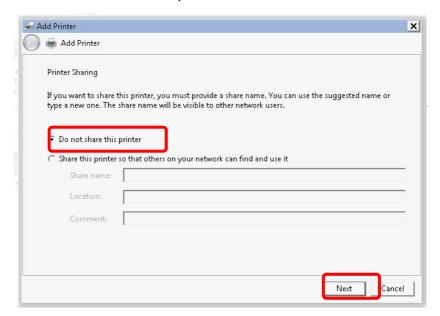
8. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click Next.



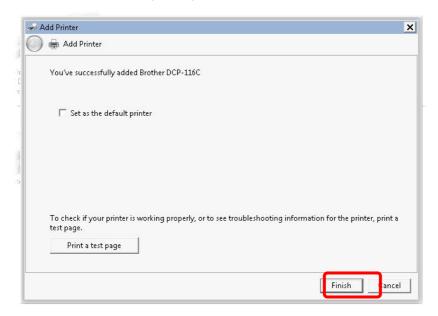
9. Type a name for the chosen printer. Click Next.



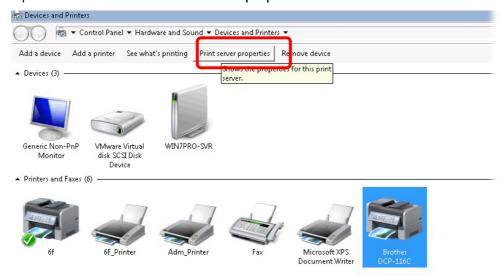
10. Choose Do not share this printer and click Next.



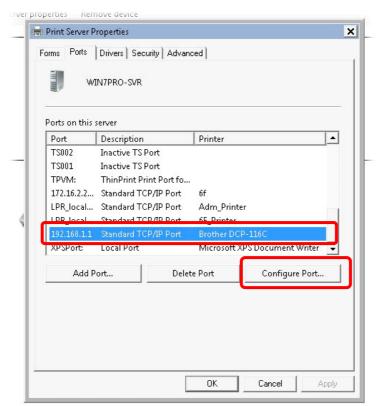
11. Then, in the following dialog, click Finish.



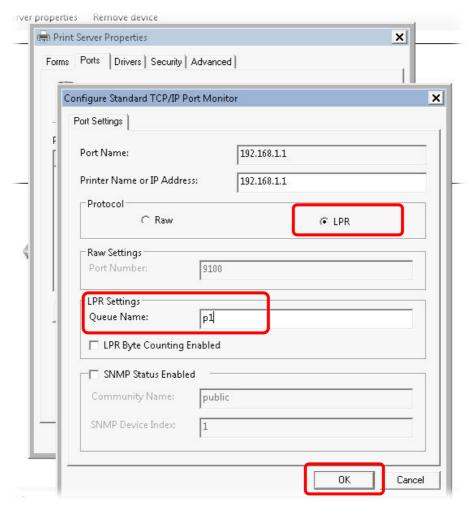
12. The new printer has been added and displayed under **Printers and Faxes**. Click the new printer icon and click **Printer server properties**.



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



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



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



Info

Some printers with the fax/scanning or other additional functions are not supported. If you do not know whether your printer is supported or not, please visit www.draytek.com to find out the printer list. Open Support >FAQ/Application Notes; find out the link of USB>>Printer Server and click it.



Then, click the What types of printers are compatible with Vigor router?



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

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.



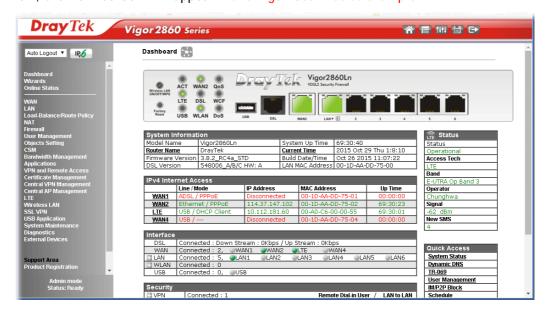
3. Please type "admin/admin" as the Username/Password and click Login.



Info

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

4. Now, the Main Screen will appear. Take Vigor2860Ln as as example.

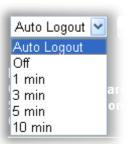




Info

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

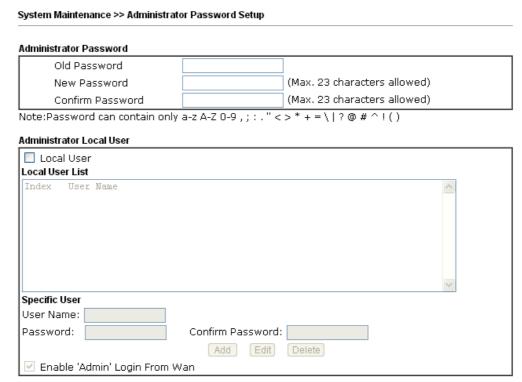
5. The web page can be logged out according to the chosen condition. The default setting is **Auto Logout**, which means the web configuration system will logout after 5 minutes without any operation. Change the setting for your necessity.



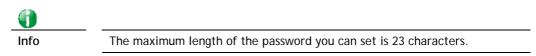
I-4 Changing Password

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.



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.



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





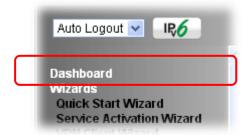
Info

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

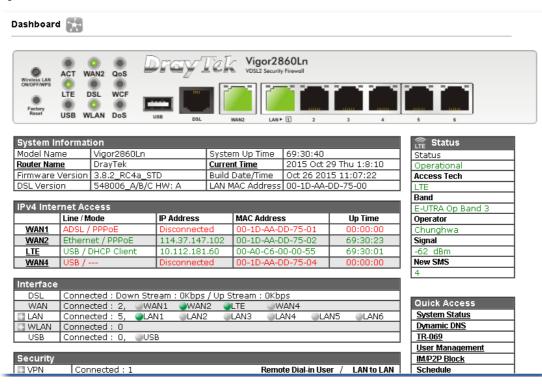
I-5 Dashboard

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:



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, VDSL/ADSL, WAN2, or LAN1 - LAN6, related web setting page will be open for you to configure if required.

Dashboard



Port	Color	Description
USB	Black	No USB device is connected.
	Green	A USB device is connected.
VDSL/ADSL	Black	No VDSL/ADSL connection.
	Green	ADSL connection is ready.
	Orange	VDSL connection is ready.
WAN2(Giga)	Black	WAN2 port is disconnected.
	Green	WAN2 port is connected at 10/100 Mbps.
	Orange	WAN2 port is connected at 1 Gbps.
GigaLAN	Black	LAN port is disconnected.
1 ~ 6	Green	LAN port is connected at 10/100 Mbps.
	Orange	LAN port is connected at 1 Gbps.

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., <u>Router Name</u>, <u>Current Time</u>, <u>WAN1~4</u> and etc.) below means you can click it to open the configuration page for modification.

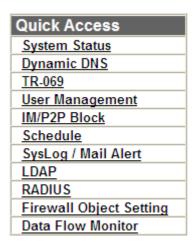
System Information			
Model Name	Vigor2860Ln	System Up Time	69:34:53
Router Name	DrayTek	<u>Current Time</u>	2015 Oct 29 Thu 1:12:26
Firmware Version	3.8.2_RC4a_STD	Ruild Date/Time	Oct 26 2015 11:07:22
DSL Version	548006_A/B/C HW: A	LAN MAC Address	00-1D-AA-DD-75-00

IPv4 Internet Access				
	Line / Mode	IP Address	MAC Address	Up Time
WAN1	ADSL / PPPoE	Disconnected	00-1D-AA-DD-75-01	00:00:00
WAN2	Ethernet / PPPoE	114.37.147.102	00-1D-AA-DD-75-02	69:34:36
<u>LTE</u>	USB / DHCP Client	10.112.181.60	00-A0-C6-00-00-55	69:34:14
WAN4	USB /	Disconnected	00-1D-AA-DD-75-04	00:00:00

I-5-3 Quick Access for Common Used Menu

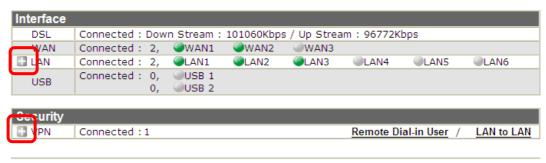
All the menu items can be accessed and arranged orderly on the left side of the main page for your request. However, some **important** and **common** used menu items which can be accessed in a quick way just for convenience.

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



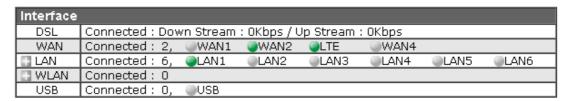
The function links of System Status, Dynamic DDNS, TR-069, User Management, IM/P2P Block, Schedule, Syslog/Mail Alert, LDAP, RADIUS, Firewall Object Setting and Data Flow Monitor are displayed here. Move your mouse cursor on any one of the links and click on it. The corresponding setting page will be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



User Mode is OFF now.

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
■ MyVigor	Activate : 0	

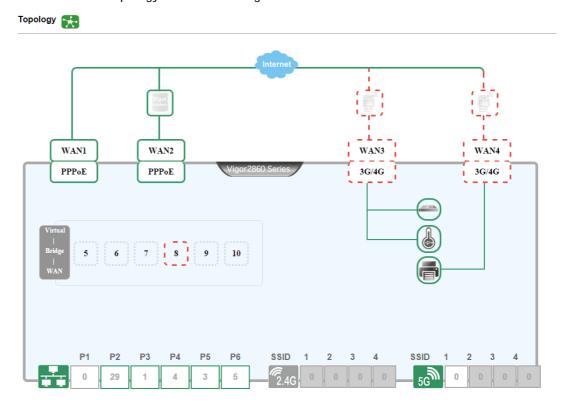
Host connected physically to the router via LAN port(s) will be displayed with green circles in the field of Connected.

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 Topology - Switch Management

A visualized dashboard is provided for the router's administrator or users to have a quick view of WAN/LAN installation, USB devices installation and software configuration. From this page, the router's administrator or users can quicky check if hardware connection (WAN connection, LAN connection) is well or not. In addition, by moving the mouse cursor on specified icons (e.g., SSID 2.4G, SSID 5G) on the dashboard, corresponding information will be open by tip window. Moreover, move the mouse cursor on the icon (e.g., Phone 1, Phone 2, DialPlan and SIP Accounts) displayed on the screen, the system will open related configuration web page immediately.

Below shows the topology of switch management:



I-5-5 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.

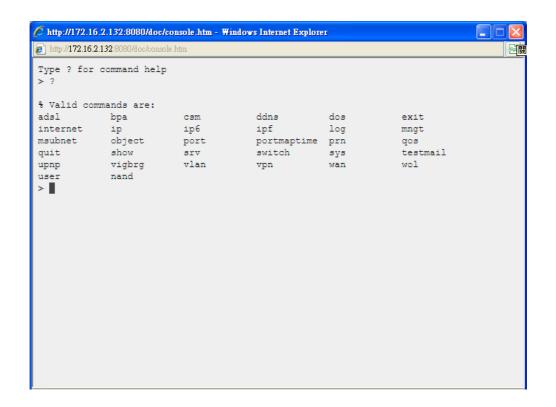
<u>Dashboard</u> Wizards	Quick Start Wizard Service Activation Wizard	VPN and Remote Access	Remote Access Control
	Service Activation Wizard	1100000	Domete Access Control
	Service Activation Wizard		
			PPP General Setup
	VPN Client Wizard		IPsec General Setup
	VPN Server Wizard		IPsec Peer Identity
	Wireless Wizard		Remote Dial-in User
	VoIP Wizard		LAN to LAN
Online Status			VPN TRUNK
	Physical Connection		Management
	Virtual WAN		Connection Management
WAN		Certificate Management	
	<u>General Setup</u>		Local Certificate
	Internet Access		Trusted CA Certificate
	Multi-PVC/VLAN		Certificate Backup
LAN		Central VPN	
	<u>General Setup</u>	Management	
	Static Route		General Setup
	<u>VLAN</u>		CPE Management
	Bind IP to MAC		<u>VPN Management</u>
	LAN Port Mirror		Log & Alert
	Wired 802.1x	Central AP Management	
	Web Portal Setup		<u>Status</u>
<u>Load-Balance/Route</u>			WLAN Profile
Policy Policy			AP Maintenance
NAT			AP Map
	Port Redirection		Traffic Graph
	Onen Porte		Roque AP Detection

I-5-6 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.

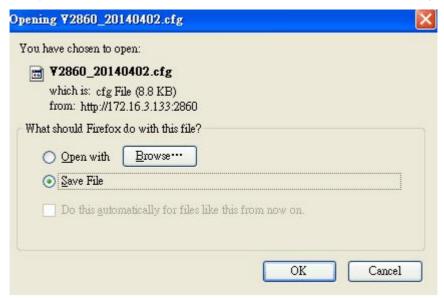


I-5-7 Config Backup



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 and a pop up dialog will appear.



Click Save to store the setting.

I-5-8 Logout



Click this icon to exit the web user interface.

I-5-9 Online Status

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

Physical Connection				System U	lptime: 2days 21:51
IF	Pv4	. ,	IPv6		
LAN Status	Primai	y DNS: 168.9	5.1.1	Secondary D	NS: 168.95.192.
IP Address	TX Packets	RX Paci	kets		
172.17.11.1	19726675	21538:	211		
WAN 1 Status					>> <u>Dial PPPol</u>
Enable	Line	Name	Mode	Up Time	
Yes	VDSL2		PPPoE	00:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
		0	0	0	0
WAN 2 Status					>> <u>Drop PPPol</u>
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	69:50:48	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
114.37.147.102	168.95.98.254	7908095	8233	9231157	3647
LTE Status					>> Release
Enable	Line	Name	Mode	Up Time	
Yes	USB		DHCP Client	69:50:26	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
10.112.181.60	10.112.181.61	3053505	2330	3454825	12068
USB Modem Status	Base Station II) Signal 9	Strength(RSSI)	Signal Quality(Cl	NR) NetWork Mode
Device Opera	ational 00:A0:C6:00:	:01:55 -62 dB	m :	38 dB	4G/3G/20
				(99%)	
WAN 4 Status	1:	N		Un Time	CiI
Enable	Line	Name	Mode	Up Time	Signal
Yes IP	USB GW IP	TV Dackets	TV Date/Dec\	00:00:00 RX Packets	- DV Dato/Dno\
IF	OVY IP	TX Packets	TX Rate(Bps)	na Packets	RX Rate(Bps)
		U	U	U	0

Physical Connection for IPv6 Protocol

Online Status				
Physical Connecti	System Uptime: 0:1:18			
	IPv4		IPv6	-
LAN Status				
IP Address				
	00:83E4:21D:AAFF FF:FEA6:2568/64 (L		obal)	
TX Packets	RX Packets	TX Bytes	RX Bytes	
147	187	34205	19176	
WAN2 IPv6 Status	3			
Enable	Mode	Up Time		
Yes	AICCU	0:00:48		
IP			Gateway IP	
	:00:3E4::2/64 (Glob F00:3E4:2/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes	
186	137	16438	33093	

Detailed explanation (for IPv4) is shown below:

Item	Description
LAN Status	Primary DNS- Displays the primary DNS server address for WAN interface.
	Secondary DNS -Displays the secondary DNS server address for WAN interface.
	IP Address-Displays the IP address of the LAN interface.
	TX Packets-Displays the total transmitted packets at the LAN interface.
	RX Packets-Displays the total received packets at the LAN interface.
WAN1/WAN2/WAN3 /WAN4 Status	Enable - Yes in red means such interface is available but not enabled. Yes in green means such interface is enabled.
	Line - Displays the physical connection (VDSL, ADSL, Ethernet, or USB) of this interface.
	Name - Display the name of the router.
	Mode - Displays the type of WAN connection (e.g., PPPoE).
	Up Time - Displays the total uptime of the interface.
	IP - Displays the IP address of the WAN interface.
	GW IP - Displays the IP address of the default gateway.
	TX Packets - Displays the total transmitted packets at the WAN interface.
	TX Rate - Displays the speed of transmitted octets at the WAN interface.
	RX Packets - Displays the total number of received packets at the WAN interface.
	RX Rate - Displays the speed of received octets at the WAN interface.

Detailed explanation (for IPv6) is shown below:

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



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

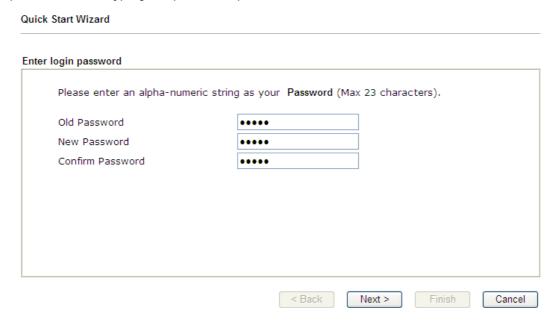
Such page displays the virtual WAN connection information.

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

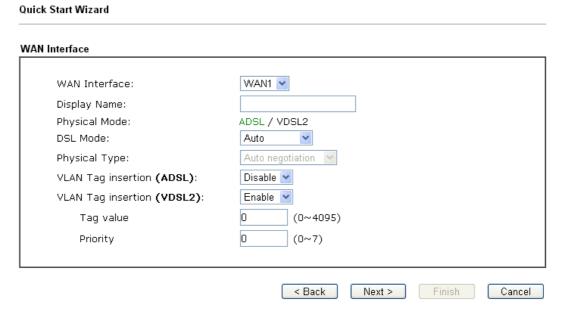
The field of Application will list the purpose of such WAN connection.

I-6 Quick Start Wizard

Quick Start Wizard can help you to deploy and use the router easily and quickly. Go to Wizards>>Quick Start Wizard. The first screen of Quick Start Wizard is entering login password. After typing the password, please click Next.



On the next page as shown below, please select the WAN interface that you use. If DSL interface is used, please choose WAN1; if Ethernet interface is used, please choose WAN2; if 3G USB modem is used, please choose WAN3 or WAN4; if LTE SIM card is used, please choose LTE. Then click Next for next step.



WAN1, WAN2, WAN3/LTE and WAN4 will bring up different configuration page. Refer to the following for detailed information. In which, WAN3 will be treated as USB WAN or LTE WAN according to the USB modem or SIM Card used for accessing Internet.

I-6-1 For WAN1 (ADSL/VDSL2)

WAN1 is specified for ADSL or VDSL2 connection.

Quick Start Wizard

WAN Interface:	WAN1 V
Display Name:	
Physical Mode:	ADSL / VDSL2
DSL Mode:	VDSL2 only ▼
Physical Type:	Auto negotiation
VLAN Tag insertion (VDSL2):	Enable 💌
Tag value	0 (0~4095)
Priority	0 (0~7)

Available settings are explained as follows:

Item	Description
Display Name	Type a name to identify such WAN.
DSL Mode	Specify the physical mode (VDSL2 only or ADSL only) for such router manually.
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 type the tag value and specify the priority for the packets sending by WAN1.
	Disable - Disable the function of VLAN with tag.
	Tag value - Type the value as the VLAN ID number. The range is from 0 to 4095.
	Priority - Type the packet priority number for such VLAN. The range is from 0 to 7.

You have to 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. In addition, the field of For ADSL Only will be available only when ADSL is detected. Then click Next for next step.

PPPoE/PPPoA

Quick Start Wizard

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

Connect to Internet WAN 1 PPPoE/PPPoA Protocol ~ For ADSL Only: PPPoE LLC/SNAP 💌 Encapsulation VPI 0 Auto detect VCI 33 Fixed IP O Yes O No(Dynamic IP) IP Address Subnet Mask Default Gateway 8.8.8.8 Primary DNS Second DNS 8.8.4.4 < Back Next > Finish Cancel

Item	Description
Protocol	There are two modes offered for you to choose for WAN1 interface. PPPoE / PPPoA PPPoE / PPPoA MPoA / Static or Dynamic IP Choose PPPoE/PPPoA as the protocol.
For ADSL Only	Such field is provided for ADSL only. You have to choose encapsulation and type the values for VPI and VCI. Or, click Auto detect to find out the best values. PPPoE LLC/SNAP PPPoE LLC/SNAP PPPoA VC MUX PPPoA VC MUX
Fixed IP	Click Yes to enable Fixed IP feature.
IP Address	Type the IP address if Fixed IP is enabled.
Subnet Mask	Type the subnet mask.
Default Gateway	Type the IP address as the default gateway.
Primary DNS	Type in the primary IP address for the router.
Secondary DNS	Type in secondary IP address for necessity in the future.
Back	Click it to return to previous setting page.

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

After finished the above settings, simply click Next. Manually enter the Username/Password provided by your ISP

Quick Start Wizard

WAN 1	
Service Name (Optional)	СНТ
Username	84005755@hinet.net
Password	•••••
Confirm Password	••••

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

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

WAN1

Please confirm your settings:

WAN Interface:

Quick Start Wizard

 Physical Mode:
 ADSL

 VPI:
 8

 VCI:
 35

 Protocol / Encapsulation:
 PPPOE / LLC

 Fixed IP:
 No

 Primary DNS:
 8 8 8 8

 Fixed IP:
 No

 Primary DNS:
 8.8.8.8

 Secondary DNS:
 8.8.4.4

< Back	Next >	Finish	Cancel

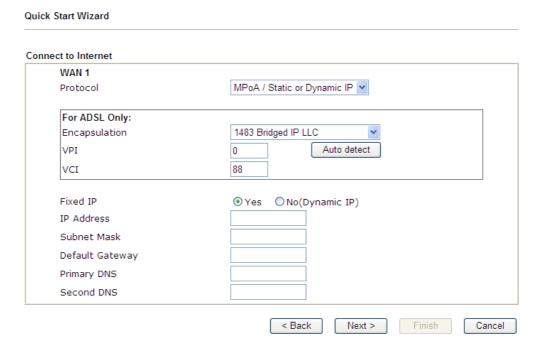
4. Click Finish. A page of Quick Start Wizard Setup OK!!! will appear. Then, the system status of this protocol will be shown.

Quick Start Wizard Setup OK!

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

MPoA / Static or Dynamic IP

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



Item	Description
Protocol	There are two modes offered for you to choose for WAN1 interface. MPoA / Static or Dynamic IP PPPoE / PPPoA MPoA / Static or Dynamic IP Choose MPoA / Static or Dynamic IP as the protocol.
For ADSL Only	Such field is provided for ADSL only. You have to choose encapsulation and type the values for VPI and VCI. Or, click Auto detect to find out the best values. 1483 Bridged IP LLC 1483 Bridged IP LLC 1483 Routed IP LLC 1483 Bridged IP VC-Mux 1483 Routed IP VC-Mux (IPoA) 1483 Bridged IP (IPoE) Yes No(Dynamic IP)
Fixed IP	Click Yes to enable Fixed IP feature.
IP Address	Type the IP address if Fixed IP is enabled.
Subnet Mask	Type the subnet mask.
Default Gateway	Type the IP address as the default gateway.
Primary DNS	Type in the primary IP address for the router.

Secondary DNS	Type in secondary IP address for necessity in the future.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

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

Please confirm your settings: WAN Interface: WAN1 Physical Mode: ADSL VPI: VCI: 35 Protocol / Encapsulation: 1483 Bridge LLC Fixed IP: No Primary DNS: 8.8.8.8 Secondary DNS: 8.8.4.4 < Back Next > Finish Cancel

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

Quick Start Wizard Setup OK!

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

Quick Start Wizard

I-6-2 For WAN2 (Ethernet)/(Wireless 2.4G)

WAN2 can be configured for physical mode of Ethernet or Wireless 2.4G. If you choose Ethernet WAN2, please specify a physical type. Then, click **Next**.

Available settings are explained as follows:

Item	Description
Display Name	Type a name for the router.
Physical Mode	Choose Ethernet or Wireless based on the physical connection. Choose Wireless 2.4G if you want to use wireless station mode to access Internet. Otherwise, choose Ethernet to access Internet through WAN2 Ethernet Port.
Physical Type	This setting is available when Ethernet is selected as Physical Mode. In general, Auto negotiation is suggested.
VLAN Tag insertion	The settings configured in this field are available when Ethernet is selected as Physical Mode.
	Disable - Disable the function of VLAN with 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 type the tag value and specify the priority for the packets sending by WAN2.
	 Tag value - Type the value as the VLAN ID number. The range is form 0 to 4095.
	 Priority - Type the packet priority number for such VLAN. The range is from 0 to 7.

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

Ethernet WAN2 - PPPoE

Quick Start Wizard

Quick Start Wizard

 Choose WAN2 as the WAN Interface and choose Ethernet as the Physical Mode. Click the Next button. The following page will be open for you to specify Internet Access Type.

WAN 2				
Select one of the follow	ring Internet Access ty	pes provided/	by your ISP.	
	PPPoE			
	O PPTP			
	O L2TP			
	O Static IP			
	ODHCP			

2. Click $\ensuremath{\mathsf{PPPoE}}$ as the Internet Access Type. Then click $\ensuremath{\mathsf{Next}}$ to continue.

PPPoE Client Mode WAN 2 Enter the user name and password provided by your ISP. Service Name (Optional) Username Password Confirm 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.

< Back

Next >

Finish

Cancel

Item	Description
Confirm Password	Retype the password.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

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



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.

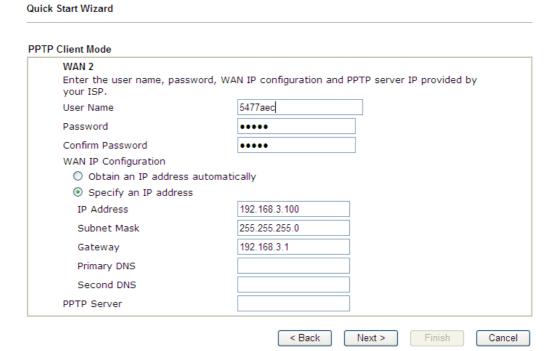
Ethernet WAN2 - PPTP/L2TP

Quick Start Wizard

 Choose WAN2 as the WAN Interface and choose Ethernet as the Physical Mode. Click the Next button. The following page will be open for you to specify Internet Access Type.

WAN 2		
Select one of the following Internet Ac	cess types provided by your ISP.	
O PPPoE		
PPTP		
O L2TP		
O Static IF	P	
O DHCP		

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



Item	Description
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	Retype the password.
WAN IP Configuration	Obtain an IP address automatically - The router will get an IP address automatically from DHCP server.
	Specify an IP address - You have to type relational settings manually.
	IP Address - Type the IP address.
	Subnet Mask - Type the subnet mask.
	Gateway - Type the IP address of the gateway.
	Primary DNS - Type in the primary IP address for the router.
	Second DNS - Type in secondary IP address for necessity in the future.
PPTP Server / L2TP Server	Type the IP address of the server.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

3. 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. < 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!

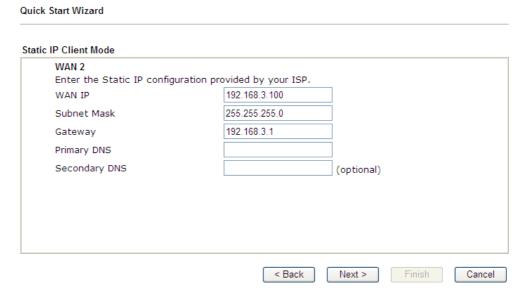
5. Now, you can enjoy surfing on the Internet.

Ethernet WAN2 - Static IP

 Choose WAN2 as the WAN Interface and choose Ethernet as the Physical Mode. Click the Next button. The following page will be open for you to specify Internet Access Type.

uick Start Wizard	
onnect to Internet	
WAN 2	
Select one of the following Internet Acc	cess types provided by your ISP.
O PPPoE	
O PPTP	
O L2TP	
Static IP	
O DHCP	
J 2	
	< Back Next > Finish Cancel

2. Click Static IP as the Internet Access type. Simply click Next to continue.



Item	Description
WAN IP	Type the IP address.
Subnet Mask	Type the subnet mask.
Gateway	Type the IP address of gateway.
Primary DNS	Type in the primary IP address for the router.
Secondary DNS	Type in secondary IP address for necessity in the future.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.

Cancel Click it to give up the quick start wizard.

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



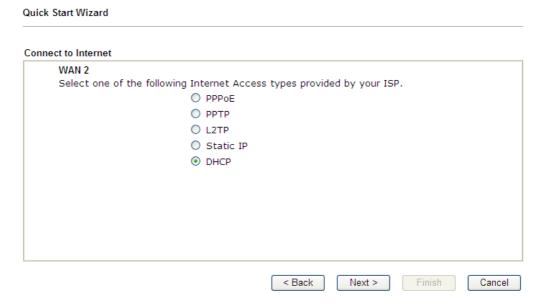
4. Click Finish. A page of Quick Start Wizard Setup OK!!! will appear. Then, the system status of this protocol will be shown.

Quick Start Wizard Setup OK!

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

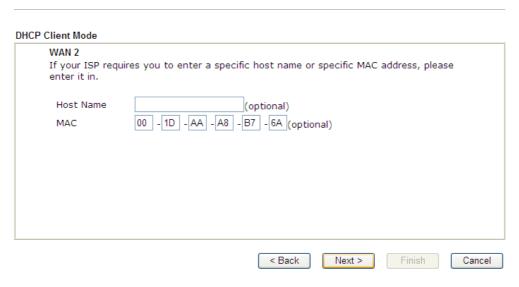
Ethernet WAN2 - DHCP

 Choose WAN2 as the WAN Interface and choose Ethernet as the Physical Mode. Click the Next button. The following page will be open for you to specify Internet Access Type.



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

Quick Start Wizard



Available settings are explained as follows:

Item	Description
Host Name	Type 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. < 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.

Wireless (2.4G) WAN2 - Static IP

Quick Start Wizard

Quick Start Wizard

Choose WAN2 as the WAN Interface and choose Wireless (2.4G) as the Physical Mode.
 Click the Next button. The following page will be open for you to specify Internet Access
 Type.

Connect to Internet WAN 2 Select one of the following Internet Access types. Static IP DHCP Access types. Access types.

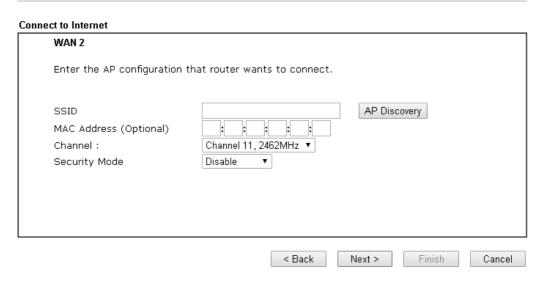
2. Click Static IP as the Internet Access Type. Simply click Next to continue.

Item	Description
WAN IP	Type the IP address.

Subnet Mask	Type the subnet mask.
Gateway	Type the IP address of gateway.
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 according to the settings of your Wireless AP. Then click **Next** for next step.

Quick Start Wizard

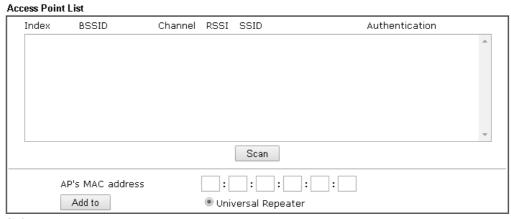


Item	Description
SSID	The identification of the Wireless AP.
MAC Address (Optional)	The MAC Address of the Wireless AP.
Channel	The channel of frequency of the Wireless AP. Please notice that, if this setting is modified, the channel of Wireless LAN (2.4GHz) would be also modified.
Security Mode	The mode to connect to the Wireless AP.
	Disable - The Router connects to the wireless AP without any encryption mechanism.
	WEP - The Router connects to the wireless AP as a WEP client and the encryption key should be entered in WEP Key.
	WPA/PSK - The Router connects to the wireless AP as a WPA client and the encryption key should be entered in PSK.
	 WPA2/PSK - The Router connects to the wireless AP as a WPA2 client and the encryption key should be entered in PSK.
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.

4. Click the AP Discovery button to choose your Wireless AP. You can also set the Wireless AP information directly and skip the next 2 steps.

Wireless LAN >> Access Point Discovery

Wireless LAN >> Access Point Discovery



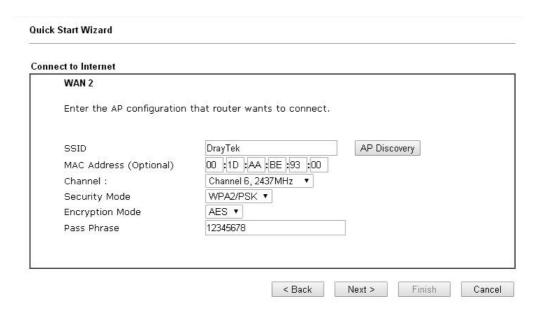
Note:

- 1. During the scanning process (\sim 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.
- 5. Click the **Scan** button of the popup window and wait for a few seconds.

Access Point List Channel RSSI Index **BSSID** SSID Authentication Mixed(WPA+WPAZ)/PSK _ 00:50:7F:19:38:80 DrayTek-LAN-A 11 47% 8 02:50:7F:22:33:88 11 31% AP900_110_Bandstee... WPA2/PSK 9 00:50:7F:22:33:88 11 31% AP900_110_2.4G-1 WPA2/PSK 11 00:50:7F:62:98:E8 31% DrayTek NONE 02:1D:AA:7E:41:7C 7% ap900 AT 2 Mixed(WPA+WPA2)/PSK 00:1D:AA:7E:41:7C 7% 13 3 ap900_AT_1 WPA2/PSK AP810_111_2.4G-2 02:1D:AA:7C:84:38 Mixed(WPA+WPA2)/PSK 14 1 52% AP810_111_2.4G-1 Mixed(WPA+WPA2)/PSK 15 00:1D:AA:7E:84:38 63% Scan AP's MAC address 00 : 1D : AA : BE : 93 : 00 Add to Universal Repeater

Note:

- 1. During the scanning process (\sim 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.
- 6. Select your Wireless AP and click the **Add to** button.



7. All settings except the encryption key will be filled automatically. If the Security Mode is WEP, type in the WEP Keys. If the Security Mode is WPA/PSK or WPA2/PSK, type in the Pass Phrase. Then click Next for next step.



8. 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!

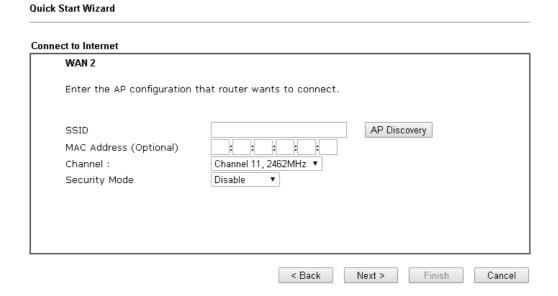
9. Now, you can enjoy surfing on the Internet.

Wireless (2.4G) WAN2 - DHCP

1. Choose WAN2 as the WAN Interface and choose Wireless (2.4G) as the Physical Mode. Click the Next button. The following page will be open for you to specify Internet Access Type.



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

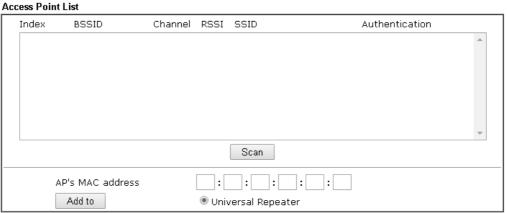


Item	Description
SSID	The identification of the Wireless AP.
MAC Address (Optional)	The MAC Address of the Wireless AP.
Channel	The channel of frequency of the Wireless AP. Please notice that, if this setting is modified, the channel of Wireless LAN (2.4GHz) would be also modified.
Security Mode	The mode to connect to the Wireless AP.
	Disable - The Router connects to the wireless AP

	 without any encryption mechanism. WEP - The Router connects to the wireless AP as a WEP client and the encryption key should be entered in WEP Key. WPA/PSK - The Router connects to the wireless AP as a WPA client and the encryption key should be entered in PSK. WPA2/PSK - The Router connects to the wireless AP as a WPA2 client and the encryption key should be entered in PSK.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
-	0 01 0
Cancel	Click it to give up the quick start wizard.

3. Click the AP Discovery button to choose your Wireless AP. You can also set the Wireless AP information directly and skip the next 2 steps.

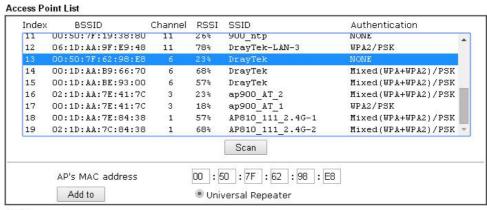
Wireless LAN >> Access Point Discovery



Note:

- 1. During the scanning process (\sim 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.
- 4. Click the **Scan** button of the popup window and wait for a few seconds.

Wireless LAN >> Access Point Discovery



Note:

- 1. During the scanning process (\sim 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.

5. Select your Wireless AP and click the **Add to** button.

Quick Start Wizard

Quick Start Wizard

Connect to Internet WAN 2 Enter the AP configuration that router wants to connect. AP Discovery SSID DrayTek 00 :50 :7F :62 :98 :E8 MAC Address (Optional) Channel 6, 2437MHz ▼ Channel: Security Mode Disable < Back Finish Cancel Next >

6. All settings except the encryption key will be filled automatically. If the Security Mode is WEP, type in the WEP Keys. If the Security Mode is WPA/PSK or WPA2/PSK, type in the Pass Phrase. Then click Next for next step.

Please confirm your settings: WAN Interface: WAN2 Physical Mode: Wireless Internet Access: DHCP Click Back to modify changes if necessary. Otherwise, click Finish to save the current settings and restart the Vigor router.

7. 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.

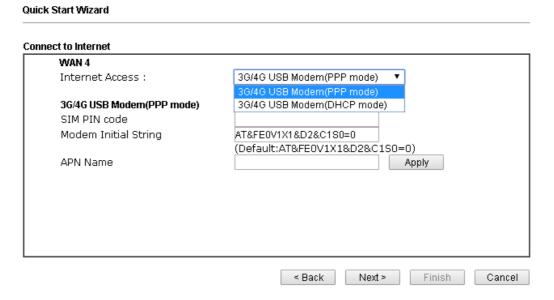
I-6-3 For WAN3/WAN4 (USB)

Quick Start Wizard

WAN3/WAN4 is dedicated to physical mode in USB.

1. Choose WAN3/WAN4 as WAN Interface.

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



Item	Description
Internet Access	Choose one of the selections as the protocol of accessing the internet.
3G/4G USB Modem (PPP mode)	SIM Pin code -Type PIN code of the SIM card that will be used to access Internet. The maximum length of the pin code you can set is 15 characters.
	Modem Initial String - Such value is used to initialize USB modem. Please use the default value. If you have any 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. Type the name and click Apply.
3G/4G USB Modem (DHCP mode)	SIM Pin code - Type PIN code of the SIM card that will be used to access Internet.
	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.

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

Quick Start Wizard

Please confirm your settings: WAN Interface: WAN4 Physical Mode: USB Physical Type: Auto negotiation Internet Access: PPP 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.

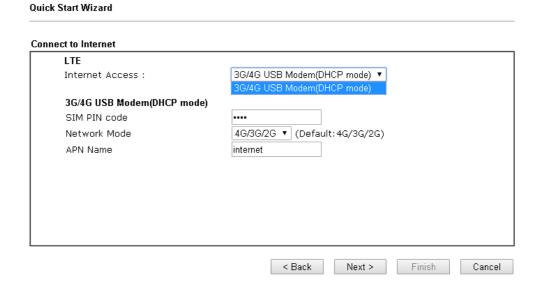
I-6-4 For LTE WAN

Quick Start Wizard

1. Choose LTE as WAN Interface.

WAN Interface: Display Name: Physical Mode: USB

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



Item	Description
Internet Access	Now, DHCP mode is the only choice for LTE WAN.
3G/4G USB Modem (DHCP mode)	SIM Pin code - Type PIN code of the SIM card that will be used to access Internet.
	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.

3. Please type in required information originally provided by your ISP. Then, click **Next** for viewing summary of such connection.



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.



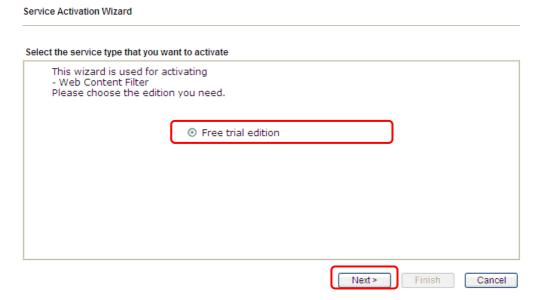
Info

Such function is available only for Admin Mode.

1. Open Wizards>>Service Activation Wizard.

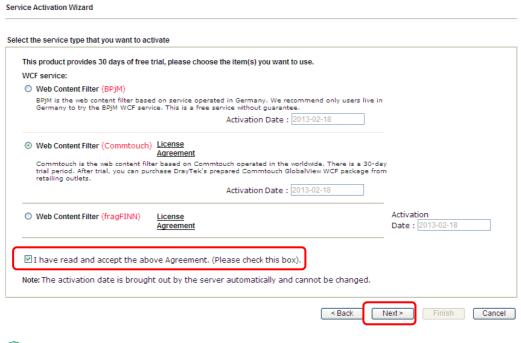


2. The screen of **Service Activation Wizard** will be shown as follows. Click **Next** to activate free trail edition.



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

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





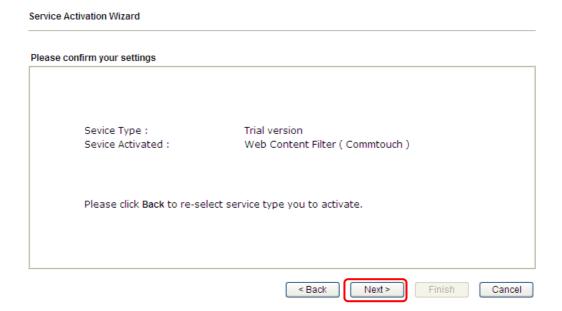
Info

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

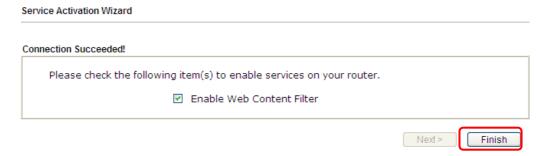
BPjM is WCF for German Speaking users. The fragfINN is whitelist for German Speaking users. The BPjM is ideal for your family to provide more Internet security for youngsters.

Web Content Filter (fragFINN) service will not be supported since January 1, 2015.

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



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



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



Info

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

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

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



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.

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



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



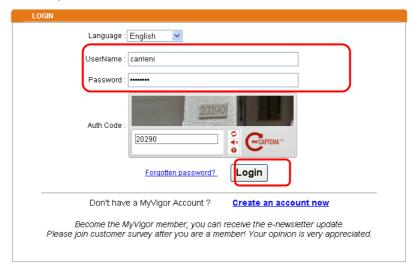
3 A Login page will be shown on the screen. Please type the account and password that you created previously. And click Login.



Please take a moment to register.

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

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





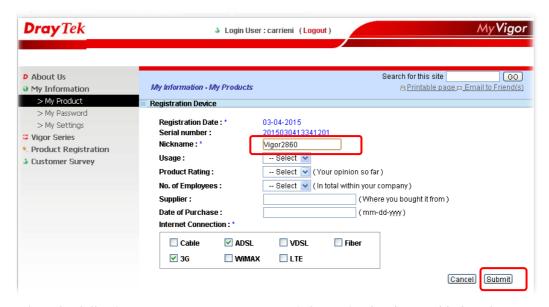
Info

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. From this page, please click Add or Product Registration.



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



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

Your device has been successfully added to the database.



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



Part II Connectivity



WAN



LAN



NAT



Applications



Routing

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

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.

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.

DNS, LAN DNS, IGMP, LDAP, UpnP, IGMP, WOL, RADIUS, SMS, Bonjour

Static Route, Load-Balance/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.

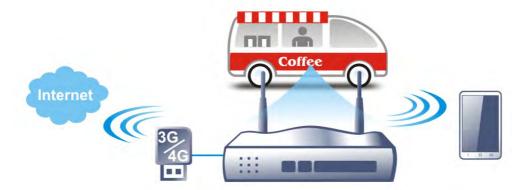
Get Your Public IP Address from ISP

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

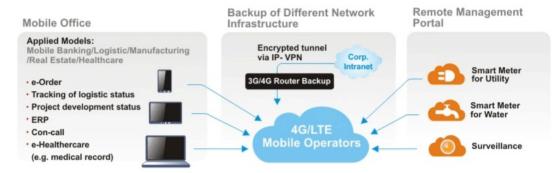
For 3G/4G mobile communication through Access Point is popular more and more, Vigor2860 adds the function of 3G/4G network connection for such purpose. By connecting 3G/4G USB Modem to the USB port of Vigor2860, it can support LTE/HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G/4G standard (HSUPA, etc). Vigor2860n 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 Vigor2860n 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.

LTE Application

Service Network



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/WAN4 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, WAN3 and WAN4 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**.

For Vigor2860 Series except Vigor2860L and Vigor2860Ln

WAN >> General Setup

Load Bala	nce Mode:	Auto Weight		
Setup				
Index	Enable	Physical Mode/Type	Line Speed(Kbps) DownLink/UpLink	Active Mode
WAN1	٧	ADSL/-	0/0	Always On
WAN2	٧	Ethernet/Auto negotiation	0/0	Always On
WAN3	V	USB/-	0/0	Always On
WAN4	٧	USB/-	0/0	Always On

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

OK

For Vigor2860L and Vigor2860Ln

WAN >> General Setup



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



	B
Item	Description

Load Balance Mode	This option is available for multiple-WAN for getting enough bandwidth for each WAN port. If you know the practical bandwidth for your WAN interface, please choose the setting of According to Line Speed. Otherwise, please choose Auto Weight to let the router reach the best load balance.	
	Load Balance Mode: Auto Weight Auto Weight According to Line Speed	
Index	Click the WAN interface link under Index to access into the WAN configuration page.	
Enable	V means such WAN interface is enabled and ready to be used.	
Physical Mode / Type	Display the physical mode and physical type of such WAN interface.	
Line Speed(Kbps) DownLink/UpLink	Display the downstream and upstream rate of such WAN interface.	
Active Mode	Display whether such WAN interface is Active device or backup device. Backup (WAN#) - Display the backup WAN interface for such WAN when it is disabled.	



Info

In default, each WAN port is enabled.

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

II-1-1-1 WAN1(ADSL/VDSL2)

Vigor router will detect the physical line is connected by ADSL or VDSL2 automatically. Therefore, this page allows you to configure settings for ADSL and VDSL2 at one time. That is, it is not necessary for you to configure different profile settings for ADSL and VDSL2 respectively.

WAN 1

Enable:	Yes 💌
Display Name:	
Physical Mode:	VDSL2
DSL Mode:	VDSL2 only 🕶
Physical Type:	Auto negotiation 💟
DSL Modem Code:	Default <u>~</u>
Line Speed(Kbps):	
DownLink	0
UpLink	0
VLAN Tag insertion (ADSL):	Disable 🕶
Tag value:	0 (0~4095)
Priority:	0 (0~7)
VLAN Tag insertion (VDSL2):	Disable 🕶
Tag value:	0 (0~4095)
Priority:	0 (0~7)
Active Mode:	Always On 🔻 Load Balance: 🗹

Note:

- 1. The line speed setting of WAN interface is available only when According to Line Speed is selected as the Load Balance Mode.
- 2. In DSL auto mode, the router will reboot automatically while switching between VDSL2 and ADSL lines.



Item	Description	
Enable	Choose Yes to invoke the settings for this WAN interface. Choose No to disable the settings for this WAN interface.	
Display Name	Type the description for such interface.	
Physical Mode	Display the physical mode of such interface. If VDSL2 is detected, this field will display "VDSL2"; if ADSL is detected, it will display "ADSL".	
DSL Mode	Specify the physical mode (VDSL or ADSL) for such router manually.	
Physical Type	For such interface, no type can be selected.	
DSL Modem Code	Choose the correct DSL modem code for ensuring the network connection. Default Default AnnexA_560816_552011 AnnexA_548006_544401 If you have no idea about the selection, simply choose Default or contact the dealer for assistance.	
Line Speed (Kpbs)	If your choose According to Line Speed as the Load Balance Mode in previous page, please type the line speed for downloading and uploading for such WAN interface. The unit is kbps.	

VLAN Tag insertion (ADSL)	The settings configured in this field are available for ADSL. Enable - Enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the WAN while sending them out. Please type the tag value and specify the priority for the packets sending by WAN1. Disable - Disable the function of VLAN with tag. Tag value - Type the value as the VLAN ID number. The range is form 0 to 4095. Priority - Type the packet priority number for such VLAN. The range is from 0 to 7.
VLAN Tag insertion (VDSL2)	The settings configured in this field are available for VDSL2. Enable - Enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the WAN while sending them out. Please type the tag value and specify the priority for the packets sending by WAN1. Disable - Disable the function of VLAN with tag. Tag value - Type the value as the VLAN ID number. The range is form 0 to 4095. Priority - Type the packet priority number for such VLAN. The range is from 0 to 7.
Active Mode	Choose Always On to make the WAN1 connection being activated always. Failover Always On Failover Load Balance: Check this box to enable auto load balance function for such WAN interface. When the data traffic is large, the WAN interface with the function enabled will balance the data transmission automatically among all of the WAN interfaces in connection status.
Active When	If you choose Failover as the Active Mode, Active When will appear. Please specify which WAN will be the Backup interface. Active Mode: Active When: Active When: Active When: Any of the selected WAN disconnect WAN 1 WAN 2 WAN 3 WAN 4 Any of the selected WAN disconnect - Such backup WAN will be activated when any master WAN interface disconnects. All of the selected WAN disconnect - Such backup WAN will be activated only when all master WAN interfaces disconnect.

After finished the above settings, click $\ensuremath{\mathsf{OK}}$ to save the settings.

II-1-1-2 WAN2 (Ethernet)/(Wireless 2.4G)

WAN2 can be configured for physical mode of Ethernet or Wireless 2.4G.

WAN >> General Setup

WAN 2 Enable: Yes 💌 Display Name: Physical Mode: Ethernet Physical Type: Auto negotiation Line Speed(Kbps): DownLink UpLink Disable 🔽 (Please configure Internet Access setting first) VLAN Tag insertion: $(0 \sim 4095)$ Tag value: Priority: (0~7) Active Mode: Failover 🔽 🛮 Load Balance: 🗹 Active When: Any of the selected WAN disconnect O All of the selected WAN disconnect ■WAN 1 ■ WAN 2 ■ WAN 3 ■ WAN 4 Note:

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



Or,

WAN >> General Setup

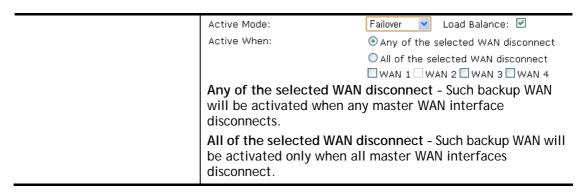
WAN 2 Enable: Yes ▼ Display Name: Physical Mode: Wireless ▼ Line Speed(kbps) DownLink UpLink Active Mode: Failover 🔻 Load Balance: 🗹 Active When: Any of the selected WAN disconnect All of the selected WAN disconnect WAN 1 WAN 2 LTE WAN 4

Note:

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



Item	Description	
Enable	Choose Yes to invoke the settings for this WAN interface. Choose No to disable the settings for this WAN interface.	
Display Name	Type the description for such WAN interface.	
Physical Mode	Choose Wireless 2.4G if you want to use wireless station mode to access Internet. Otherwise, choose Ethernet to access Internet through WAN2 Ethernet Port.	
Physical Type	You can change the physical type or choose Auto negotiation for determined by the system. Auto negotiation Auto negotiation 10M half duplex 100M full duplex 100M full duplex 100M full duplex 1000M full duplex 1000M full duplex	
Line Speed	If your choose According to Line Speed as the Load Balance Mode, please type the line speed for downloading and uploading for such WAN interface. The unit is kbps.	
VLAN Tag insertion	It is available only when Ethernet is selected as Physical Mode. Enable - Enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the WAN while sending them out. Please type the tag value and specify the priority for the packets sending by WAN1. Disable - Disable the function of VLAN with tag. Tag value - Type the value as the VLAN ID number. The range is form 0 to 4095. Priority - Type the packet priority number for such VLAN. The range is from 0 to 7.	
Active Mode	Choose Always On to make the WAN2 connection being activated always. Failover Always On Failover Load Balance: Check this box to enable auto load balance function for such WAN interface. When the data traffic is large, the WAN interface with the function enabled will balance the data transmission automatically among all of the WAN interfaces in connection status.	
Active When	If you choose Failover as the Active Mode, Active When will appear. Please specify which WAN will be the Backup interface.	

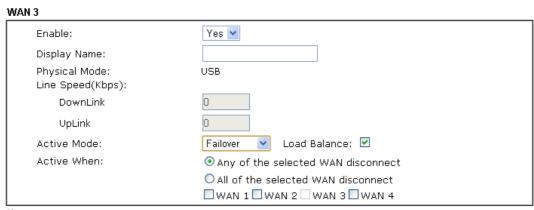


After finished the above settings, click **OK** to save the settings.

II-1-1-3 WAN3/WAN4 (USB)

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

WAN >> General Setup



Note:

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



Item	Description
Enable	Choose Yes to invoke the settings for this WAN interface. Choose No to disable the settings for this WAN interface.
Display Name	Type the description for such WAN interface.
Physical Mode	Display the physical mode of such WAN interface.
Line Speed	If your choose According to Line Speed as the Load Balance Mode, please type the line speed for downloading and uploading for such WAN interface. The unit is kbps.
Active Mode	Choose Always On to make the WAN1 connection being activated always. Failover Always On Failover Load Balance: Check this box to enable auto load balance function for such WAN interface.

	function enabled will bala	arge, the WAN interface with the ance the data transmission of the WAN interfaces in connection
Active When	If you choose Failover as the Active Mode, Active When will appear. Please specify which WAN will be the Backup interface.	
	Active Mode:	Failover 💌 Load Balance: 🗹
	Active When:	Any of the selected WAN disconnect
		○ All of the selected WAN disconnect □ WAN 1 □ WAN 2 □ WAN 3 □ WAN 4
	Any of the selected WAN disconnect - Such backup WAN will be activated when any master WAN interface disconnects.	
	All of the selected WAN of be activated only when all disconnect.	disconnect - Such backup WAN will I master WAN interfaces

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 or LTE/WAN4) for Internet Access. Due to different Physical Mode for WAN interface, the Access Mode for these connections also varies. Refer to the following figures for examples.

Access Mode for ADSL/VDSL2,

WAN >> Internet Access

Internet Access Index Display Name **Physical Mode** Access Mode WAN1 ADSL / VDSL2 PPPoE / PPPoA Details Page IPv6 None WAN2 Ethernet Details Page IPv6 PPPoE / PPPoA MPoA / Static or Dynamic IP WAN3 USB Details Page IPv6 None WAN4 None Details Page USB IPv6

Note: 1. Device on USB port 1 applies WAN3 configuration.
Device on USB port 2 applies WAN4 configuration.

Advanced You can configure DHCP client options here.

Access Mode for LTE (for L model only),

WAN >> Internet Access

Internet Access Index Display Name **Physical Mode Access Mode** WAN1 ADSL / VDSL2 PPPoE / PPPoA Details Page IPv6 WAN2 Ethernet PPP0E Details Page IPv6 LTE USB 3G/4G LTE Modem(DHCP mode) ▼ Details Page IPv6 WAN4 Details Page USB None IPv6

Note: 1. Device on USB port 1 applies WAN3 configuration.
Device on USB port 2 applies WAN4 configuration.

Advanced You can configure DHCP client options here.

Access Mode for Etherenet / USB,



Access Mode for Wireless 2.4G,

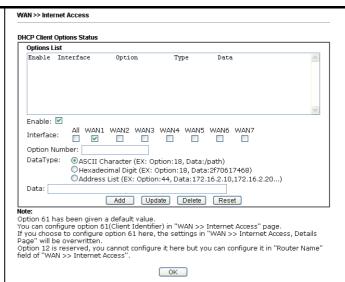
WAN >> Internet Access

Internet Access Index Display Name Physical Mode **Access Mode** WAN1 ADSL / VDSL2 MPoA / Static or Dynamic IP Details Page IPv6 WAN2 Static or Dynamic IP Wireless Details Page IPv6 None LTE USB Details Page IPv6 WAN4 USB None Details Page IPv6

Note: 1. Device on USB port 1 applies WAN3 configuration.
Device on USB port 2 applies WAN4 configuration.

Advanced You can configure DHCP client options here.

Item	Description
Index	Display the WAN interface.
Display Name	It shows the name of the WAN1/WAN2/WAN3/WAN4 that entered in general setup.
Physical Mode	It shows the physical connection for WAN1(ADSL/VDSL2)/WAN2 (Ethernet/Wireless 2.4G)/WAN3 or LTE/WAN4 (3G/4G USB Modem) accroding 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. Note that Details Page will be changed slightly based on ADSL/VDSL2 physical mode specified on WAN>>General Setup.
IPv6	This button will open different web page (based on Physical Mode) to setup IPv6 Internet Access Mode for WAN interface.
Advanced	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.



Enable/Disable - Enable/Disable the function of DHCP Option. Each DHCP option is composed by an option number with data. For example,

Option number: 100

Data: abcd

When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets.

Interface - Specify the WAN interface(s) that will be overwritten by such function. WAN5 ~ WAN7 can be located under WAN>>Multi-PVC/VLAN.

Option Number - Type a number for such function.

DataType - Choose the type (ASCII or Hex) for the data to be stored.

Data - Type the content of the data to be processed by the function of DHCP option.



Info

WAN >> Internet Access

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

II-1-2-1 Details Page for PPPoE in WAN1 (Physical Mode: VDSL2)

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 1 MPoA / Static or Dynamic IP IPv6 PPPoE / PPPoA ISP Access Setup O Disable Enable Service Name¹ Modern Settings (for ADSL only) Username Multi-PVC channel Channel 1 Password VPI Separate Account for ADSL VCI 33 PPP Authentication PAP or CHAP **Encapsulating Type** LLC/SNAP V IP Address From ISP WAN IP Alias Protocol PPPoE 🕶 Fixed IP O Yes O No (Dynamic IP) Modulation Multimode Fixed IP Address PPPoE Pass-through Default MAC Address For Wired LAN2 Specify a MAC Address For Wireless LAN MAC Address: 00 1D AA BC 4D C1 WAN Connection Detection Index(1-15) in Schedule Setup: Mode ARP Detect 💌 MTU (Max:1500) 1492 Path MTU Discovery Detect

Item	Description
	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.
	It is not necessary to configure settings in these fields for modem settings are prepared for ADSL only.
Ğ	The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction. For Wired LAN - If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet. For Wireless LAN - It is available for <i>n</i> 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

	N. I. T. I. DDD A.D
	Note: To have PPPoA Pass-through, please choose PPPoA protocol and check the box(es) here. The router will behave like a modem which only serves the PPPoE client on the LAN. That's, the router will offer PPPoA dial-up connection.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.
	 Mode - Choose ARP Detect or Ping Detect for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items. Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. TTL (Time to Live) - Set TTL value of PING operation. Ping Interval - Type the interval for the system to
	execute the PING operation.
	 Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
MTU	It means Max Transmit Unit for packet. 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.
	192.168.1.1/doc/pathuntu.htm
	Path MTU to: IPv4 Host MTU reduce size by 8
	Detect Note: You may reduce the Path MTU Size(max 1500) by 1 to 100. Accept Cancel
	Note: You may reduce the Path MTU Size(max 1500) by 1 to 100.
	Note: You may reduce the Path MTU Size(max 1500) by 1 to 100. Accept Cancel Path MTU to - Type the IP address as the specific
	Path MTU to - Type the IP address as the specific transmit path. 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,
	 Note: You may reduce the Path MTU Size(max 1500) by 1 to 100. Accept Cancel Path MTU to - Type the IP address as the specific transmit path. 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.
ISP Access Setup	Path MTU to - Type the IP address as the specific transmit path. 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. Enter your allocated username, password and authentication parameters according to the information provided by your ISP.
ISP Access Setup	Path MTU to - Type the IP address as the specific transmit path. 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. Enter your allocated username, password and authentication parameters according to the information provided by your

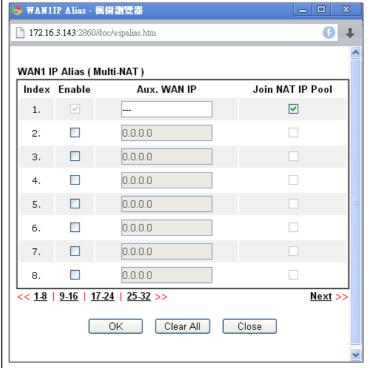
Separate Account for ADSL - In default, WAN1 supports VDSL2/ADSL and uses the same PPPoE account and password for connection. If required, you can configure another account and password for ADSL connection by checking this box. If it is checked, the system will ask you to type another group of account and password additionally.

PPP Authentication - Select PAP only or PAP or CHAP for PPP.

IP Address From ISP

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

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



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

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

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

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.

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

II-1-2-2 Details Page for MPoA/Static or Dynamic IP in WAN1 (Physical Mode: VDSL2)

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

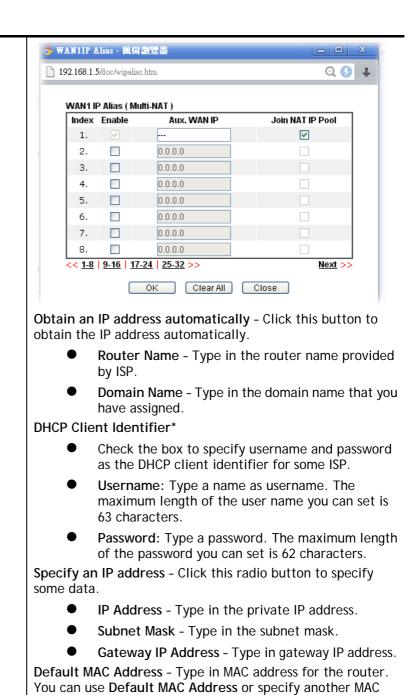
WAN 1 PPPoE / PPPoA MPoA / Static or Dynamic IP Enable Disable WAN IP Network Settings WAN IP Alias Obtain an IP address automatically Modern Settings (for ADSL only) Router Name drayrouter Multi-PVC channel Channel 2 Domain Name Encapsulation DHCP Client Identifier * 1483 Bridged IP LLC Username VPI Password VCI 88 Specify an IP address Modulation Multimode IP Address WAN Connection Detection Subnet Mask Mode ARP Detect 💌 Gateway IP Address MTU (Max:1500) 1492 Default MAC Address Specify a MAC Address Detect Path MTU Discovery MAC Address: 00 1D AA BC 4D C1 RIP Protocol DNS Server IP Address Enable RIP Primary IP Address 8.8.8.8 Bridge Mode Secondary IP Address 8.8.4.4 Enable Bridge Mode Bridge Subnet LAN 1 💙

WAN >> Internet Access

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.
Modem Setting (for ADSL only)	It is not necessary to configure settings in these fields for modem settings are prepared for ADSL only.
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 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.
	 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

^{*:} Required for some ISPs

mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. TTL (Time to Live) - Set TTL value of PING operation. • Ping Interval - Type the interval for the system to execute the PING operation. Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged. MTU It means Max Transmit Unit for packet. Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit Click Detect to open the following dialog. 🗎 192.168.1.1/doc/pathmtu.htm Path MTU to: | IPv4 Host 💌 MTU reduce size by Detect Note: You may reduce the Path MTU Size(max 1500) by 1 to 100. Accept Cancel Path MTU to - Type the IP address as the specific transmit path. 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 Protocol** Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function. **Bridge Mode** 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. **WAN IP Network Settings** This group allows you to obtain an IP address automatically and allows you type in IP address manually. WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 32 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.



router manually.

Specify a MAC Address - Type in the MAC address for the

Type in the primary IP address for the router. If necessary, type in secondary IP address for necessity in the future.

address for your necessity.

<u>'</u>

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

DNS Server IP Address

II-1-2-3 Details Page for PPPoE/PPPoA in WAN1 (Physical Mode: ADSL)

WAN >> Internet Access

PPPoE / PPPoA	MPoA / Static or	Dynamic IP	IPv6
EnableDis	sable	ISP Access Setup	
Modem Settings (for ADS	L only)	Service Name ¹	
Multi-PVC channel	Channel 1	Username	
VPI	0	Password	
VCI	33	Separate Accoun	t for ADSL
	LLC/SNAP V	PPP Authentication	PAP or CHAP
Encapsulating Type		IP Address From ISP	WAN IP Alias
Protocol	PPP₀E ▼	Fixed IP Yes	No (Dynamic IP)
Modulation	Multimode	Fixed IP Address	
PPPoE Pass-through			
For Wired LAN ²		Default MAC Add	dress
For Wireless LAN		Specify a MAC A	Address
WAN Connection Detecti	On .	MAC Address: 00	·1D ·AA BC ·4D ·C1
Mode	ARP Detect	Index(1-15) in Sche	edule Setup:
		=> ,	, ,
MTU	1492 (Max: 1500)		
Path MTU Discovery	Detect		

Notes

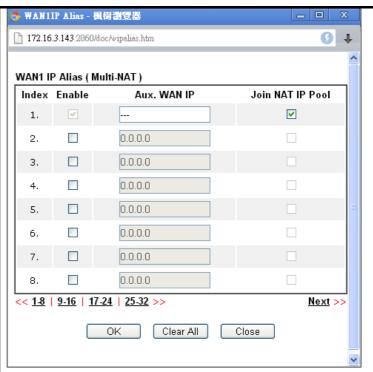
- 1: (Optional) Required for some ISPs. Leave blank if in doubt because the connection request might be denied if "Service Name" is incorrect.
- 2: If this box is checked while using the PPPoA protocol, the router will behave like a modem which only serves the PPPoE client on the LAN.



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.
Modem Settings (for ADSL only)	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 Internet Access >> Multi PVCs. 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	g is Multimode. Choose the one
	that fits the requirement of	
	Modulation	Multimode T1.413 G.Lite G.DMT ADSL2(G.992.3) ADSL2 annex M ADSL2+(G.992.5) ADSL2+ annex M Multimode
PPPoE Pass-through	also can establish the PPPo clients to your ISP via the V is selected, the PPPoE pack transformed into PPPoA pac Thus, the PC can access Int For Wired LAN - If you che	al-up connection. Besides, you E connection directly from local ligor router. When PPPoA protocol tage transmitted by PC will be ckage and sent to WAN server. Therefore through such direction. It is box, PCs on the same of PPPoE session (different with Internet.
	this box, PCs on the same v	ailable for <i>n</i> model. If you check vireless network can use another ent with the Host PC) to access
	protocol and check the box like a modem which only se	through, please choose PPPoA (es) here. The router will behave erves the PPPoE client on the LAN. r PPPoA dial-up connection.
WAN Connection Detection	Such function allows you to connection is alive or not the	verify whether network nrough ARP Detect or Ping Detect.
	Mode - Choose ARP Detect execute for WAN detection detection mode, you have following items. Primary/Secondary Ping detection mode, you have address in this field for Ping Gateway IP - If you mode, you also can enable gateway IP address for p With the IP address for p With the IP address(es) the WAN connection is continuous TTL (Time to Live) - See Ping Interval - Type the execute the PING operation.	or Ping Detect for the system to . If you choose Ping Detect as the to type required settings for the g IP - If you choose Ping Detect as we to type Primary or Secondary IP pinging. u choose Ping Detect as detection ble this setting to use current WAN binging. pinging, Vigor router can check if on or off. t TTL value of PING operation. interval for the system to tion. umber of times that the system is PING operation before WAN
MTU	It means Max Transmit Unit	for packet.
		used to detect the maximum MTU egmented in specific transmit

	192.168.1.1/doc/pathmtu.htm	
	Path MTU to: IPv4 Host MTU reduce size by Detect Note: You may reduce the Path MTU Size(max 1500) by 1 to 100. Accept Cancel	
	 Path MTU to - Type the IP address as the specific transmit path. 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. 	
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP. Username - Type in the username provided by ISP in this field. Password - Type in the password provided by ISP in this field. 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. PPP Authentication - Select PAP only or PAP or CHAP for PPP. Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action.	
IP Address From ISP	Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.	



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

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

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

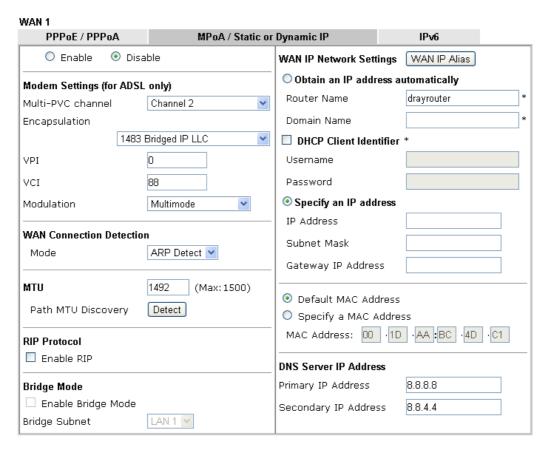
Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Applications >> Schedule web page and you can use the number that you have set in that web page.

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

II-1-2-4 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.



^{*:} Required for some ISPs

Note: 1. If enable firewall in bridge mode, IPv6 connection type would be change to DHCPv6 mode.

- 2. Bridge Subnet cannot be selected by Multi-WAN Interface at the same time.
- If both Bridge Mode and Firewall are enabled, the settings under User Management will be ignored.



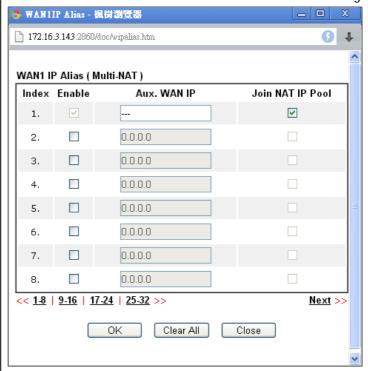
Item	Description
Enable/Disable	Click Enable for activating this function. If you click Disable, this function will be closed and all the settings that you adjusted in this page will be invalid.
Modem Settings (for ADSL only)	Set up the DSL parameters required by your ISP. These settings configured here are specified for ADSL only.
-	Multi-PVC channel - The selections displayed here are determined by the page of Internet Access >> Multi PVCs. Select M-PVCs Channel means no selection will be chosen.
	Encapsulating - Drop down the list to choose the type provided by ISP.
	VPI - Type in the value provided by ISP.
	VCI - Type in the value provided by ISP.
	Modulation -Default setting is Multimode. Choose the one that fits the requirement of your router.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.
	Mode - Choose ARP Detect or Ping Detect for the system to

execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items. • Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. • Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. TTL (Time to Live) - Set TTL value of PING operation. Ping Interval - Type the interval for the system to execute the PING operation. • Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged. MTU It means Max Transmit Unit for packet. Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit Click Detect to open the following dialog. 172.17.11.1/doc/pathmtu.htm Path MTU to: IPv4 Host ▼ 8 MTU reduce size by Detect Note: You may reduce the Path MTU Size(max 1500) by 1 to 100. Cancel Accept Path MTU to - Type the IP address as the specific transmit path. 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 Protocol** Routing Information Protocol is abbreviated as RIP(RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function. **Bridge Mode** 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.

WAN IP Network Settings

This group allows you to obtain an IP address automatically and allows you type in IP address manually.

WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 32 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.



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

- 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 -

- Enable: Check the box to specify username and password as the DHCP client identifier for some ISP.
- Username: Type a name as username. The maximum length of the user name you can set is 63 characters.
- Password: Type a password. The maximum length of the password you can set is 62 characters.

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

- IP Address Type in the private IP address.
- Subnet Mask Type in the subnet mask.
- Gateway IP Address Type in gateway IP address.

Default MAC Address - Type in MAC address for the router. You can use **Default MAC Address** or specify another MAC address for your necessity.

Specify a MAC Address - Type in the MAC address for the

	router manually.
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.

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

II-1-2-5 Details Page for PPPoE in WAN2 (Physical Mode: Ethernet)

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

WAN >> Internet Access WAN 2 Static or Dynamic IP PPTP/L2TP IPv6 **PPPoE** PPP/MP Setup O Enable Disable PAP or CHAP 💌 PPP Authentication ISP Access Setup second(s) Idle Timeout Service Name (Optional) IP Address Assignment Method (IPCP) Username WAN IP Alias Password Fixed IP: O Yes O No (Dynamic IP) Index(1-15) in Schedule Setup: Fixed IP Address Default MAC Address WAN Connection Detection Specify a MAC Address Mode ARP Detect 💌 MAC Address: 00 ·1D ·AA :BC ·4D ·C2 MTU 1500 (Max: 1500) Path MTU Discovery Detect

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



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.
	Service Name (Optional) - Enter the description of the specific network service.
	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.
	Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set

	previously in Application >> Schedule web page and you can use the number that you have set in that web page.	
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode - Choose ARP Detect or Ping Detect for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items. Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. TTL (Time to Live) - Set TTL value of PING operation. Ping Interval - Type the interval for the system to execute the PING operation. Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.	
MTU	It means Max Transmit Unit for packet. 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.	
	172.17.11.1/doc/pathmtu.htm	
	Path MTU to: IPv4 Host MTU reduce size by B Detect Note: You may reduce the Path MTU Size(max 1500) by 1 to 100. Accept Cancel	
	Path MTU to - Type the IP address as the specific transmit path.	
	 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	PPP Authentication - Select PAP only or PAP or CHAP for PPP. Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action	
IP Address Assignment Method (IPCP)	Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address	

whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function.

WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 32 public IP addresses other than the current one you are using. Type the additional WAN IP address and check the Enable box. Then click **OK** to exit the dialog.

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

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

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

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

II-1-2-6 Details Page for Static or Dynamic IP in WAN2 (Physical Mode: Ethernet)

For static IP mode, you usually receive a fixed public IP address or a public subnet, namely multiple public IP addresses from your DSL or Cable ISP service providers. In most cases, a Cable service provider will offer a fixed public IP, while a DSL service provider will offer a public subnet. If you have a public subnet, you could assign an IP address or many IP address to the WAN interface.

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

WAN 2 PPTP/L2TP **PPPoE** Static or Dynamic IP IPv6 O Enable Disable WAN IP Network Settings WAN IP Alias Obtain an IP address automatically **Keep WAN Connection** Router Name Enable PING to keep alive Domain Name PING to the IP ■ DHCP Client Identifier * PING Interval minute(s) Username **WAN Connection Detection** Password ARP Detect Mode Specify an IP address IP Address MTU 1500 (Max: 1500) Subnet Mask Path MTU Discovery Detect Gateway IP Address RIP Protocol ■ Enable RIP Default MAC Address Specify a MAC Address Bridge Mode MAC Address: 00 ·1D ·AA :BC ·4D ·C2 ☐ Enable Bridge Mode Bridge Subnet LAN 1 V **DNS Server IP Address** Primary IP Address 8.8.8.8 Secondary IP Address 8.8.4.4

Note: 1. If enable firewall in bridge mode, IPv6 connection type would be change to DHCPv6 mode.

- 2. Bridge Subnet cannot be selected by Multi-WAN Interface at the same time.
- 3. If both Bridge Mode and Firewall are enabled, the settings under User Management will be ignored.



Item	Description
Enable / Disable	Click Enable for activating this function. If you click Disable, this function will be closed and all the settings that you adjusted in this page will be invalid.
Keep WAN Connection	Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time. Check Enable PING to keep alive box to activate this function. PING to the IP - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive. PING Interval - Enter the interval for the system to execute the PING operation.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode - Choose ARP Detect, 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. Primary/Secondary Ping IP - If you choose Ping Detect as

^{*:} Required for some ISPs

	 detection mode, you have to type Primary or Secondary IP address in this field for pinging. Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. TTL (Time to Live) - Set TTL value of PING operation. Ping Interval - Type the interval for the system to execute the PING operation. Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged. 	
MTU	It means Max Transmit Unit for packet. 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.	
	Path MTU to: IPv4 Host MTU reduce size by Detect Note: You may reduce the Path MTU Size(max 1500) by 1 to 100. Accept Cancel	
	 Path MTU to - Type the IP address as the specific transmit path. 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 Protocol	Routing Information Protocol is abbreviated as RIP(RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.	
Bridge Mode	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.	
WAN IP Network Settings	This group allows you to obtain an IP address automatically and allows you type in IP address manually. WAN IP Alias - If you have multiple public IP addresses and	

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

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

- Router Name: Type in the router name provided by ISP.
- Domain Name: Type in the domain name that you have assigned.

DHCP Client Identifier for some ISP

- Enable: Check the box to specify username and password as the DHCP client identifier for some ISP.
- Username: Type a name as username. The maximum length of the user name you can set is 63 characters.
- Password: Type a password. The maximum length of the password you can set is 62 characters.

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

- IP Address: Type the IP address.
- Subnet Mask: Type the subnet mask.
- Gateway IP Address: Type the gateway IP address.

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

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

DNS Server IP Address

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

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

II-1-2-7 Details Page for PPTP/L2TP in WAN2 (Physical Mode: Ethernet)

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 2 **PPPoE** Static or Dynamic IP PPTP/L2TP IPv6 PPP Setup ○ Enable PPTP ○ Enable L2TP ⊙ Disable PAP or CHAP PPP Authentication Server Address Specify Gateway IP Address Idle Timeout second(s) IP Address Assignment Method (IPCP) WAN IP Alias **ISP Access Setup** O Yes No (Dynamic IP) Fixed IP: Username Fixed IP Address WAN IP Network Settings Password Obtain an IP address automatically Index(1-15) in Schedule Setup: Specify an IP address IP Address MTU 1460 (Max: 1460) Subnet Mask Path MTU Discovery Detect ΟK Cancel

Available settings are explained as follows:

WAN >> Internet Access

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.		
	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.		
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.			
	172.17.11.1/doc/pathmtu.htm			
	Path MTU to: IPv4 Host ▼ MTU reduce size by Detect Note: You may reduce the Bath MTU Size(may 1500) by 1 to 100			
	Note: You may reduce the Path MTU Size(max 1500) by 1 to 100.			
	Accept Cancel			
	Path MTU to - Type the IP address as the specific transmit path.			
	 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	PPP Authentication - Select PAP only or PAP or CHAP for PPP.			
	Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action.			
IP Address Assignment Method(IPCP)	WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 32 public IP addresses other than the current one you are using.			
	Fixed IP - Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Click Yes to use this function and type in a fixed IP address in the box. Fixed IP Address -Type a fixed IP address.			
WAN IP Network Settings	Obtain an IP address automatically - Click this button to			
	obtain the IP address automatically. Specify an IP address - Click this radio button to specify some data.			
	IP Address - Type the IP address.			
	Subnet Mask - Type the subnet mask.			

After finishing all the settings here, please click $\ensuremath{\mathsf{OK}}$ to activate them.

II-1-2-8 Details Page for Static or Dynamic IP in WAN2 (Physical Mode: Wireless 2.4G)

When Wireless 2.4G is selected as Physical Mode, WAN2 uses wireless station mode to access Internet. The Router acts as a 2.4GHz wireless station and connects to the specific Wireless AP

To use Static or Dynamic IP as the accessing protocol of the internet, please select Static or Dynamic IP from the WAN>>Internet Access>>WAN2 page. The following web page will be shown.

WAN 2	
Static or Dynamic IP	
Enable Disable	
Obtain an IP address automatically	
Specify an IP address	
IP Address	192.168.3.100
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.3.1
WAN Connection Detection	
Mode	ARP Detect ▼
мти	1500 (Max: 1500)
Universal Repeater Parameters	
SSID	DrayTek AP Discovery
MAC Address (Optional)	00 :50 :7F :62 :98 :E8
Channel:	Channel 6, 2437MHz ▼
Security Mode	Disable ▼

OK

Cancel

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.	
Obtain an IP address automatically	Click this radio button to obtain the IP address automatically if you want to use Dynamic IP mode.	
Specify an IP address	Click this radio button to specify dome data if you want to use Static IP mode. IP address - Type the IP address. Subnet Mask - Type the subnet mask. Gateway IP Address - Type the gateway IP address.	
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 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. • Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. • Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. TTL (Time to Live) - Set TTL value of PING operation. • Ping Interval - Type the interval for the system to execute the PING operation. • Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged. MTU It means Max Transmit Unit for packet. AP Discovery Click this button to open the Access Point Discovery window. Let wireless 2.4GHz do AP discovery and choose the Wireless AP you wan to connect to. Wireless LAN >> Access Point Discovery Access Point List BSSID Channel RSSI SSID Authentication Index 02:1D:AA:9F:E9:48 11 78% DravTek-LAN-B Mixed(WPA+WPA2)/PSK A 00:1D:AA:9F:E9:48 11 02:1D:AA:90:20:80 11 AP900-airtime ap902_2.4G_114_2 WPA2/PSK ap902_Wifi_114_1 AP900_110_Bandstee. AP900_110_2.4G-1 00:1D:AA:90:20:80 WPA2/PSK 02:50:7F:22:33:88 WPA2/PSK 11 WPA2/PSK Mixed(WPA+WPA2)/PSK 00:50:7F:22:33:88 TestRoaming2.4G-E 02:1D:AA:7E:41:80 00:1D:AA:7E:41:80 TestRoaming2.4G-A Mixed(WPA+WPA2)/PSK Mixed(WPA+WPA2)/PSK * 00:1D:AA:DD:75:00 v2860 lte 1 Scan AP's MAC address]:[]:[]:[] Universal 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 **SSID** The identification of the Wireless AP. The MAC Address of the Wireless AP. MAC Address (Optional) Channel The channel of frequency of the Wireless AP. Please notice that, if this setting is modified, the channel of Wireless LAN (2.4GHz) would be also modified. Security Mode The mode to connect to the Wireless AP. Disable - The Router connects to the wireless AP without any encryption mechanism. WEP - The Router connects to the wireless AP as a WEP client and the encryption key should be entered in WEP Key. 64-Bit - For 64 bits WEP key, either 5 ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.) • 128-Bit - For 128 bits WEP key, either 13 ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D). WEP keys - Four keys can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.

WPA/PSK - The Router connects to the wireless AP as a WPA client and the encryption key should be entered in PSK.

WPA/PSK uses TKIP as Encryption Mode. WPA2/PSK uses AES as Encryption Mode.

WPA2/PSK - The Router connects to the wireless AP as a WPA2 client and the encryption key should be entered in PSK

Pass Phrase - The PSK. Either 8~63 ASCII characters, such as 012345678.. (or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

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

II-1-2-9 Details Page for 3G/4G USB Modem (PPP mode) in WAN3/WAN4

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 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) Modem Support List 3G/4G USB Modem(PPP mode) O Enable O Disable SIM PIN code AT&FE0V1X1&D2&C1S0=0 Modem Initial String (Default: AT&FE0V1X1&D2&C1S0=0) APN Name Apply ΑT Modem Initial String2 Modem Dial String ATDT*99# (Default: ATDT*99#, CDMA: ATDT#777, TD-SCDMA: ATDT*98*1#) Service Name (Optional) PPP Username (Optional) PPP Password (Optional) PPP Authentication PAP or CHAP Index(1-15) in Schedule Setup: **WAN Connection Detection** Mode ARP Detect V

Available settings are explained as follows:

OK

Item	Description	Description				
Modem Support List	It lists all of the	It lists all of the modems supported by such router.				
	i8.1.1/doc/pppsuptlst.htm	38.1.1/doc/pppsupdst.htm				
	3G/4G Modern Support List	3G/4G Modern Support List(PPP mode)				
	environment or countries.	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.				
	Aiko	Model Aiko 83D	LTE	Status Y		
	Alcatel	Alcatel L100V	Ø	· ·		
	Alcatel	Alcatel W100	<u> </u>	' '		
	BandRich	Bandluxe C170	9	Y		
	BandRich	Bandluxe C170		Y		
	BandRich	Bandluxe C321		Y		
	BandRich	Bandluxe C330		Ÿ		
	BandRich	Bandluxe C331		Y		
	BandRich	Bandluxe C502		Y		
	D-Link	D_LINK DWM221 B1	Ø	Y		
	Huawei	Huawei E169u		Y		
	Huawei	Huawei E220		Y		
	Huawei	Huawei E303D		Y		
	1	in a service of the s	İ			
3G /4G USB Modem (PPP mode)		activating this fund II be closed and all				

Cancel

Default

	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. Type 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	Type the PPP username (optional). The maximum length of the name you can set is 63 characters.	
PPP Password	Type 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.	
Index (1-15) in Schedule Setup	You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page	
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.	
	Mode - Choose ARP Detect or Ping Detect for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items.	
	 Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. 	
	 Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. 	
	With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off.	
	TTL (Time to Live) - Set TTL value of PING operation.	
	Ping Interval - Type the interval for the system to	

execute the PING operation.
 Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.

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

II-1-2-10 Details Page for 3G/4G USB Modem (DHCP mode) in WAN3/WAN4

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/WAN4. The following web page will be shown.

WAN >> Internet Access WAN 3 3G/4G USB Modem(PPP mode) 3G/4G USB Modem(DHCP mode) Modem Support List 3G/4G USB Modem(DHCP mode) Enable Disable SIM PIN code Network Mode 4G/3G/2G (Default: 4G/3G/2G) APN Name MTU 1380 (Default: 1380) Choose IP Path MTU Discovery LTE hardware version **WAN Connection Detection** ARP Detect 💌

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



Item	Description				
Modem Support List	It lists all of the modems supported by such router.				
	≥ http://192.1661.1/40c/explict(G.htm - windows Internet Explorer © 192.1681.1/40c/explict(G.htm - windows Internet Explorer				
	4G Modern Support List				
		Last up	dated on 2013-05-13		
	Standard	Brand	Module	Status	
	LTE	ZTE	ZTE MF821D	*	
3G/4G USB Modem (DHCP mode)	Click Enable for activating this function. If you click Disable, this function will be closed and all the settings that you adjusted in this page will be invalid.				
SIM PIN code	Type PIN code of the SIM card that will be used to access Internet.				
	The maximum length of the PIN code you can set is 19 characters.				
Network Mode	Force Vigor router to connect Internet with the mode specified here. If you choose 4G/3G/2G as network mode,				

	the router will choose a suitable one according to the actual wireless signal automatically.
APN Name	APN means Access Point Name which is provided and required by some ISPs. Type the name and click Apply .
	The maximum length of the name you can set is 47 characters.
MTU	It means Max Transmit Unit for packet. Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path. Click Choose IP to open the following dialog.
	172.17.11.1/doc/pathmtu.htm
	Path MTU to: IPv4 Host ▼ MTU reduce size by B Detect Note: You may reduce the Path MTU Size(max 1500) by 1 to 100. Accept Cancel
	 Path MTU to - Type the IP address as the specific transmit path. 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
WAN Connection Detection	displayed in the field of MTU. Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode - Choose ARP Detect or Ping Detect for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items.
	 Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging.
	 Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off.
	• TTL (Time to Live) - Set TTL value of PING operation.
	 Ping Interval - Type the interval for the system to execute the PING operation.
	 Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.

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

II-1-2-11 Details Page for 3G/4G USB Modem (DHCP mode) in LTE WAN

It is available for "L" model only. LTE WAN uses the embedded LTE module to access internet.

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 LTE. The following web page will be shown.

WAN >> Internet Access LTE 3G/4G LTE Modem(DHCP mode) IPv6 3G/4G USB Modem(DHCP mode) Enable Disable SIM PIN code 4G/3G/2G ▼ (Default:4G/3G/2G) Network Mode APN Name UserName (Optional) Password (Optional) Authentication None (Default: 1380) MTU 1380 Path MTU Discovery Choose IP 20002 LTE hardware version **WAN Connection Detection** ARP Detect ▼ Mode Note: Please note that in some case USB port connection will be terminated temporarily to activate the

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

Item	Description		
3G/4G USB Modem (DHCP mode)	Click Enable for activating this function. If you click Disable, this function will be closed and all the settings that you adjusted in this page will be invalid.		
SIM PIN code	Type PIN code of the SIM card that will be used to access Internet. The maximum length of the PIN code you can set is 19 characters.		
Network Mode	Force Vigor router to connect Internet with the mode specified here. If you choose 4G/3G/2G as network mode, the router will choose a suitable one according to the actual wireless signal automatically.		
APN Name	APN means Access Point Name which is provided and required by some ISPs. Type the name and click Apply . The maximum length of the name you can set is 47 characters.		
UserName	Type the username (optional). The maximum length of the name you can set is 63 characters.		
Password	Type the password (optional). The maximum length of the password you can set is 62 characters.		
Authentication	Select None or PAP or CHAP.		

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 Choose IP to open the following dialog. 172.17.11.1/doc/pathmtu.htm Path MTU to: IPv4 Host ▼ MTU reduce size by Detect Note: You may reduce the Path MTU Size(max 1500) by 1 to 100. Accept Cancel Path MTU to - Type the IP address as the specific transmit path. 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. LTE hardware version The hardware version of the embedded LTE module. **WAN Connection** Such function allows you to verify whether network Detection connection is alive or not through ARP Detect or Ping Detect. Mode - Choose ARP Detect or Ping Detect for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items. Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. • Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. TTL (Time to Live) - Set TTL value of PING operation. Ping Interval - Type the interval for the system to execute the PING operation. Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.

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

II-1-2-12 Details Page for IPv6 – Offline in WAN1/WAN2/WAN3/WAN4

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



II-1-2-13 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.



Available settings are explained as follows:

Item	Description
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.
	 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.

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





Info

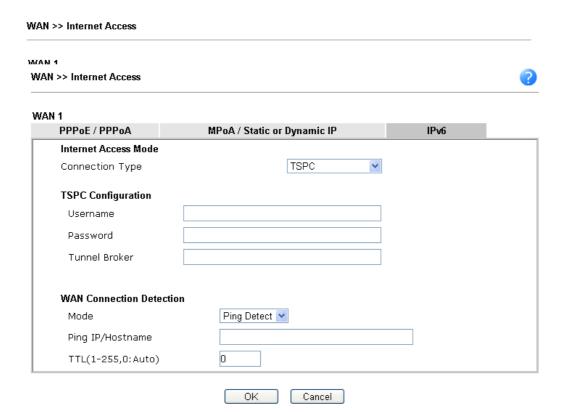
At present, the IPv6 prefix can be acquired via the PPPoE mode connection which is available for the areas such as Taiwan (hinet), the Netherlands, Australia and UK.

II-1-2-14 Details Page for IPv6 – TSPC in WAN1/WAN2/WAN3/WAN4

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.



Available settings are explained as follows:

Item	Description		
Username	Type the name obtained from the broker. It is suggested for you to apply another username and password for http://gogonet.gogo6.com/page/freenet6-account. The maximum length of the name you can set is 63 characters.		
Password	Type the password assigned with the user name. The maximum length of the name you can set is 19 characters.		
Tunnel Broker	Type 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. 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-1-2-15 Details Page for IPv6 – AICCU in WAN1/WAN2/WAN3/WAN4

1			
PPPoE / PPPoA	MPoA/S	tatic or Dynamic IP	IPv6
Internet Access Mod	le		
Connection Type		AICCU 💌	
AICCU Configuration	n		
Always On			
Username			
Password			
Tunnel Broker	tic.sixxs.net		
Tunnel ID			
Subnet Prefix		/	

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



Item	Description		
Always On	Check this box to keep the network connection always.		
Username	Type the name obtained from the broker. Please apply new account at http://www.sixxs.net/. It is suggested for you to apply another username and password. The maximum length of the name you can set is 19 characters.		
Password	Type 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. Type 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). Type the ID offered by Tunnel Broker.		
Subnet Prefix	Type 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.

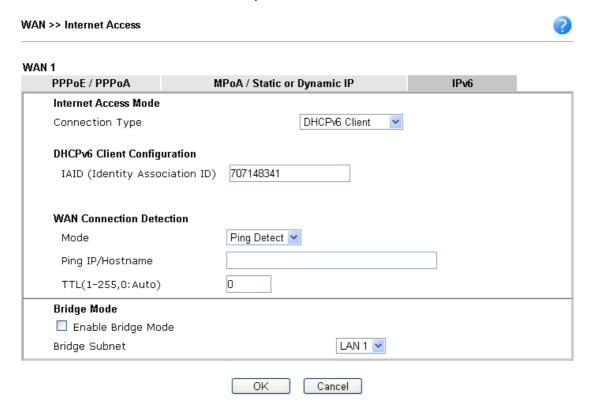
Mode - Choose **Always On** or **Ping Detect** for the system to execute for WAN detection.

- 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-1-2-16 Details Page for IPv6 – DHCPv6 Client in WAN1/WAN2

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



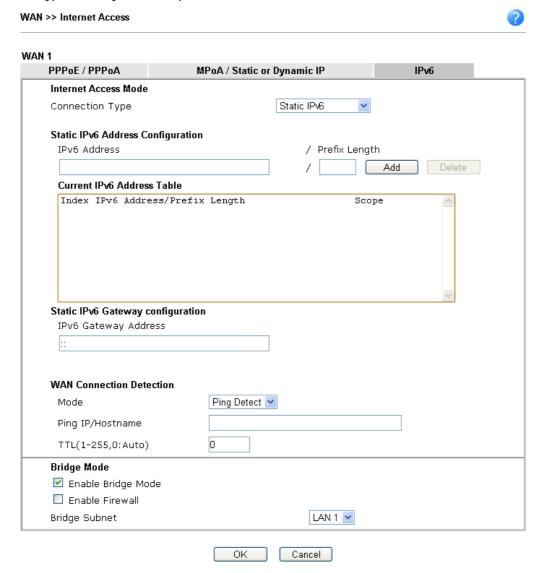
Item	Description			
Identify Association	Choose Prefix Delegation or Non-temporary Address as the identify association.			
IAID	Type a number as IAID.			
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through NS Detect or Ping Detect.			
	Mode - 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.			
	 Ping IP/Hostname - If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. 			
	 TTL (Time to Live) -If you choose Ping Detect as detection mode, you have to type TTL value. 			
Bridge Mode	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-1-2-17 Details Page for IPv6 – Static IPv6 in WAN1/WAN2

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



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

Detection	connection is alive or not through Ping Detect.			
Detection	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.			
	 Ping IP/Hostname - If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. 			
	 TTL (Time to Live) -If you choose Ping Detect as detection mode, you have to type TTL value. 			
Bridge Mode	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.			

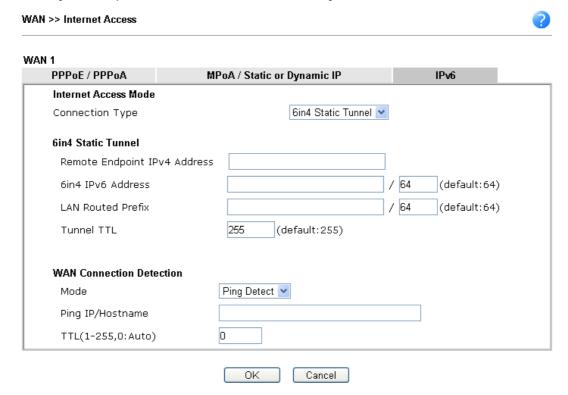
After finished the above settings, click \mathbf{OK} to save the settings.

II-1-2-18 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.



Available settings are explained as follows:

Item	Description		
Remote Endpoint IPv4 Address	Type the static IPv4 address for the remote server.		
6in4 IPv6 Address	Type the static IPv6 address for IPv4 tunnel with the value for prefix length.		
LAN Routed Prefix	Type the static IPv6 address for LAN routing with the value for prefix length.		
Tunnel TTL	Type the number for the data lifetime in tunnel.		
WAN Connection Detection	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.		
	 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. 		

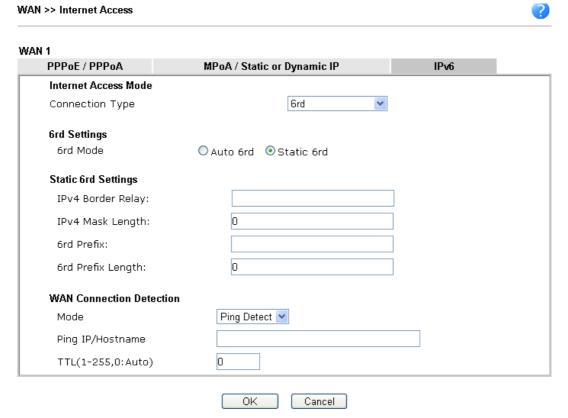
After finished the above settings, click \mathbf{OK} to save the settings.

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

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

II-1-2-19 Details Page for IPv6 – 6rd in WAN1/WAN2

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



Item	Description
6rd Mode	Auto 6rd - Retrieve 6rd prefix automatically from 6rd service provider. The IPv4 WAN must be set as "DHCP". Static 6rd - Set 6rd options manually.

IPv4 Border Relay	Type the IPv4 addresses of the 6rd Border Relay for a given 6rd domain.
IPv4 Mask Length	Type a number of high-order bits that are identical across all CE IPv4 addresses within a given 6rd domain. It may be any value between 0 and 32.
6rd Prefix	Type the 6rd IPv6 address.
6rd Prefix Length	Type the IPv6 prefix length for the 6rd IPv6 prefix in number of bits.
WAN Connection Detection	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.
	 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 IPv4				System Uptime: 0day 0:9:15
			IPv6	THE CONTRACTOR OF THE STREET
LAN Status				
IP Address				
	55:1D00:21D:AAFF: FF:FE83:11B4/64 (bal)	
TX Packets	RX Packets	TX Bytes	RX Bytes	
15	113	1354	18040	
WAN1 IPv6 Status	5		Part to the second	
Enable	Mode	Up Time		
Yes	6rd	0:09:06		
IP			Gateway IP	
(Global)	55:1D01:21D:AAFF:	FE83:11B5/128	<u> </u>	
	51D/128 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes	
13	29	967	2620	

II-1-3 Multi-PVC/VLAN

This router allows you to create multi-PVC for different data transferring for using. Simply go toWAN and select Multi-PVC/VLAN page.

General

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

WAN >> Multi-PVC//LAN

Mul	Multi-PVC/VLAN							
	General Advanced		Advanced					
Ch	annel	Enable	WAN Type	VPI/VCI	VLAN Tag	Port-based Bridge		
1		Yes	ADSL	0/33	None			
2		Yes	Ethernet(WAN2)		None			
<u>5.</u>	WAN5	No	ADSL	1/45	None	☐ Enable ☐ P1 ☐ P2 ☐ P3 ☐ P4 ☐ P5 ☐ P6		
<u>6.</u>	WAN6	No	ADSL	1/46	None	☐ Enable ☐ P1 ☐ P2 ☐ P3 ☐ P4 ☐ P5 ☐ P6		
<u>Z.</u>	WAN7	No	ADSL	1/47	None	Enable P1 P2 P3 P4 P5 P6		
<u>8.</u>		No	ADSL	1/48	None	☐ Enable ☐ P1 ☐ P2 ☐ P3 ☐ P4 ☐ P5 ☐ P6		
<u>9.</u>		No	ADSL	0/0	None	Enable P1 P2 P3 P4 P5 P6		
<u>10.</u>	<u>.</u>	No	ADSL	0/0	None	☐ Enable ☐ P1 ☐ P2 ☐ P3 ☐ P4 ☐ P5 ☐ P6		

Note:

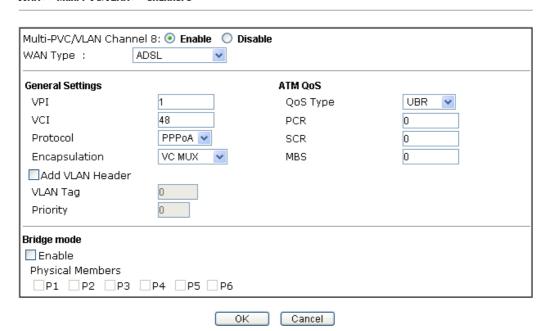
Channel 3 and channel 4 are reserved for USB WAN.



Item	Description
Channel	Display the number of each channel.
	Channels 1 and 2 are used by the Internet Access web user interface and can not be configured here.
	Channels 5 ~ 10 are configurable.
Enable	Display whether the settings in this channel are enabled (Yes) or not (No).
WAN Type	Displays the physical medium that the channel will use.
VPI/VCI	Display the value for VPI and VCI.
VLAN Tag	Displays the VLAN tag value that will be used for the packets traveling on this channel.
Port-based Bridge	The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value.
	Enable - Check this box to enable the port-based bridge function on this channel.
	P1 ~ P6 - Check the box(es) to build bridge connection on LAN.

Click any index (8~10) to get the following web page:

WAN >> Multi-PVC/VLAN >> Channel 8



Item	Description
Multi-VLAN Channel 8/9/10	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-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. ADSL VDSL Ethernet(WAN2)
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. Encapsulation - Choose a proper type for this channel. The types will be different according to the protocol setting that you choose. 1483 Route IP LLC 1483 Route IP LC 1483 Route IP LCC
	Add VLAN Header - Check the box to enable the following two options.
	VLAN Tag - Type the value as the VLAN ID number. Valid

	settings are in the range from 1 to 4095. The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value. Priority - Choose the number to determine the packet priority for such VLAN. The range is from 0 to 7.
ATM OoS	QoS Type - Select a proper QoS type for the channel. UBR UBR CBR ABR nrtVBR rtVBR Type the values for PCR, SCR and MBS respectively.
Bridge mode	Enable - Click it to enable Bridge mode for such channel. Physical Members - Group the physical ports by checking the corresponding check box(es) for applying the bridge connection.

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

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

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

Multi-PVC/VLAN Chanr WAN Type :	nel 5: Enable Disa ADSL	ble		
General Settings		ATM QoS		
VPI	1	QoS Type	UBR 🔻	
	45	PCR	0	
VCI				
Protocol	PPPoA 💌	SCR	0	
Encapsulation 	VC MUX	MBS	0	
Add VLAN Header				
VLAN Tag	0			
Priority	0			
Open Port-based Bridge Connection for this Channel Physical Members □ P1 □ P2 □ P3 □ P4 □ P5 □ P6 ✓ Open WAN Interface for this Channel WAN Application: Management ✓ WAN Connection Detection Mode □ ARP Detect ✓				
PPPoE/PPPoA Client		MPoA (RFC1483/26	84)	
ISP Access Setup		Obtain an IP ad	ldress automatically	
ISP Name		Router Name	Vigor *	
Username		Domain Name	*	
Password		*: Required for s	some ISPs	
PPP Authentication	PAP or CHAP	Specify an IP a	ddress	
☑ Always On		IP Address		
Idle Timeout	-1 second(s)	Subnet Mask		
IP Address From ISP		Gateway IP Add	ress	
	No (Dynamic IP)	DNS Server IP Add	reee	
Fixed IP Ves 🔮	(- , ,	DIAS SELVEL IF AUG	11033	
Fixed IP O Yes • Fixed IP Address		Primary IP Address		

Available settings are explained as follows:

Item	Description
Multi-VLAN Channel 5/6/7	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.

Cancel

OK

	ADSL VDSL Ethernet(WAN2)
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. Encapsulation - Choose a proper type for this channel. The types will be different according to the protocol setting that you choose.
	1483 Route IP LLC 1483 Bridged IP LLC 1483 Route IP LLC 1483 Route IP LLC 1483 Route IP LLC 1483 Route IP VC-Mux 1483 Bridged IP VC-Mux 1483 Routed IP VC-Mux(IPoA) 1483 Bridged IP(IPoE) Add VLAN Header - Check the box to enable the following
	two options. VLAN Tag - Type the value as the VLAN ID number. Valid settings are in the range from 1 to 4095. The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value.
	Priority - Choose the number to determine the packet priority for such VLAN. The range is from 0 to 7.
ATM OoS	QoS Type - Select a proper QoS type for the channel. Type the values for PCR, SCR and MBS respectively.
Open Port-based Bridge Connection for this Channel	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.
	Physical Members - Group the physical ports by checking the corresponding check box(es) for applying the port-based bridge connection.
Open WAN Interface for this Channel	Check the box to enable relating function. WAN Application - 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.
WAN Setup	It is available only when VDSL or Ethernet (WAN2) is selected as WAN Type. Choose PPPoE/PPPoA Client or Static or Dynamic IP as the WAN mode for such channel. If PPPoE/PPPoA Client is selected as WAN Setup, you have to configure the settings listed under ISP Access Setup. Enter your allocated username, password and authentication parameters according to the information
	provided by your ISP.

ISP Name - Type in the name of your ISP.

Username - Type in the username provided by ISP in this field. The maximum length of the name you can set is 80 characters.

Password - Type in the password provided by ISP in this field. The maximum length of the password you can set is 48 characters.

PPP Authentication - Select PAP only or PAP or CHAP for PPP.

- Always On Check it to keep the network connection always.
- ➤ Idle Timeout Set the timeout for breaking down the Internet after passing through the time without any action.

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

 If Static or Dynamic IP is selected as WAN Setup, you have to configure the settings listed under WAN IP Network Settings.

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

- Router Name Type in the router name provided by ISP.
- Domain Name Type in the domain name that you have assigned.

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

- > IP Address Type in the private IP address.
- > Subnet Mask Type in the subnet mask.
- > Gateway IP Address Type in gateway IP address.

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

Such function is available only when ADSL is selected as WAN Type.

It allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.

Mode - Choose ARP Detect or Ping Detect for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items.

- Primary/Secondary Ping IP If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging.
- Ping Gateway IP If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging.

With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off.

- TTL (Time to Live) Set TTL value of PING operation.
- Ping Interval Type the interval for the system to execute the PING operation.
- Ping Retry Type the number of times that the system is allowed to execute the PING operation before WAN

	disconnection is judged.		
PPPoE/PPPoA Client	Enter your allocated username, password and authentication parameters according to the information provided by your ISP.		
	ISP Name - Type in the name of your ISP.		
	Username - Type in the username provided by ISP in this field. The maximum length of the name you can set is 80 characters.		
	Password - Type in the password provided by ISP in this field. The maximum length of the password you can set is 48 characters.		
	PPP Authentication - Select PAP only or PAP or CHAP for PPP.		
	Always On - Check it to keep the network connection always.		
	Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action.		
	Fixed IP - Click Yes to use this function and type in a fixed IP address in the box of Fixed IP Address.		
MPoA (RFC1483/2684)	Obtain an IP address automatically - Click this button to obtain the IP address automatically.		
	 Router Name - Type in the router name provided by ISP. 		
	 Domain Name - Type in the domain name that you have assigned. 		
	Specify an IP address - Click this radio button to specify some data.		
	IP Address - Type in the private IP address.		
	Subnet Mask - Type in the subnet mask.		
	Gateway IP Address - Type in gateway IP address.		
	DNS Server IP Address - Type in the primary IP address for the router if you want to use Static IP mode. If necessary, type in secondary IP address for necessity in the future.		

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

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 **PCR** SCR MBS **PVC to PVC Binding** QoS Type 1. UBR 0 0 0 Disable 🔻 0 0 0 2. Disable 🔽 5. 0 0 0 Disable 🔻 0 0 0 6. Disable 💌 0 0 0 7. Disable 🔻 UBR 0 0 0 8. Disable 🔻 0 9. 0 0 UBR 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 and channel 4 are reserved for USB WAN.



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		tup	Monitor Page		
Index	Enable	Quota	When quota exceeded	Time cycle	Duration
WAN1	X	OMB/OMB			0/00/00 00:00~0/00/00 00:00
WAN2	×	OMB/OMB			0/00/00 00:00~0/00/00 00:00
WAN3	×	OMB/OMB			0/00/00 00:00~0/00/00 00:00
WAN4	×	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.
 - When hardware acceleration function is used, the monitored WAN traffic of Ethernet WAN interfaces may be slightly inaccurate.

Click WAN1/WAN2/WAN3/WAN4 link to open the following web page.

WAN >> WAN Budget

O		ND W
Quota Limit:	U	MB 💌
When quota exceeded :	Shutdo\	vn WAN interface
	Send Ma	ail Alert to Administrator
	Send SN	1S messages to Administrator
Monthly	Custom	
Select the day of a month when your (cellular) data resets.		

- Note: 1. Please make sure the <u>Time and Date</u> of the router is configured.
- 2. After clicking OK, the counter used in WAN Budget for this WAN interface will be reset.



Item	Description
Enable	Check the box to enable such function.
Quota Limit	Type 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. Send Mail Alert to Administrator - 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.

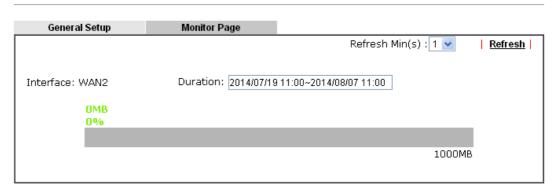
		dministrator - The system will se Idministrator when the quota is	end
Monthly		the network limitation based on this setting is to offer a mechanisecord every month.	
	Monthly	Custom	
	Select the day of a mont Data quota resets on da	h when your (cellular) data reset y 1 💟 at 00:00 💟	s.
	Data quota resets on day day in one month.	u You can determine the start	ing
Custom	This setting allows the us according to his request.	ser to define the billing cycle	
	The WAN budget will be reset with an interval of billing cycle.		
	period is required, use Cu is between 1 day and 60 of	ult setting. If long period or a shoustom. The period of cycle durations. You can determine the cycle days and the hours. In addition yof today is in a cycle.	ion le
	Monthly	Custom	
		t the beginning of each cycle. days and 0 v hours	
	record. For example, 20 means the whole cy	fy the days to reset the traffic 7 means the whole cycle is 7 day ycle is 20 days. When the time is the traffic record automatically.	
	point which Vigor rout	the day in the cycle as the start ter will reset the traffic record. F he third day of the cycle duration	or

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

II-1-4-2 Monitor Page

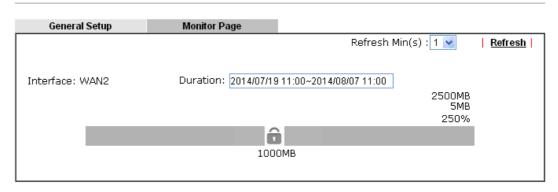
The monitor page displays the status WAN budget, including the duration and the usage.

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 configure settings for IPv6 Service in Vigor2860

Due to the shortage of IPv4 address, more and more countries use IPv6 to solve the problem. However, to continually use the original rich resources of IPv4, both IPv6 and IPv4 networks shall communicate for each other via intercommunication mechanism to complete the shifting job from IPv4 to IPv6 gradually. At present, there are three common types of intercommunication mechanisms:

Dual Stack

The user can use both IPv4 and IPv6 techniques at the same time. That means adding an IPv6 stack on the origin network layer to let the host own the communication capability of IPv4 and IPv6.

Tunnel

Both IPv6 hosts can communication for each other via existing IPv4 network environment. The IPv6 packets will be encapsulated with the header of IPv4 first. Later, the packets will be transformed and judged by IPv4 router. Once the packets arrive the border between IPv4 and IPv6, the header of IPv4 on the packets will be removed. Then, the packets with IPv6 address will be forwarded to the destination of IPv6 network.

Translation

Such feature is active only for the user who uses IPv4 to communicate with other user using IPv4 service.

Before configuring the settings on Vigor2860, you need to know which connection type that your IPv6 service used.



Info

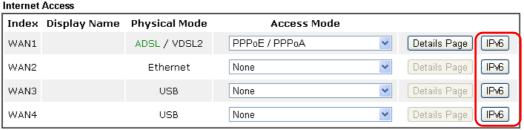
For the IPv6 service, you have to configure WAN/LAN settings before using the service.

I. Configuring the WAN Settings

For the IPv6 WAN settings for Vigor2860, there are five connection types to be chosen: PPP, TSPC, AICCU, DHCPv6 Client and Static IPv6.

Access into the web user interface of Viogr2860. Open WAN>> Internet Access. Choose
one of the WAN interfaces as the one supporting IPv6 service. Then, click the IPv6
button of the selected WAN.

WAN >> Internet Access



Note: 1. Device on USB port 1 applies WAN3 configuration.
Device on USB port 2 applies WAN4 configuration.

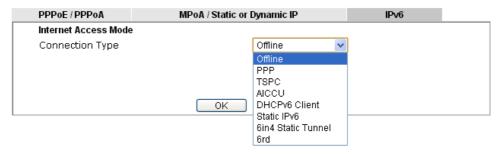
Advanced You can configure DHCP client options here.



Info

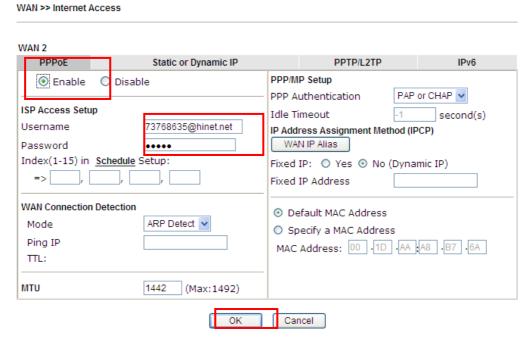
Only one WAN interface support IPv6 service at one time. In this example, WAN2 is chosen as the one supporting IPv6 service.

2. In the following figure, use the drop down list to choose a proper connection type.



Different connection types will bring out different configuration page. Refer to the following:

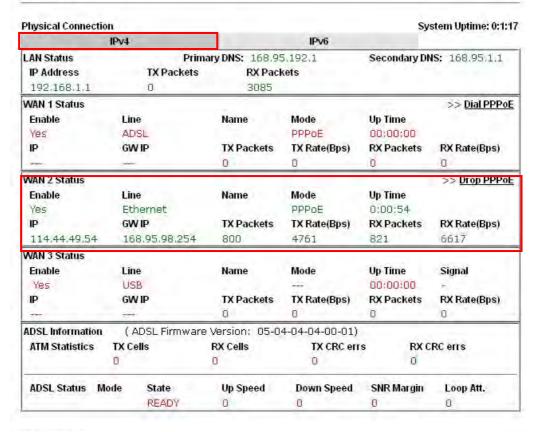
PPP - Dual Stack application, IPv4 and IPv6 services can be utilized at the same time
 Choose PPP and type the information for PPPoE of IPv4.



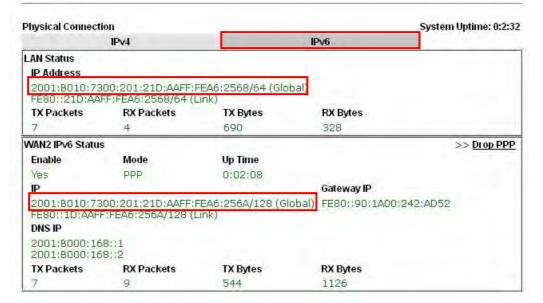
Access into the setting page for IPv6 service, it is not necessary for you to configure anything.



Click **OK** and open **Online Status**. If the connection is successful, you will get the IP address for IPv4 and IPv6 at the same time.



Online Status



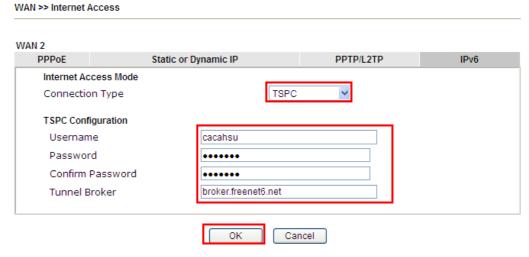
TSPC - Tunnel application, both IPv6 hosts communicate through IPv4 network
 Choose TSPC and type the information for TSPC service.

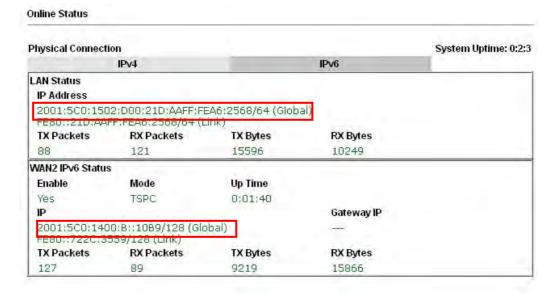


Info

While using such mode, you have to make sure the IPv4 network connection is normal.

(In the following figure, the TSPC information is obtained from http://gogo6.com/ after applied for the service.)





AICCU - Tunnel application

Choose AICCU and type the information for AICCU of IPv6.



Info

WAN >> Internet Access

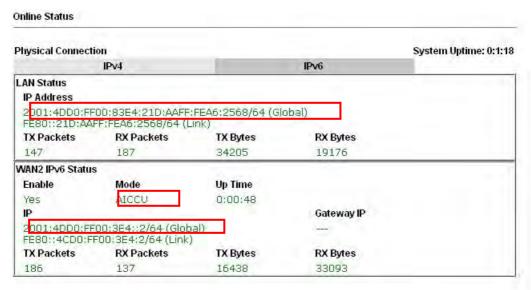
While using such mode, you have to make sure the IPv4 network connection is normal.

(In the following figure, the AICCU information is obtained from https://www.sixxs.net/main/ after applied for the service.)

WAN 2 Static or Dynamic IP PPTP/L2TP IPv6 **PPPoE** Internet Access Mode AICCU Connection Type **AICCU Configuration** Always On JCR3-SIXXS Username Password •••• Confirm Password •••• Tunnel Broker Subnet Prefix 2001:4DD0:FF00:8805::2 / 64

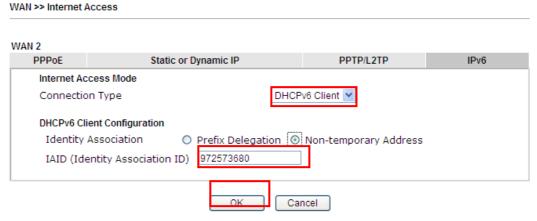
Note: If "Always On" is not enabled, AICCU connection would only retry three times.

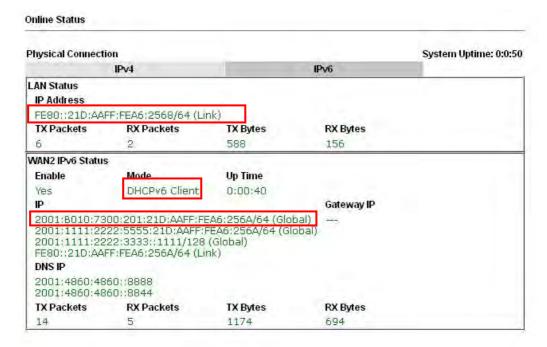




DHCPv6 Client

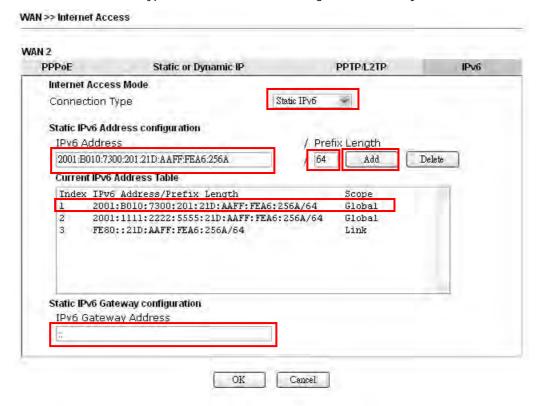
Choose DHCPv6 Client. Click one of the identity associations and type the IAID number.

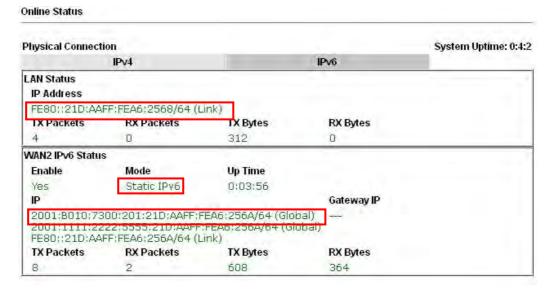




Static IPv6

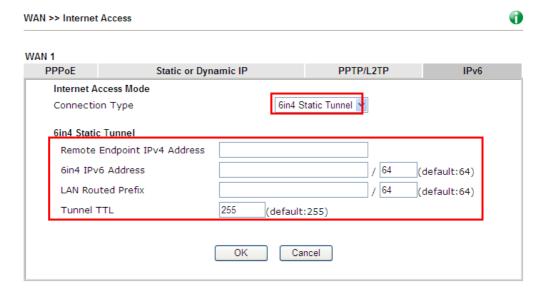
Choose Static IPv6. Type IPv6 address, Prefix Length and Gateway Address.

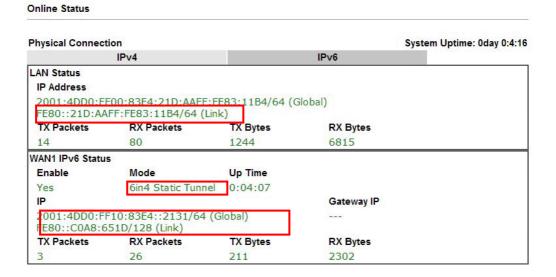




6in4 Static Tunnel

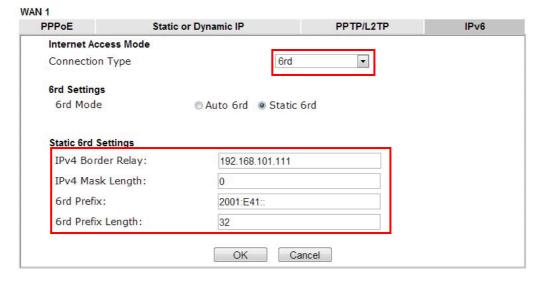
Choose 6in4 Static Tunnel. Type remote endpoint IPv4 address, 6in4 IPv6 Address, LAN Routed Prefix and Tunnel TTL.





6rd

Choose 6rd. Type IPv4 Border Relay, IPv4 Mask Length, 6rd Prefix and 6rd Prefix Length.



Click **OK** and open **Online Status**. If the connection is successful, the physical connection will be shows as follows:

Online Status **Physical Connection** System Uptime: 0day 0:9:15 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** 18040 15 113 1354 WAN1 IPv6 Status Enable Mode **Up Time** Yes 6rd 0:09:06 IP Gateway IP 2001:E41:A865:1D01:21D:AAFF:FE83:11B5/128 FE80::C0A8:651D/128 (Link) TX Bytes **RX** Bytes TX Packets **RX Packets** 13 29 967 2620

II. Configuring the LAN Settings

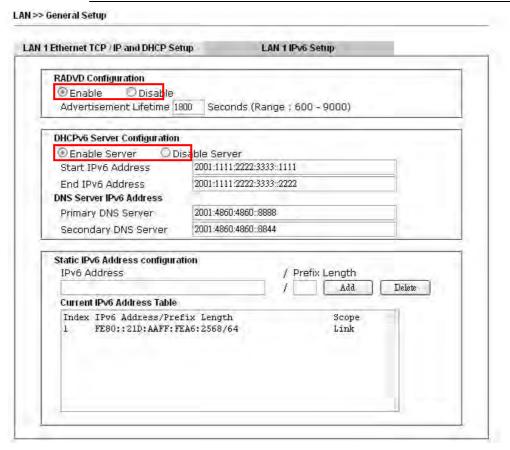
After finished the WAN settings for IPv6, please configure the LAN settings to make the router's client get the IPv6 address.

 Access into the web user interface of Viogr2860. Open LAN>> General Setup. Click the IPv6 button.



Info

Only the subnet of LAN1 supports IPv6 feature.



- 2. In the field of RADVD Configuration, the default setting is Enable. The client's PC will ask RADVD service for the Prefix of IPv6 address automatically, and generate an Interface ID by itself to compose a full and unique IPv6 address.
- 3. In the field of DHCPv6 Server Configuration, when DHCPv6 service is enabled, you can assign available IPv6 address for the client manually.



Info

When both mechanisms are enabled, the client can determine which mechanism to be used (e.g., the default mechanism for Windows7 is RADVD).

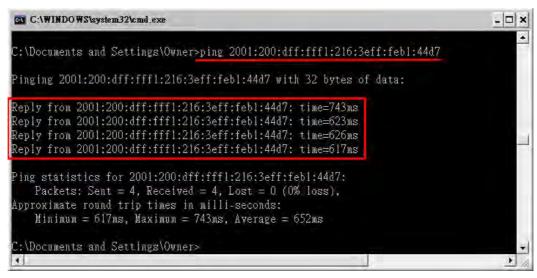
III. Confirming IPv6 Service Run Successfully

1. Make sure you have obtained the correct IPv6 IP address. Get into MS-DOS interface and type the command of "ipconfig". Refer to the following figure.

```
CAWINDOWS\system32\cmd_exe
                                                              - 0 ×
:\Documents and Settings\Owner>ipconfig
indows IP Configuration
Ethernet adapter Test Line 5:
     Connection-specific DNS Suffix . :
     IP Address. . . . . . . . . : 192.168.1.10
                            . . : 255.255.255.0
     Subnet Mask
     IP Address. . . . . . . . . . . : fe80::211:95ff:fe83:e1bc%4
     Default Gateway . . . . . . . . . . . . 192.168.1.1
                                 fe80::250:7fff:feea:7ee0%4
Ethernet adapter DrayTek Virtual Interface:
     Media State . . . . . . . . . . . . Media disconnected
```

From the above figure we can see IPv6 IP address has been captured by the system.

2. Use the Ping command to ping any IPv6 address indicating an IPv6 website. For example, www.kame.net is a website supporting IPv4 IP and IPv6 IP services. Its IPv6 address is seen with a format of 2001:200:dff:fff1:216:3eff:feb1:44d7.



After getting the above message, it means the IPv6 service has been activated successfully.

3. Connect to the website for IPv6. Open a web browser and type an URL of IPv6, e.g., www.kame.net. If your computer accesses into the website by using IPv6 address, you may see a turtle dancing on the screen. If not, only a steady turtle will be seen.

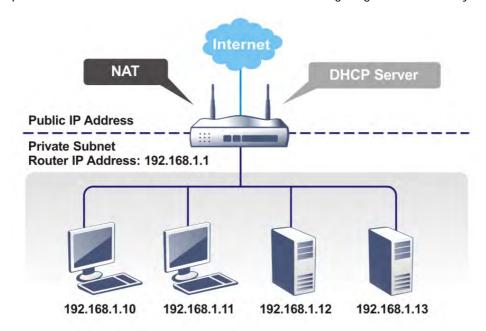


If you can see a turtle dancing on the screen, that means IPv6 service is ready for you to access and utilize.

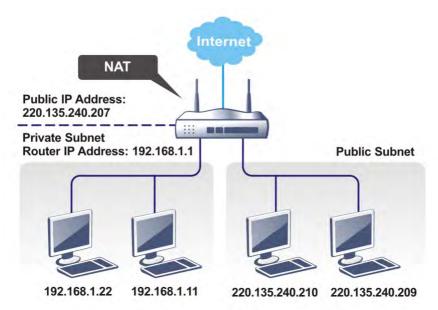
II-2 LAN

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)

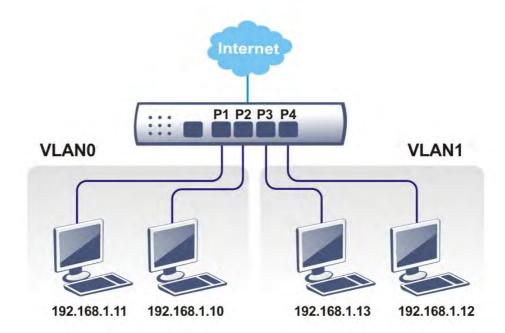
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

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 six subnets provided by the router which allow users to divide groups into different subnets (LAN1 - LAN6). 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 - LAN6 can be operated under NAT or Route mode. IP Routed Subnet can be operated under Route mode.

LAN >> General Setup

General Setup					
Index	Status	DHCP	IP Address		
LAN 1	٧	٧	192.168.1.1	Details Page	IPv6
LAN 2	\checkmark	~	192.168.5.1	Details Page	IPv6
LAN 3		✓	192.168.3.1	Details Page	IPv6
LAN 4		~	192.168.4.1	Details Page	IPv6
LAN 5		✓	192.168.5.1	Details Page	IPv6
LAN 6		~	192.168.6.1	Details Page	IPv6
DMZ Port		V	192.168.7.1	Details Page	IPv6
IP Routed Subnet		\checkmark	192.168.0.1	Details Page	

Advanced You can configure DHCP server options here.

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

Inter-LAN Routing

Subnet	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5	LAN 6	DMZ Port
LAN 1	✓						
LAN 2	✓	V					
LAN 3			V				
LAN 4				V			
LAN 5					✓		
LAN 6						✓	
DMZ Port							✓

Note: LAN 2/3/4/5/6 are available when VLAN is enabled.

DMZ subnet is default bound to P1, and will overwrite the settings of P1 at LAN>>VLAN page.



Item	Description
General Setup	Allow to configure settings for each subnet respectively. Index - Display all of the LAN items. Status- Basically, LAN1 status is enabled in default. LAN2 -LAN6 and IP Routed Subnet can be observed by checking the box of Status.

DHCP- LAN1 is configured with DHCP in default. If required, please check the DHCP box for each LAN. IP Address - Display the IP address for each LAN item. Such information is set in default and you can not modify it. Details Page - Click it to access into the setting page. Each LAN will have different LAN configuration page. Each LAN must be configured in different subnet. IPv6 - Click it to access into the settings page of IPv6. DHCP packets can be processed by adding option number and Advanced data information when such function is enabled. I AN >> General Setur **DHCP Server Customized Status** Customized List Enable Interface Option Enable: 🗹 Interface: All LAN1 LAN2 LAN3 LAN4 LAN5 LAN6 DMZ IP Routed Subnet Next Server IP Address/SIAddr : Option Number: DataType:
• ASCII Character (EX:Option:18, Data:/path) O Hexadecimal Digit (EX: Option: 18, Data: 2f70617468) O Address List (EX :Option: 44, Data: 172.16.2.10,172.16.2.20...) Data: Add Update Delete Reset Enable/Disable - Enable/Disable the function of DHCP Option. Each DHCP option is composed by an option number with data. For example, Option number: 100 Data: abcd When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets. Interface - Choose the interface for such option. Next Server IP Address/SIAddr - Type the IP address of PXE server which is helpful for downloading boot loader via network. **Option Number -** Type a number for such function. DataType - Choose the type (ASCII or Hex or IP) for the data to be stored. Data - Type the content of the data to be processed by the function of DHCP option. Force Vigor router to use DNS servers configured in Force router to use DNS LAN1/LAN2/LAN3/LAN4/LAN5/LAN6 instead of DNS servers server IP address 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		DHCP Server Configuration	
For NAT Usage			
IP Address	192.168.1.1	☐Enable Relay Agent	
Subnet Mask	255.255.255.0	Start IP Address 192.168.1.10	
		IP Pool Counts 200	
RIP Protocol Control	Disable 💌	Gateway IP Address 192.168.1.1	
		Lease Time 86400	(s)
		Clear DHCP lease for inactive clients periodically	
		DNS Server IP Address	
		Primary IP Address	
		Secondary IP Address	

Note: Change IP Address or Subnet Mask in Network Configuration will also change <u>HA</u> LAN1 Virtual IP to the same domain IP.

0K

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.
	Enable Server - Let the router assign IP address to every host in the LAN.
	Disable Server - Let you manually assign IP address to every host in the LAN.
	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.

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).

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:



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.

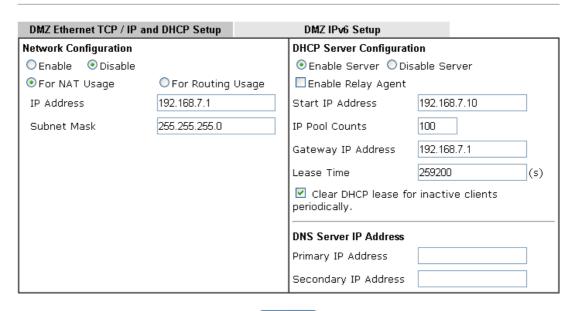
If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable)

connection.

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

II-2-1-2 Details Page for LAN2 ~ LAN6 and DMZ

LAN >> General Setup



OK

Item	Description
Network Configuration	Enable/Disable - Click Enable to enable such configuration; click Disable to disable such configuration.
	For NAT Usage - Click this radio button to invoke NAT function.
	For Routing Usage - Click this radio button to invoke this function.
	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: 255.255.25.0/ 24)
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.
	Enable Server - Let the router assign IP address to every host in the LAN.
	Disable Server - Let you manually assign IP address to every host in the LAN.
	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.
	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.

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.

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:



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.

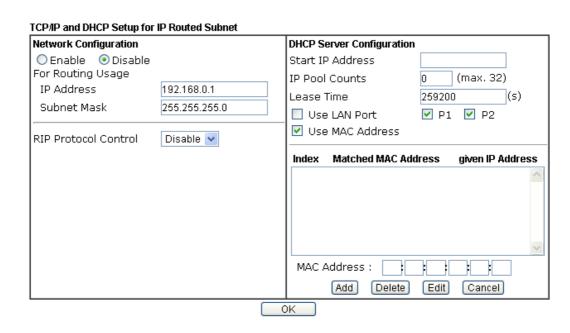
If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable)

connection.

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

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

LAN >> General Setup



Item	Description
Network Configuration	Enable/Disable - Click Enable to enable such configuration; click Disable to disable such configuration.
	For Routing Usage,
	IP Address - Type in private IP address for connecting to a local private network (Default: 192.168.1.1).
	Subnet Mask - Type in an address code that determines the size of the network. (Default: 255.255.25.0/ 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 dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.
	If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
	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.

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

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

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

MAC Address: Enter the MAC Address of the host one by one and click Add to create a list of hosts 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.

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

Delete - Click it to delete the selected MAC address.

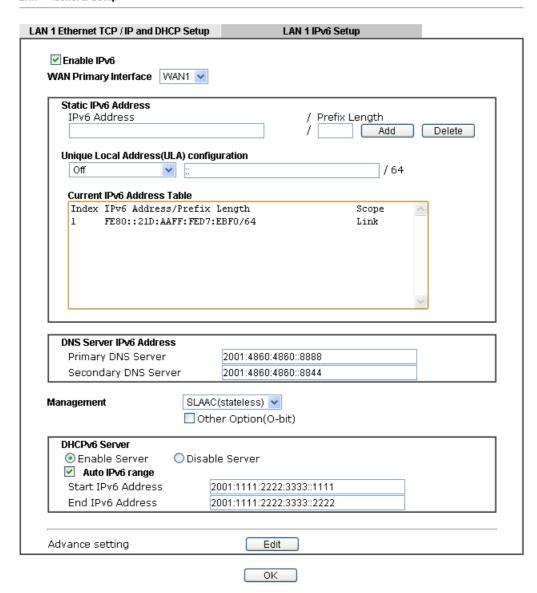
Edit - Click it to edit the selected MAC address.

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

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

II-2-1-4 Details Page for LAN IPv6 Setup

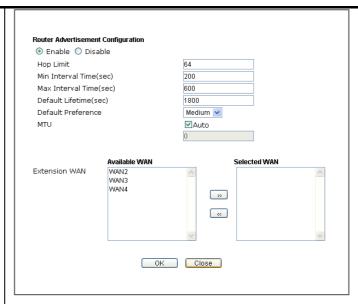
There are two configuration pages for LAN1/LAN2/LAN3/LAN4/LAN5/LAN6/DMZ Port, Ethernet TCP/IP and DHCP Setup (based on IPv4) and IPv6 Setup. Click the tab for each type and refer to the following explanations for detailed information. Below shows the settings page for IPv6.



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

Item	Description
Enable	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 configuration	IPv6 Address -Type static IPv6 address for LAN. Prefix Length - Type the fixed value for prefix length. Add - Click it to add a new entry. Delete - Click it to remove an existed entry.
Unique Local Address (ULA) configuration	Such feature is used for the host without assigned IPv6 address to obtain IPv6 address automatically or have an IPv6 address specified manually via ULA configuration. It is convenient for communication among different subnets.

	Off Off Auto ULA Prefix Manually ULA Prefix
	Auto ULA Prefix - The system will generate the required IPv6 address. Manually ULA Prefix - A user can type the ULA IPv6 address manually.
Current IPv6 Address Table	Display current used IPv6 addresses.
DNS Server IPv6 Address	Primary DNS Sever - Type the IPv6 address for Primary DNS server. Secondary DNS Server - Type another IPv6 address for DNS server if required.
Management	Host under LAN can be assigned IP address from Vigor router via the following method. SLAAC(stateless) DHCPv6(stateful) Off SLAAC(stateless) - The IP address (with Prefix) of the host shall be formed according to RA transmitted by Vigor router. DHCPv6(stateful) - The IP address of the host shall be assigned after communicating with DHCPv6 server for answering the request of client. Off - No IP address is assigned. Other Option (O-bit) - Check this box to enable the O-bit for obtaining additional information (e.g., DNS) from DHCPv6.
DHCPv6 Server Configuration	Enable Server -Click it to enable DHCPv6 server. DHCPv6 Server could assign IPv6 address to PC according to the Start/End IPv6 address configuration. Disable Server -Click it to disable DHCPv6 server. Start IPv6 Address / End IPv6 Address -Type the start and end address for IPv6 server.
Advance setting	More options are offered under the Advance setting . Click Edit to open the pop-up window.



Router Advertisement Server - 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 Limt - 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, Vigor2925 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.

Extension WAN - Not only the IP address can be obtained from the primary WAN, but also the prefix for IPv6 LAN IP address can be assigned by extension WAN specified here.

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

II-2-2 VLAN

With the 6-port Gigabit switch on the LAN side, 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 (Vigor2860n/Vigor2860n-plus/Vigor2860Vn-plus/Vigor2860ac/Vigor2860Vac), 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 ~ P6) 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 Vigor2860n:

LAN >> VLAN Configuration

VLAN Configuration ✓ Enable Wireless LAN VLAN Tag LAN P1 P2 P3 P4 P5 P6 SSID1 SSID2 SSID3 SSID4 Enable Subnet VID Priority VLANO | | | | | | | LAN 1 🔻 0 0 🕶 VLAN1 LAN 1 😽 0 🕶 VLAN2 0 LAN 1 🔽 0 🕶 VLAN3 0 LAN 1 🕶 0 🕶 0 VLAN4 | | | | | | | | LAN 1 🔻 0 🕶 0 0 🕶 LAN 1 💌 VLAN6 | | | | | | | | 0 0 🕶 LAN 1 🔻 0 VLAN7 0 🗸 LAN 1 💟

- Permit untagged device in P1 to access router
- 1. Tag based VLAN only applied for LAN Ports;
- The checked Wireless LAN SSID will not has VLAN tagging function but regarded as joining VLAN group;
- 3. The set VLAN ID (VID) must be unique and not duplicate.

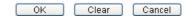


For Vigor2860n-plus series, the web page will be shown as follows:

LAN >> VLAN Configuration

VLAN Configuration ✓ Enable Wireless LAN(2.4GHz) Wireless LAN(5GHz) VLAN Tag P1 P2 P3 P4 P5 P6 SSID1 SSID2 SSID3 SSID4 SSID1 SSID2 SSID3 SSID4 Subnet Enable VID Priority VLAN0 🗸 🗌 🗸 🗸 🗸 🗸 V V V V V V LAN 1 💌 0 0 🕶 LAN 2 💌 0 0 🕶 VLAN2 🗌 🔲 🔲 🗹 🗸 LAN 3 🔽 V 172 0 🕶 VLAN3 🔲 🗎 🔲 🔲 🔲 LAN 1 🔽 0 0 🕶 VLAN4 | | | | | | | | | | LAN 1 🔽 0 0 🕶 LAN 1 💌 0 VLAN5 | | | | | | | | | 0 🕶 VLAN6 | | | | | | | | | LAN 1 💌 0 0 🕶 VLAN7 | | | | | | | | | 0 0 🗸 LAN 1 🔽

- Permit untagged device in P1 to access router
- 1. For each VLAN row, if enable is checked for the VLAN Tag then the corresponding VID will be applied to wired LAN traffic.
- 2. Wireless LAN traffic is always untagged, but will still be a member of the VLAN group selected.
- 3. Each VID must be unique.





Info

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

Item	Description
Enable	Click it to enable VLAN configuration.
LAN	P1 - P6 - Check the LAN port(s) to group them under the selected VLAN.
Wireless LAN (2.4GHz)	SSID1 - SSID4 - Check the SSID boxes to group them under the selected VLAN.
Wireless LAN (5GHz)	SSID1 - SSID4 - Check the SSID boxes to group them under the selected VLAN.
Subnet	Choose one of them to make the selected VLAN mapping to the specified subnet only. For example, LAN1 is specified for VLAN0. It means that PCs grouped under VLAN0 can get the IP address(es) that specified by the subnet.
	Subnet LAN 1 LAN 1 LAN 2 LAN 3 LAN 4 LAN 5 LAN 6

VLAN Tag	Enable - Check the box to enable the function of VLAN with tag.
	The router will add specific VLAN number to all packets on the LAN while sending them out.
	Please type the tag value and specify the priority for the packets sending by LAN.
	VID - Type the value as the VLAN ID number. The range is form 0 to 4095.
	Priority - Type the packet priority number for such VLAN. The range is from 0 to 7.
Permit untagged device in P1 to access router	It can help users to communicate with the router still even though configuring wrong VLAN tag setting. It is recommended to enable the management port (LAN 1) to ensure the data transmission is unimpeded.



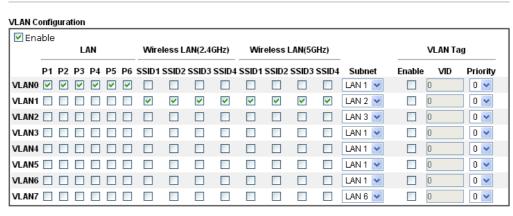
Info

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

Vigor2860 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).
- Open LAN>>VLAN Configuration. Check the boxes according to the statement in step 1 and Step 2.



- ✓ Permit untagged device in P1 to access router
- 1. For each VLAN row, if enable is checked for the VLAN Tag then the corresponding VID will be applied to wired LAN traffic.
- 2. Wireless LAN traffic is always untagged, but will still be a member of the VLAN group selected.
- 3. Each VID must be unique.

LAN >> VLAN Configuration



4. Click OK.

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

LAN >> General Setup

General Setup					
Index	Status	DHCP	IP Address		
LAN 1	V	V	172.17.11.1	Details Page	IPv6
LAN 2		✓	192.168.2.1	Details Page	IPv6
LAN 3		€	192.168.3.1	Details Page	IPv6
LAN 4		₫	192.168.4.1	Details Page	IPv6
LAN 5		€	192.168.5.1	Details Page	IPv6
LAN 6		₫	192.168.6.1	Details Page	IPv6
DMZ Port		€	192.168.7.1	Details Page	IPv6
IP Routed Subnet		€	192.168.0.1	Details Page	

Advanced You can configure DHCP server options here.

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

Inter-LAN Routing

Subnet	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5	LAN 6	DMZ Port
LAN 1	₩.						
LAN 2	•	of.					
LAN 3			4				
LAN 4				€			
LAN 5					₫		
LAN 6						₩	
DMZ Port							€

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



Info

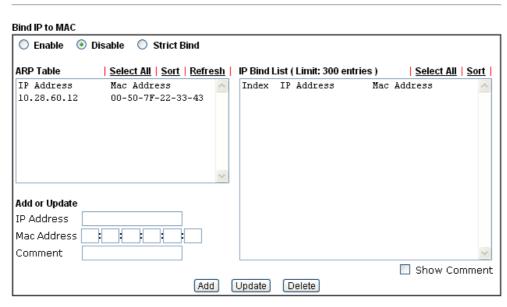
As for the VLAN applications, refer to "Appendix I: VLAN Application on Vigor Router" for more detailed information.

II-2-3 Bind IP to MAC

LAN >> Bind IP to MAC

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

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



Note: IP-MAC binding presets DHCP Allocations.

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

Backup IP Bind List : Backup	Upload From File: 選擇檔案 未選擇檔案 Restore

0K

Item	Description
Enable	Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.
Disable	Click this radio button to disable this function. All the settings on this page will be invalid.
Strict Bind	Click this radio button to block the connection of the IP/MAC which is not listed in IP Bind List.
ARP Table	This table is the LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking Add below.
Select All	Click this link to select all the items in the ARP table.
Sort	Reorder the table based on the IP address.

Refresh	Refresh the ARP table listed below to obtain the newest ARP table information.
Add or Update	IP Address - Type the IP address that will be used for the specified MAC address. Mac Address - Type the MAC address that is used to bind with the assigned IP address.
	Comment - Type a brief description for the entry.
	Show Comment - Check this box to display the comment on IP Bind List box.
IP Bind List	It displays a list for the IP bind to MAC information.
Add	It allows you to add the one you choose from the ARP table or the IP/MAC address typed in Add and Edit to the table of IP Bind List.
Update	It allows you to edit and modify the selected IP address and MAC address that you create before.
Delete	You can remove any item listed in IP Bind List. Simply click and select the one, and click Delete. The selected item will be removed from the IP Bind List.
Backup	Store the configuration for Bind IP to MAC as a file.
Restore	Restore the previously stored configuration file and apply to such page.



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:								
	Port1	Port2	Port3	Port4	Port5	Port6	WAN1	WAN2
Mirror Port		0	0	0	0	0		
Mirrored Tx Port								
Mirrored Rx Port								

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 80	02.1X				
Wired 802.1X					
LAN 802.1X:					
☑ Enable					
Authentication	Type: Extern	nal RADIUS 💌			
802.1X ports:					
□P1	□P2	□ P3	□ P4	□P5	□P6
Please note that 802.1X enabled LAN ports will support EAPOL authentication for one network device only. Therefore,802.1X enabled LAN ports will have issues when connecting to a L2 switch.If you want 802.1X support for multiple network devices, please disable 802.1X here and configure 802.1X on the connecting switch. External RADIUS supports PEAP and EAP-TLS. Please configure the User Profile if Local 802.1X is used.					
		(OK		

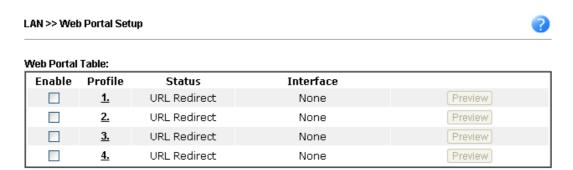
Available settings are explained as follows:

Item	Description
Enable	Check the box to enable LAN 802.1x function.
Authentication Type	Use the drop down list to choose which server (External RADIUS or Local 802.1x) will be used for authenticating LAN user.
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-2-6 Web Portal Setup

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



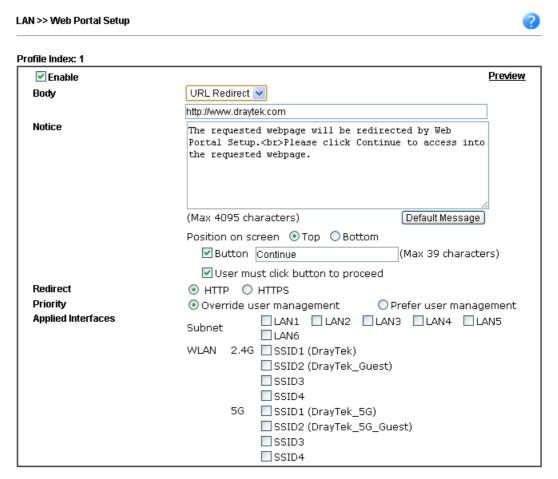
Note: The router must connect to the Internet before webpage redirection will work.



Each item is explained as follows:

Item	Description
Enable	Check the box to enable the selected profile.
Profile	Display the number link which allows you to configure the profile.
Status	Display the content (Disable, URL Redirect or Message) of the profile.
Interface	Display the applied interface of the profile.
Preview	Open a preview window according to the configured settings.

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



Note: 1. URL Redirect may fail to display some web sites because of their protection for phishing attack. Please click the "Preview" icon to test.

HTTPS Redirect will normally generate an untrusted certificate warning to web browsers, the user would need to ignore this warning to successfully display the web portal.



Item	Description	
Enable	Check the box to enable this function.	
Body	Two types can be specified for web portal setup. URL Redirect - Any user who wants to access into Internet through this router will be redirected to the URL specified here first. It is a useful method for the purpose of advertisement. For example, force the wireless user(s) in hotel to access into the web page that the hotel wants the user(s) to visit. Message - Type words or sentences here. The message will be displayed on the screen for several seconds when the wireless	
	 users access into the web page through the router. Default Message - Click it to restore the default content. 	
Notice	Content given in this field will be displayed on the screen when a web page is redirected by web portal mechanism. Position on Screen - The content of notice and the defined button can be shown upside (Top) or downside (Bottom) the text defined for message body.	

	 Button - Define the word (default word is "Continue") shown on the button. User must click button to proceed - Check the box to force the user click the button (with the word defined on Button box) to proceed the operation.
Redirect	Choose the protocol (HTTP or HTTPS) that corresponding web pages based on that protocol will be redirected.
Priority	If User Management (refer to VII-3 User Management) mode and such web portal profile are configured and enabled for filtering users, you have to determine which one shall have the highest priority. Override user management - Web portal profile will be used to filter users first. Prefer user management - User Management profile will be used to filter users first.
Applied Interfaces	Check the box(es) representing different interfaces to be applied by such profile. The advantage is that each SSID (1/2/3/4) for wireless network can be applied with different web portal separately.

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

II-3 NAT

Usually, the router serves as an NAT (Network Address Translation) router. NAT is a mechanism that one or more private IP addresses can be mapped into a single public one. Public IP address is usually assigned by your ISP, for which you may get charged. Private IP addresses are recognized only among internal hosts.

When the outgoing packets destined to some public server on the Internet reach the NAT router, the router will change its source address into the public IP address of the router, select the available public port, and then forward it. At the same time, the router shall list an entry in a table to memorize this address/port-mapping relationship. When the public server response, the incoming traffic, of course, is destined to the router's public IP address and the router will do the inversion based on its table. Therefore, the internal host can communicate with external host smoothly.

The benefit of the NAT includes:

- Save cost on applying public IP address and apply efficient usage of IP address. NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.
- Enhance security of the internal network by obscuring the IP address. There are many attacks aiming victims based on the IP address. Since the attacker cannot be aware of any private IP addresses, the NAT function can protect the internal network.



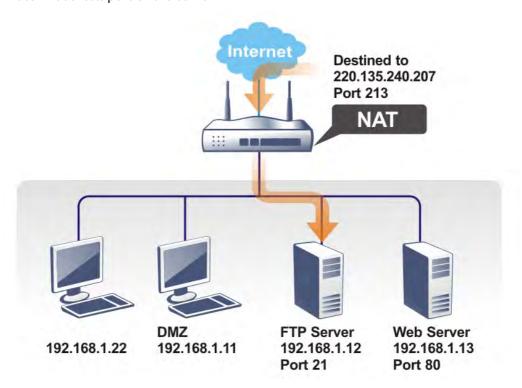
Info

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-3-1 Port Redirection

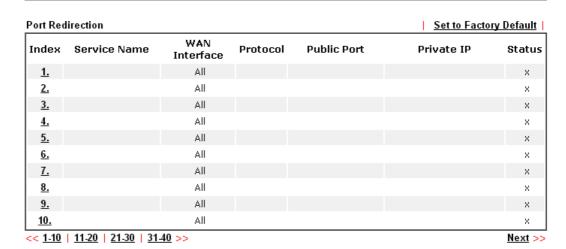
Port Redirection is usually set up for server related service inside the local network (LAN), such as web servers, FTP servers, E-mail servers etc. Most of the case, you need a public IP address for each server and this public IP address/domain name are recognized by all users. Since the server is actually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



The port redirection can only apply to incoming traffic.

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

NAT >> Port Redirection



Note: The configured ports in the $\underline{\text{Management}}$ and $\underline{\text{SSL VPN}}$ webUIs will be used by the router and not be sent to the local computer defined here.

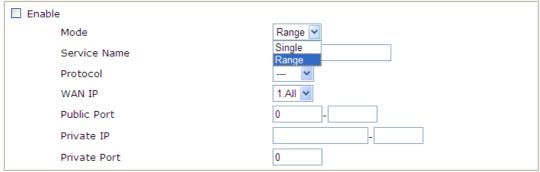
Each item is explained as follows:

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

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

NAT >> Port Redirection

Index No. 1



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



Item	Description
Enable	Check this box to enable such port redirection setting.
Mode	Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select Range. In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered, the system will calculate and display the ending IP of private IP automatically.
Service Name	Enter the description of the specific network service.
Protocol	Select the transport layer protocol (TCP or UDP).
WAN IP	Select the WAN IP used for port redirection. There are eight WAN IP alias that can be selected and used for port redirection. The default setting is AII 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. Type the required number on the first box (as the starting port) and the second box (as the ending port).
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.

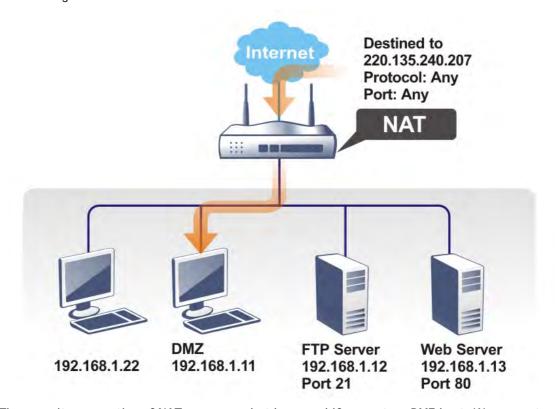
For example, the built-in web user interface in the router is with default port 80, which may conflict with the web server in the local network, http://192.168.1.13:80. Therefore, you need to change the router's http port to any one other than the default port 80 to avoid conflict, such as 8080. This 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.



IPv4 Management Setup	IPv6 Management Setup	
Router Name DrayTek		
Default:Disable Auto-Logout Enable Validation Code in Internet/l Access Note: IE8 and below version does NOT	Telnet Port 23 (Default: 23)	
support DrayOS CAPTCHA auth code.	HTTP Port 80 (Default: 80) HTTPS Port 443 (Default: 443)	
Internet Access Control Allow management from the Internet Domain name allowed	FTP Port 21 (Default: 21) TR069 Port 8069 (Default: 8069) SSH Port 22 (Default: 22)	
□ FTP Server☑ HTTP Server☑ HTTPS Server	TLS/SSL Encryption Setup Enable SSL 3.0	
 ✓ Telnet Server ✓ TR069 Server □ SSH Server □ Disable PING from the Internet 	CVM Access Control CVM Port CVM SSL Port R443 CVM SSL Port	
LAN Access Control Allow management from LAN FTP Server HTTP Server HTTPS Server	Respond to external device Respond to external device	

II-3-2 DMZ Host

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

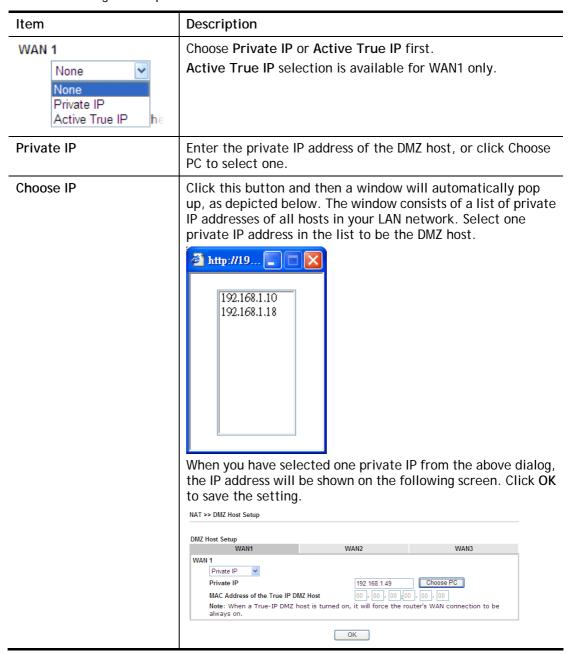


The security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

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



Available settings are explained as follows:



DMZ Host for WAN2, WAN3, LTE or WAN4 is slightly different with WAN1. Active True IP selection is available for WAN1 only.

See the following figure.





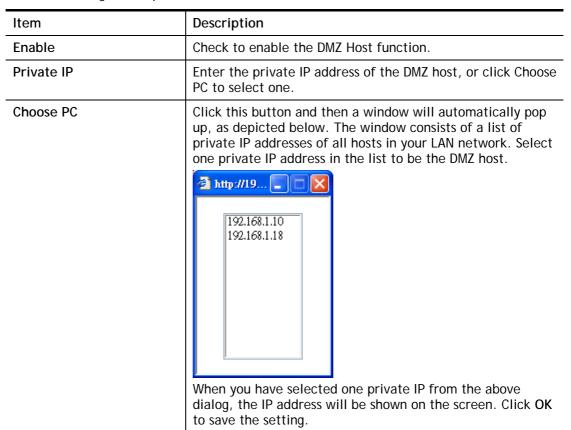
If you previously have set up WAN Alias for PPPoE or Static or Dynamic IP mode in WAN2 interface, you will find them in Aux. WAN IP for your selection.

NAT >> DMZ Host Setup DMZ Host Setup WAN1 WAN2 WAN3 WAN4 WAN 2 Enable Aux. WAN IP Private IP Index 0.0.0.0 Choose IP 1. 10.39.0.10 10.39.0.150 0.0.0.0 Choose IP 2.

Clear

OΚ

Available settings are explained as follows:



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

II-3-3 Open Ports

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

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

Click Open Ports to open the following page:

NAT >> Open Ports

Open Ports Se	etup		Set to Fa	ctory Default
Index	Comment	WAN Interface	Local IP Address	Status
<u>1.</u>				×
<u>2.</u>				×
<u>3.</u>				×
4.				×
<u>5.</u>				×
<u>6.</u>				×
<u>7.</u>				×
<u>8.</u>				×
<u>9.</u>				X
<u>10.</u>				×
<< <u>1-10 11-</u>	20 21-30 31-40 >>			Next >>

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

Available settings are explained as follows:

Item	Description
Index	Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.
Comment	Specify the name for the defined network service.
WAN Interface	Display the WAN interface used by such index.
Aux. WAN IP	Display the IP alias setting used by such index. If no IP alias setting exists, such field will not appear.
Local IP Address	Display the private IP address of the local host offering the service.
Status	Display the state for the corresponding entry. X or V is to represent the Inactive or Active state.

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

Index No. 10 ☑ Enable Open Ports Comment WAN Interface WAN1 💌 Private IP Choose IP End Port End Port Protocol Start Port Protocol Start Port 0 0 1. 2. 3. 0 0 4. v 0 -----5. -----0 0 6. v 0 0 ٧ 7. 0 0 0 0 8. 0 9. 0 10. 0 0

Clear

Cancel

Available settings are explained as follows:

ΟK

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.	
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 \mathbf{OK} to save the configuration.

NAT >> Open Ports

Open Ports Setup Set to Factor		ctory Default		
Index	Comment	WAN Interface	Local IP Address	Status
<u>1.</u>	P2261	WAN1	192.168.1.49	V
<u>2.</u>				х
<u>3.</u>				х
<u>4.</u>				х
<u>5.</u>				X
<u>6.</u>				Х
<u>7.</u>				X

II-3-4 Port Triggering

Port Triggering is a variation of open ports function.

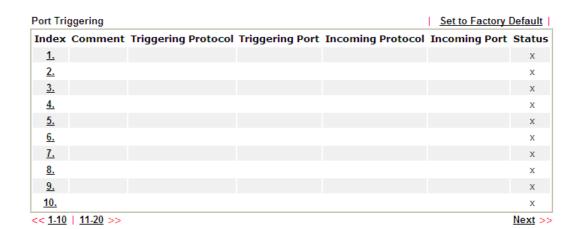
The key difference between "open port" and "port triggering" is:

- 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



Available settings are explained as follows:

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

Click the index number link to open the configuration page.

No. 1 ✓ Enable User Defined 🕶 Service Comment Triggering Protocol TCP 80 Triggering Port Incoming Protocol UDP Incoming Port 1024 $\begin{tabular}{ll} \textbf{Note:} The Triggering Port and Incoming Port should be input like this: $123-456,777-789 (legal),123-456,789 (legal), but $123-456-789 (illegal).$ \\ \end{tabular}$ OK Clear Cancel

Available settings are explained as follows:

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

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

II-4 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 Vigor2860 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.

LDAP /Active Directory Setup

Lightweight Directory Access Protocol (LDAP) is a communication protocol for using in TCP/IP network. It defines the methods to access distributing directory server by clients, work on directory and share the information in the directory by clients. The LDAP standard is established by the work team of Internet Engineering Task Force (IETF).

As the name described, LDAP is designed as an effect way to access directory service without the complexity of other directory service protocols. For LDAP is defined to perform, inquire and modify the information within the directory, and acquire the data in the directory securely, therefore users can apply LDAP to search or list the directory object, inquire or manage the active directory.

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.

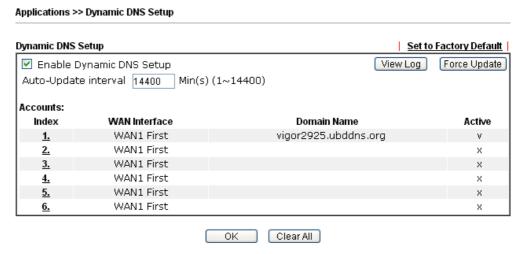
In addition, such PC must have installed a network card supporting WOL function. By the way, WOL function must be set as "Enable" on the BIOS setting.

Web User Interface

II-4-1 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. In the DDNS setup menu, check **Enable Dynamic DNS Setup**.



Available settings are explained as follows:

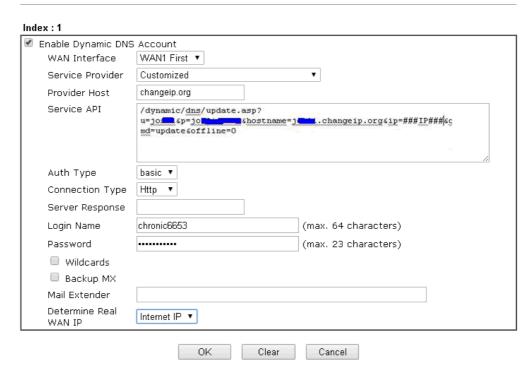
Item	Description
Enable Dynamic DNS Setup	Check this box to enable DDNS function.
Set to Factory Default	Clear all profiles and recover to factory settings.
View Log	Display DDNS log status.
Force Update	Force the router updates its information to DDNS server.
Auto-Update interval	Set the time for the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

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



If **Customized** is specified as the service provider, the web page will be changed slightly as follows:

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



Item	Description
Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
WAN Interface	WAN1/WAN2/WAN3/WAN4/LTE First - While connecting, the router will use WAN1/WAN2/WAN3/WAN4/LTE as the first channel for such account. If WAN1/WAN2/WAN3/WAN4/LTE fails, the router will use another WAN interface instead. WAN1/WAN2/WAN3/WAN4/LTE Only - While connecting, the router will use WAN1/WAN2/WAN3/WAN4/LTE as the

	only channel for such account.
Service Provider	Select the service provider for the DDNS account.
Service Type	Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field.
	Note that such option is not available when Customized is selected as Service Provider.
Domain Name	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.
	Note that such option is not available when Customized is selected as Service Provider.
Provider Host	Type the IP address or the domain name of the host which provides related service. Note that such option is available when Customized is selected as Service Provider.
Service API	Type the API information obtained from DDNS server. Note that such option is available when Customized is selected as Service Provider. (e.g:
	/dynamic/dns/update.asp?u=jo***&p=jo******&hostname=j* ***.changeip.org&ip=###IP### &cmd=update&offline=0)
Auth Type	Two types can be used for authentication.
	Basic - Username and password defined later can be shown from the packets captured.
	URL - Username and password defined later can be shown in URL. (e.g., http://ns1.vigorddns.com/ddns.php?username=xxxx&
	password=xxxx&domain=xxxx.vigorddns.com) Note that such option is available when Customized is selected as Service Provider.
Connection Type	There are two connection types (HTTP and HTTPs) to be specified. Note that such option is available when Customized is selected as Service Provider.
Server Response	Type any text that you want to receive from the DDNS server.
	Note that such option is available when Customized is selected as Service Provider.
Login Name	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.
Wildcard and Backup MX	The Wildcard and Backup MX (Mail Exchange) features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.
Mail Extender	If the mail server is defined with another name, please type the name in this area. Such mail server will be used as backup mail exchange.
Determine Real WAN IP	If a Vigor router is installed behind any NAT router, you can enable such function to locate the real WAN IP. When the WAN IP used by Vigor router is private IP, this function can detect the public IP used by the NAT router and use the detected IP address for DDNS update.

There are two methods offered for you to choose:

- 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.

Disable the Function and Clear all Dynamic DNS Accounts

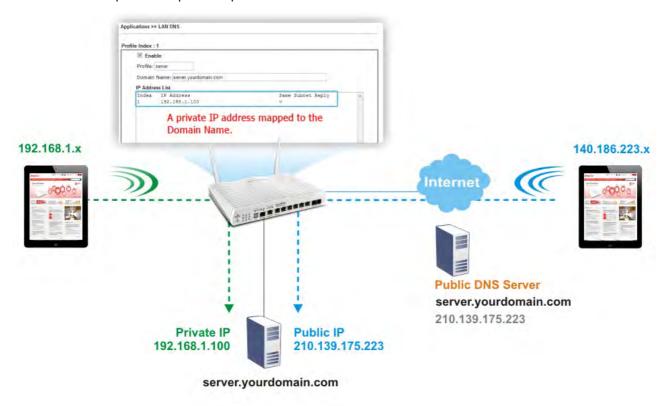
Uncheck Enable Dynamic DNS Setup, and click Clear All button to disable the function and clear all accounts from the router.

Delete a Dynamic DNS Account

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

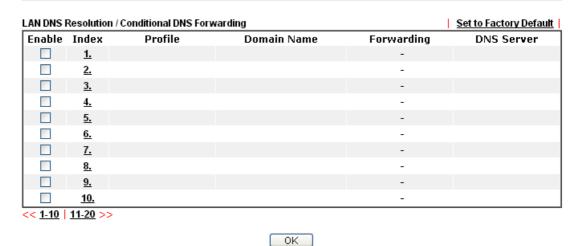
II-4-2 LAN DNS / DNS Forwarding

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 Vigor2860 series will respond the specified private IP address.



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

Applications >> LAN DNS / DNS Forwarding



Each item is explained as follows:

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

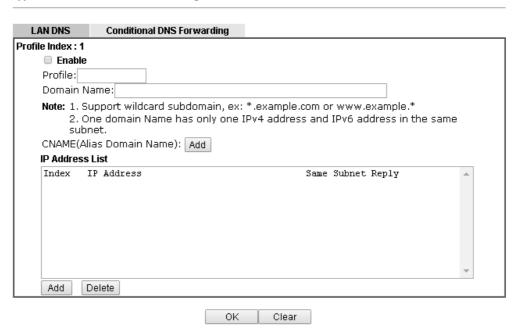
Enable	Check the box to enable the selected profile.
Index	Click the number below Index to access into the setting page.
Profile	Display the name of the LAN DNS profile.
Domain Name	Display the domain name of the LAN DNS profile.
Forwarding	Display that such profile is conditional DNS forwarding or not.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

You can set up to 20 LAN DNS profiles.

To create a LAN DNS profile:

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

Applications >> LAN DNS / DNS Forwarding



Item	Description
Enable	Check this box to enable such profile.
Profile	Type a name for such profile. Note: If you type a name here for LAN DNS and click OK to save the configuration, the name also will be applied to conditional DNS forwarding automatically.
Domain Name	Type the domain name for such profile.
IP Address List	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 type the host's IP address.



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



Item	Description
Enable	Check this box to enable such profile.
Profile	Type a name for such profile.
	Note: If you type a name here for conditional DNS forwarding and click OK to save the configuration, the name also will be applied to LAN DNS automatically.
Domain Name	Type the domain name for such profile.
DNS Server IP Address	Type the IP address of the DNS server you want to use for DNS forwarding.

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

II-4-3 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:			Set to Factory Default
Index	Status	Index	Status
<u>1.</u>	X	<u>9.</u>	x
<u>2.</u>	X	<u>10.</u>	x
<u>3.</u>	x	<u>11.</u>	x
<u>4.</u>	X	<u>12.</u>	x
<u>5.</u>	X	<u>13.</u>	x
<u>6.</u>	X	<u>14.</u>	x
<u>7.</u>	X	<u>15.</u>	x
<u>8.</u>	X		

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

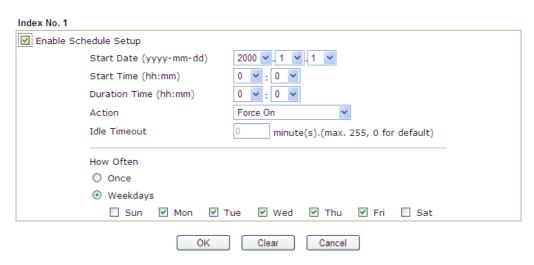
Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles and recover to factory settings.
Index	Click the number below Index to access into the setting page of schedule.
Status	Display if this schedule setting is active or inactive.

You can set up to 15 schedules. Then you can apply them to your Internet Access or VPN and Remote Access >> LAN-to-LAN settings.

To add a schedule:

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



Available settings are explained as follows:

Item	Description
Enable Schedule Setup	Check to enable the schedule.
Start Date (yyyy-mm-dd)	Specify the starting date of the schedule.
Start Time (hh:mm)	Specify the starting time of the schedule.
Duration Time (hh:mm)	Specify the duration (or period) for the schedule.
Action	Specify which action Call Schedule should apply during the period of the schedule.
	Force On -Force the connection to be always on.
	Force Down -Force the connection to be always down.
	Enable Dial-On-Demand -Specify the connection to be dial-on-demand and the value of idle timeout should be specified in Idle Timeout field.
	Disable Dial-On-Demand -Specify the connection to be up when it has traffic on the line. Once there is no traffic over idle timeout, the connection will be down and never up again during the schedule.
Idle Timeout	Specify the duration (or period) for the schedule.
	How often -Specify how often the schedule will be applied Once -The schedule will be applied just once
	Weekdays -Specify which days in one week should perform the schedule.

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).



- 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-4-4 RADIUS/TACACS+

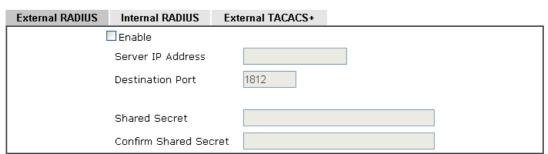
Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting, which is widely used by Internet service providers. It is the most common method of authenticating and authorizing dial-up and tunneled network users.

II-4-4-1 External RADIUS

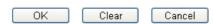
The built-in RADIUS client feature enables the router to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.

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.

Applications >> RADIUS/TACACS+



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

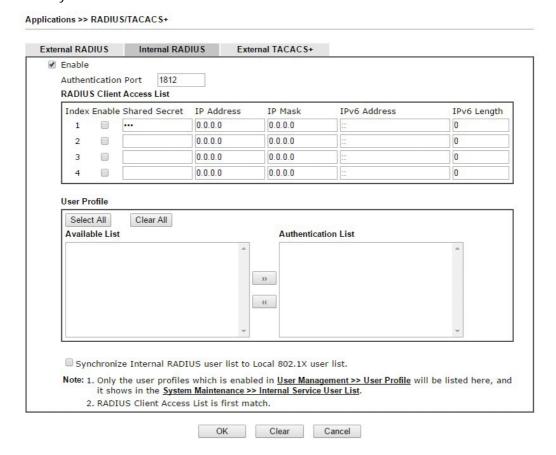


Item	Description
Enable	Check to enable RADIUS client feature.
Server IP Address	Enter the IP address of RADIUS server

Destination Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret. The maximum length of the shared secret you can set is 36 characters.
Confirm Shared Secret	Re-type the Shared Secret for confirmation.

II-4-4-2 Internal RADIUS

Except for being a built-in RADIUS client, Vigor router also can be operated as a RADIUS server which performs security authentication by itself. This page is used to configure settings for internal RADIUS server. Then LAN user of Vigor router will be authenticated by Vigor router directly.



Item	Description
Enable	Check to enable internal RADIUS client feature.
Authentication Port	Set a port number for internal RADIUS server.
RADIUS Client Access List	Allow to configure that clients under specified domain (IPv4 and IPv6) must be authenticated with the specified shared secret.
	Enable - Check to enable RADIUS client feature.
	Shared Secret - The RADIUS server and client share a secret

	that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret. The maximum length of the shared secret you can set is 36 characters.
	IP Address - Type the IP addres of the wired/wireless client.
	IP Mask - Type the subnet mask required for the IP address.
	IPv6 Address - Type the IPv6 address of the wired/wireless client.
	IPv6 Length - Type the prefix length required for the IPv6 address.
User Profile	During the process of security authentication, user account and user password will be required for identity authentication. Before configuring such page, create at least one user profile in User Management>>User Profile first.
	Select All - Click it to select all of the user profiles in Available List.
	Clear All- Click to remove all of the user profiles in Available List.
	Available List - The user profiles without RADIUS server enabled in User Management >> User Profile will be listed in this field.
	Authentication List -The user profiles with RADIUS server enabled in User Management >> User Profile will be listed in this field.
Synchronize Internal RADIUS user list to Local 802.1X user list	Users can be authenticated by RADIUS server and local 802.1X to get certain network service. It is not necessary to create new user profiles (containing user accounts and user passwords) for RADIUS and local 802.1X respectively.
	Simply check this box; all of the user profiles (prepared for RADIUS server authentication) listed in Authentication List will be synchronized for local 802.1X user authentication.

II-4-4-3 External TACACS+

It means Terminal Access Controller Access-Control System Plus. It works like RADIUS does. Click the TACACS+ Setup to open the following page:



Item	Description
Enable	Check to enable TACACS+ feature.
Server IP Address	Enter the IP address of TACACS+ server.
Destination Port	The UDP port number that the TACACS+ server is using.
Shared Secret	The TACACS+ server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Confirm Shared Secret	Re-type the Shared Secret for confirmation.

II-4-5 LDAP /Active Directory Setup

Lightweight Directory Access Protocol (LDAP) is a communication protocol for using in TCP/IP network. It defines the methods to access distributing directory server by clients, work on directory and share the information in the directory by clients. The LDAP standard is established by the work team of Internet Engineering Task Force (IETF).

As the name described, LDAP is designed as an effect way to access directory service without the complexity of other directory service protocols. For LDAP is defined to perform, inquire and modify the information within the directory, and acquire the data in the directory securely, therefore users can apply LDAP to search or list the directory object, inquire or manage the active directory.

General Setup

Applications >> Active Directory /LDAP

This page allows you to enable the function and specify general settings for LDAP server.

Active Directory /LDAP Set to Factory Default Active Directory / General Setup LDAP Profiles Enable Bind Type Simple Mode Server Address **Destination Port** 389 Use SSL Regular DN Regular Password OΚ Cancel Note: After finishing the configuration of the LDAP profiles, they will be listed in the page of VPN and Remote Access >> PPP General Setup. If you want to use the profiles for VPN authentication, check the boxes under PPTP LDAP Profiles in VPN and Remote Access >>

Available settings are explained as follows:

PPP General Setup first.

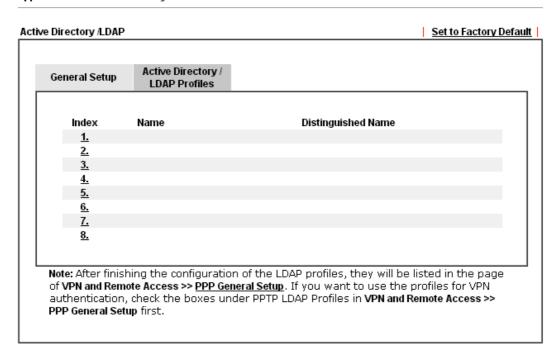
Item	Description
Enable	Check to enable such function.
Bind Type	There are three types of bind type supported.
	Simple Mode - Just simply do the bind authentication without any search action.
	 Anonymous - Perform a search action first with Anonymous account then do the bind authentication.
	 Regular Mode- Mostly it is the same with anonymous mode. The different is that, the server will firstly check if you have the search authority.
	For the regular mode, you'll need to type in the Regular DN

	and Regular Password.
Server Address	Enter the IP address of LDAP server.
Destination Port	Type a port number as the destination port for LDAP server.
Use SSL	Check the box to use the port number specified for SSL.
Regular DN	Type this setting if Regular Mode is selected as Bind Type.
Regular Password	Specify a password if Regular Mode is selected as Bind Type.

Profiles

You can configure eight AD/LDAP profiles. These profiles would be used with User Management for different purposes in management.

Applications >> Active Directory /LDAP



Click any index number link to open the following page.

Applications >> Active Directory /LDAP>>Server Profiles

Index No. 1 RD1 Name UID Common Name Identifier 9 Base Distinguished Name Additional Filter Note: Please type in your additional filter for BaseDN search request. For example, 1) For OpenLDAP: (gidNumber=500) 2) For AD: (msNPAllowDialin=TRUE) Group Distinguished Name 9 Cancel ΟK

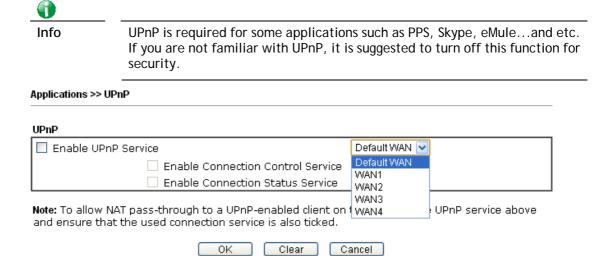
Available settings are explained as follows:

Item	Description
Name	Type a name for such profile. The length of the user name is limited to 19 characters.
Common Name Identifier	Type or edit the common name identifier for the LDAP server. The common name identifier for most LDAP server is "cn".
Additional Filter	Type the condition for additional filter.
Base Distinguished Name / Group Distinguished Name	Type or edit the distinguished name used to look up entries on the LDAP server. Sometimes, you may forget the Distinguished Name since it's too long. Then you may click the button to list all the account information on the AD/LDAP Server to assist you finish the setup.

After finished the above settings, click \mathbf{OK} to save and exit this page. A new profile has been created.

II-4-6 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.



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

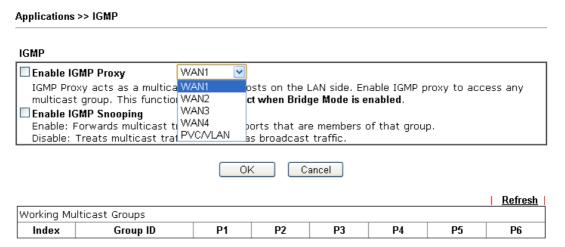
Activating the UPnP function on your network may incur some security threats. You should consider carefully these risks before activating the UPnP function.

- 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-4-7 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.



Available settings are explained as follows:

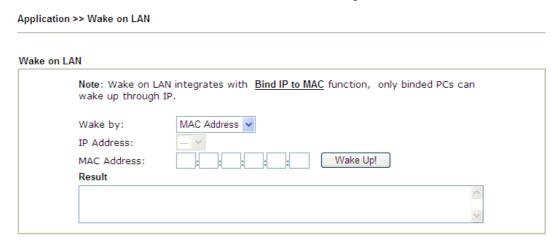
Item	Description
Enable IGMP Proxy	Check this box to enable this function. The application of multicast will be executed through WAN/LTE/PVC/VLAN port. In addition, such function is available in NAT mode.
Enable IGMP Snooping	Check this box to enable this function. Multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.
Refresh	Click this link to renew the working multicast group status.
Group ID	This field displays the ID port for the multicast group. The available range for IGMP starts from 224.0.0.0 to 239.255.255.254.
P1 to P6	It indicates the LAN port used for the multicast group.

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

II-4-8 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.



Item	Description
Wake by	 Two types provide for you to wake up the binded IP. If you choose Wake by MAC Address, you have to type the correct MAC address of the host in MAC Address boxes. If you choose Wake by IP Address, you have to choose the correct IP address.
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-4-9 SMS / Mail Alert Service

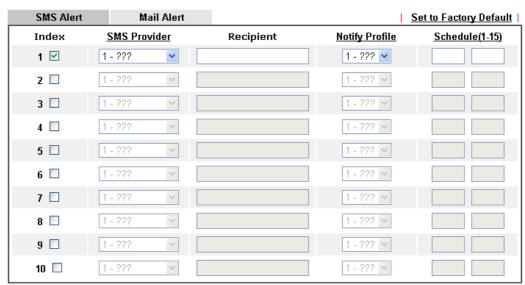
The function of SMS (Short Message Service)/Mail Alert is that Vigor router sends a message to user's mobile or e-mail box through specified service provider to assist the user knowing the real-time abnormal situations.

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

SMS Alert

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

Applications >> SMS / Mail Alert Service



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



Available settings are explained as follows:

Item	Description
Index	Check the box to enable such profile.
SMS Provider	Use the drop down list to choose SMS service provider. You can click SMS Provider link to define the SMS server.
Recipient	Type the name of the one who will receive the SMS.
Notify Profile	Use the drop down list to choose a message profile. The recipient will get the content stated in the message profile. You can click the Notify Profile link to define the content of the SMS.
Schedule (1-15)	Type the schedule number that the SMS will be sent out. You can click the Schedule(1-15) link to define the schedule.

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

Mail Alert

This page allows you to specify Mail Server profile, who will get the notification e-mail, what the content is and when the message will be sent.

Application >> SMS / Mail Alert Service

SMS Alert	Mail Alert		5	Set to Factory Default
Index	Mail Service	Recipient	Notify Profile	<u>Schedule(1-15)</u>
1 🗹	1 - ??? 💌		1 - ??? 💌	
2 🗆	1 - ??? 💌		1 - ??? 💌	
3 🗆	1 - ??? 💌		1 - ??? 💟	
4 🗆	1 - ??? 💌		1 - ??? 💌	
5 🗆	1 - ??? 💌		1 - ??? 💟	
6 🗆	1 - ??? 💌		1 - ??? 💌	
7 🗆	1 - ??? 💌		1 - ??? 💟	
8 🗆	1 - ??? 💌		1 - ??? 💌	
9 🗆	1 - ??? 💌		1 - ??? 💌	
10 🗆	1 - ??? 💌		1 - ??? 🔽	

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



Available settings are explained as follows:

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

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

II-4-10 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.

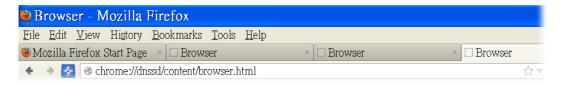
Usually, users have to configure the router or personal computers to use above services. Sometimes, the configuration (e.g., IP settings, port number) is complicated and not easy to complete. The purpose of Bonjour is to decrease the settings configuration (e.g., IP setting). If the host and user's computer 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.

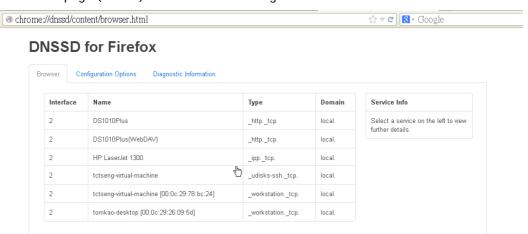


Below shows an example for applying the bonjour feature that Vigor router can be used as the FTP server.

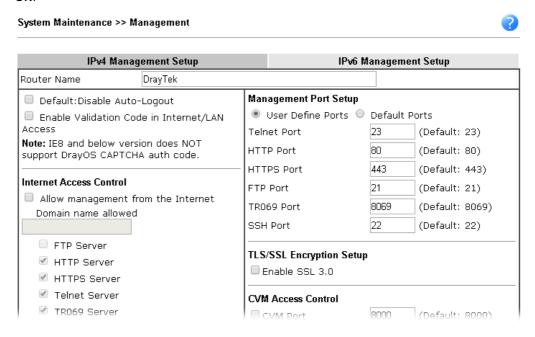
1. Here, we use Firefox and DNSSD to discover the service in such case. Therefore, just ensure the Bonjour client program and DNSSD for Firefox have been installed on the computer.



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



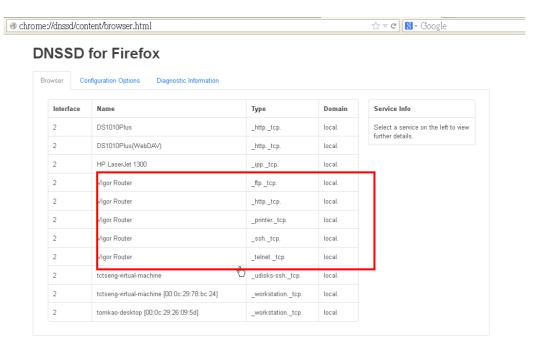
Open System Maintenance>>Management. Type a name as the Router Name and click OK.



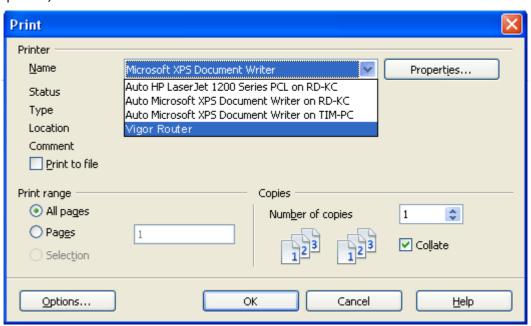
4. Next, open Applications>>Bonjour. Check the service that you want to use via Bonjour.



5. 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.



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



Application Notes

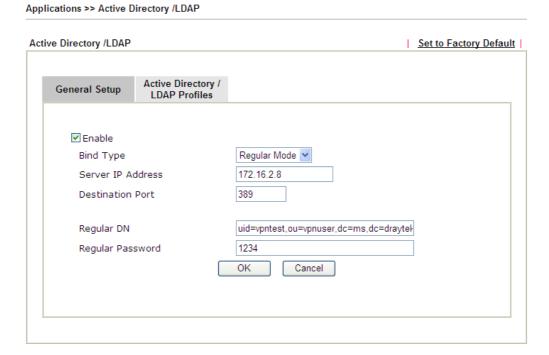
A-1 How to Implement the LDAP/AD Authentication for User Management?

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

There is no need to pre-configure user profile for each user on Vigor router anymore. We only need to configure the Groups DN, then the Vigor router (e.g., Vigor 2860 series) can pass the authentication to LDAP server with the pre-defined Group path.

Below shows the configuration steps:

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



There are three types of bind type supported:

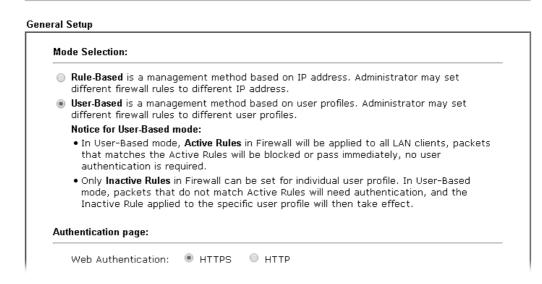
- Simple Mode Just simply do the bind authentication without any search action.
- Anonymous Perform a search action first with Anonymous account then do the bind authentication.
- Regular Mode- Mostly it is the same with anonymous mode. The different is that, the server will firstly check if you have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

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

Index No. 1 rd1 Name Common Name Identifier uid Base Distinguished Name ou=people,dc=ms,dc=draytek,dc=com Group Distinguished Name cn=rd1,ou=group,dc=ms,dc=draytek,dc=c OK Cancel and Applications >> Active Directory /LDAP>> Server Profiles Index No. 2 shrd uid Common Name Identifier Base Distinguished Name ou=people,dc=ms,dc=draytek,dc=com Group Distinguished Name cn=shrd,ou=group,dc=ms,dc=draytek,dc= OK Cancel

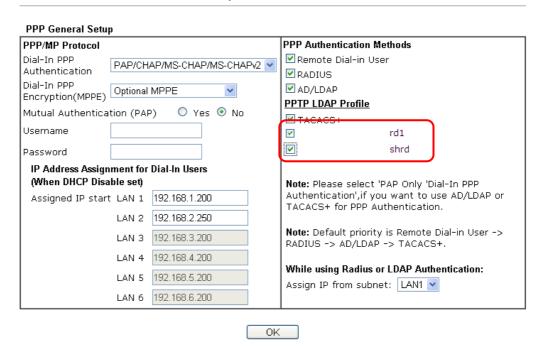
- 4. Click **OK** to save the settings above.
- 5. Open User Management>>General Setup. Select User-Based as the Mode option.

User Management >> General Setup



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

VPN and Remote Access >> PPP General Setup

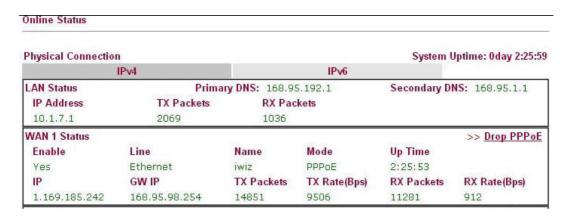


After above configurations, users belong to either "rd1" or "shrd" group can access Internet after inputting their credentials on LDAP server.

A-2 How to Configure Customized DDNS?

This article describes how to configure customized DDNS on Vigor routers to update your IP to the DDNS server. We will take "Changeip.org" and "3322.net" as example. Before setting, please make sure that the WAN connection is up.

Part A: Changeip.org



Note that,

Username: jo***
Password: jo********

Host name: j*****.changeip.org WAN IP address: 1.169.185.242

Following is the screenshot of editing the HTML script on the browser to update your IP to the DDNS server.



Now we have to configure the router so it can do the same job for us automatically.

Please go to Applications >> Dynamic DNS to create a profile for Customized DDNS client.

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

1 = 11 = 1 = 1		
Enable Dynamic DNS		
WAN Interface	WAN1 First ▼	
Service Provider	Customized	▼
Provider Host	changeip.org	
Service API	/dynamic/dns/update.asp? u=jo to	e=j==###IP###sc
Auth Type	basic ▼	
Connection Type	Http ▼	
Server Response		
Login Name	chronic6653	(max. 64 characters)
Password		(max. 23 characters)
Wildcards		
Backup MX		
Mail Extender		
Determine Real WAN IP	Internet IP ▼	

- 2. Set the Service Provider as Customized.
- 3. Set the Service API as: /dynamic/dns/update.asp?u=jo***&p=jo******&hostname=j****.changeip.org&ip=###IP ### &cmd=update&offline=0

In which, ###IP### is a value which will be replaced with the current interface IP address automatically when DDNS service is running. In this case the IP will be 1.169.185.242.

4. After setting, the Customized DDNS service will be up, and our IP will be updated to the DDNS server.

Part B: 3322.net

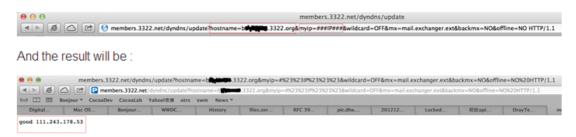
	WAN 1
Link Status	: Connected
MAC Address	: 00-50-7F-C8-C6-A1
Connection	: PPPoE
IP Address	: 111.243.178.53
Default Gateway	: 168.95.98.254
Primary DNS	: 168.95.192.1
Secondary DNS	: 168.95.1.1

Username: bi******
Password: 88********

Host name: bi*****.3322.org

WAN IP address: 111.243.178.53

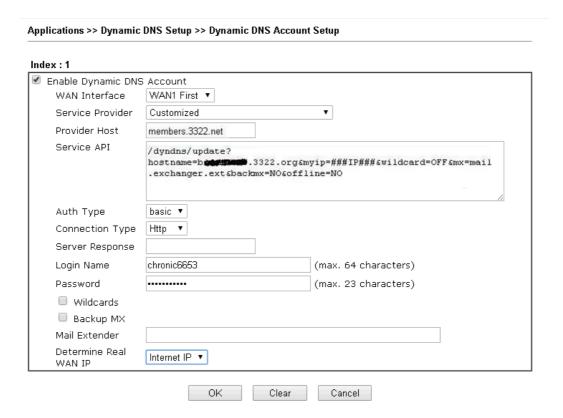
To update the IP to the DDNS server via editing the HTML script, we can type the following script on the browser:



"good 111.243.178.53" means our IP has been updated to the server successfully.

Now we have to configure the router so it can do the same job for us automatically.

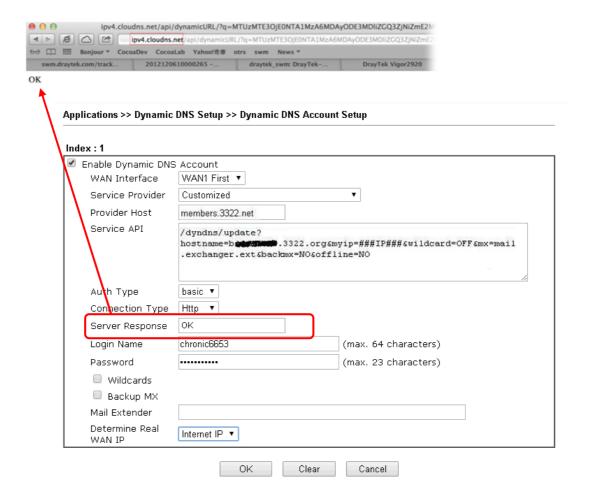
 Please go to Applications >> Dynamic DNS to create a profile for Customized DDNS client.



- 2. Set the Service Provider as Customized.
- 3. Set the Provider Host as member.3322.net.
- 4. Set the Service API as: /dyndns/update?hostname=yourhost.3322.org&myip=###IP###&wildcard=OFF&mx=mail .exchanger.ext&backmx=NO&offline=NO
- 5. Enter your account and password.
- 6. After the setting, the Customized DDNS service will be up, and our IP will be updated to the DDNS server automatically.

Part C: Extend Note

The customized Service Provider is also eligible with the ClouDNS.net.



II-5 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 >>FAQ/Application Notes on www.draytek.com.

Web User Interface

II-5-1 Static Route

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

Static Route for IPv4

LAN >> Static Route Setup

IPv4	IPv6		Se	t to Factory Default View Ro	outing Table
Index	Destination Address	Status	Index	Destination Address	Status
<u>1.</u>	???	?	<u>6.</u>	???	?
<u>2.</u>	???	?	<u>7.</u>	???	?
<u>3.</u>	???	?	<u>8.</u>	???	?
<u>4.</u>	???	?	<u>9.</u>	???	?
<u>5.</u>	???	?	<u>10.</u>	???	?
cc 1.10 11.2	N 21.30 >>				Next >>

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

Available settings are explained as follows:

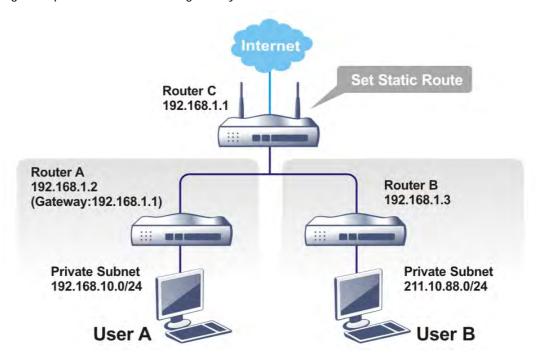
Item	Description		
Index	The number (1 to 30) under Index allows you to open next page to set up static route.		
Destination Address	Displays the destination address of the static route.		
Status	Displays the status of the static route.		
Set to Factory Default	Clear all of the settings and return to factory default settings.		
Viewing Routing Table	Diagnostics >> View Routing Table Current Running Routing Table Rey: C - connected, S - static, R - RIP, * - default, ~ - private C~ 192.168.1.0/ 255.255.255.0 directly connected LAN1		

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.



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.

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

Index No. 1 Enable Destination IP Address Subnet Mask Gateway IP Address Network Interface Note: WAN5, WAN6, WAN7 are router-borne WANs. OK Cancel Delete

Available settings are explained as follows:

LAN >> Static Route Setup

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

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

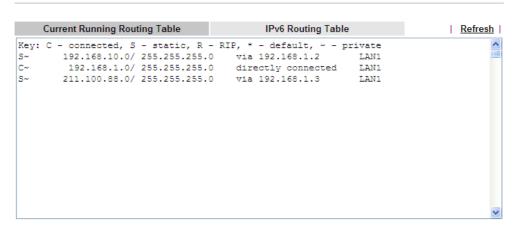
Index No. 1 Enable Destination IP Address Subnet Mask Subnet Mask Gateway IP Address 192.168.1.3 Network Interface Note: WAN5, WAN6, WAN7 are router-borne WANs.

[Delete]

OK Cancel

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

Diagnostics >> View Routing Table



Static Route for IPv6

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

LAN >> Static Route Setup

IPv4		IPv6		Set to Fa	actory Default View IPv6 Ro	uting Table
Index	Destinat	ion Address	Status	Index	Destination Address	Status
<u>1.</u>		::/0	X	<u>11.</u>	::/0	x
<u>2.</u>		::/0	X	<u>12.</u>	::/0	X
<u>3.</u>		::/0	X	<u>13.</u>	::/0	X
<u>4.</u>		::/0	X	<u>14.</u>	::/0	X
<u>5.</u>		::/0	X	<u>15.</u>	::/0	x
<u>6.</u>		::/0	X	<u>16.</u>	::/0	X
<u>7.</u>		::/0	X	<u>17.</u>	::/0	x
<u>8.</u>		::/0	X	<u>18.</u>	::/0	x
<u>9.</u>		::/0	X	<u>19.</u>	::/0	x
<u>10.</u>		::/0	X	<u>20.</u>	::/0	x
<< 1 - 20 21	1 - 40 >>					Next >>

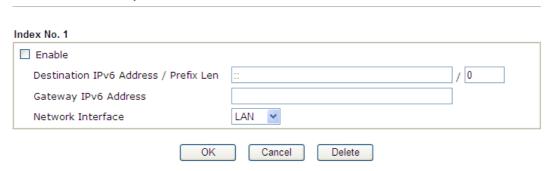
Status: v --- Active, x --- Inactive, ? --- Empty

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.
Destination Address	Displays the destination address of the static route.
Status	Displays the status of the static route.
Set to Factory Default	Clear all of the settings and return to factory default settings.
Viewing IPv6 Routing Table	Displays the routing table for your reference.

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

LAN >> Static Route Setup



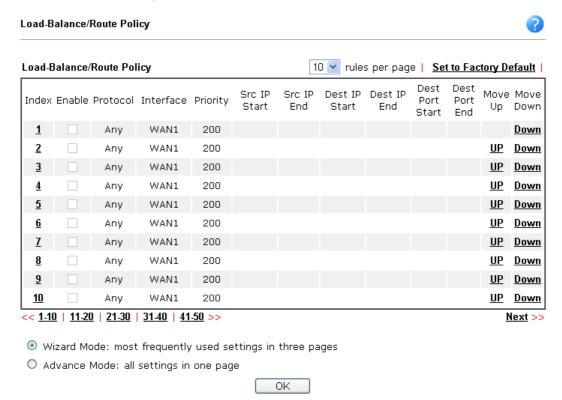
Available settings are explained as follows:

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

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

II-5-2 Load-Balance /Route Policy

II-5-2-1 General Setup



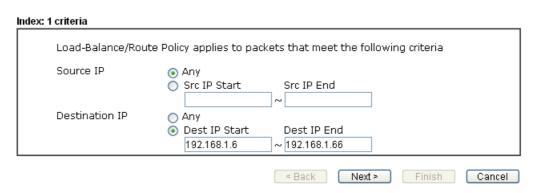
Available settings are explained as follows:

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	Display the IP address for the start of the source IP.
Src IP End	Display the IP address for the end of the source IP.
Dest IP Start	Display the IP address for the start of the destination IP.
Dest IP End	Display the IP address for the end of the destination IP.
Dest Port Start	Display the IP address for the start of the destination port.
Dest Port End	Display 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	Allow to configure frequently used settings of route policy via three setting pages
Advance Mode	Allow to configure detailed settings of route policy.

To use Wizard Mode, simple do the following steps:

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

Load-Balance/Route Policy

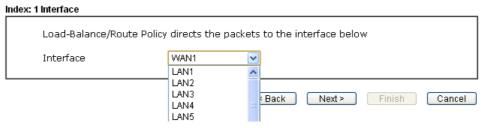


Available settings are explained as follows:

Item	Description	
Source IP	Any - Any IP can be treated as the source IP.	
	Src IP Start - Type the source IP start for the specified WAN interface.	
	Src IP End - Type the source IP end for the specified WAN interface. If this field is blank, it means that all the source IPs inside the LAN will be passed through the WAN interface.	
Destination IP	Any - Any IP can be treated as the destination IP. Dest IP Start- Type the destination IP start for the specified	
	WAN interface.	
	Dest IP End - Type the destination IP end for the specified WAN interface. If this field is blank, it means that all the destination IPs will be passed through the WAN interface.	

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

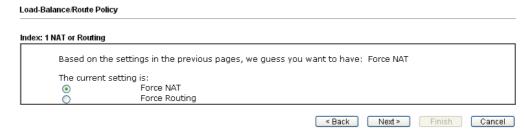
Load-Balance/Route Policy



Available settings are explained as follows:

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

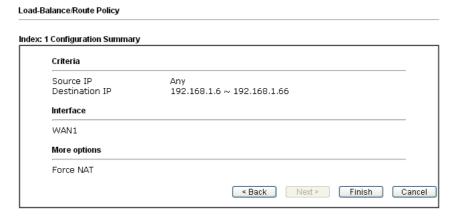
4. After specifying the interface, click **Next** to get the following page.



Available settings are explained as follows:

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

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

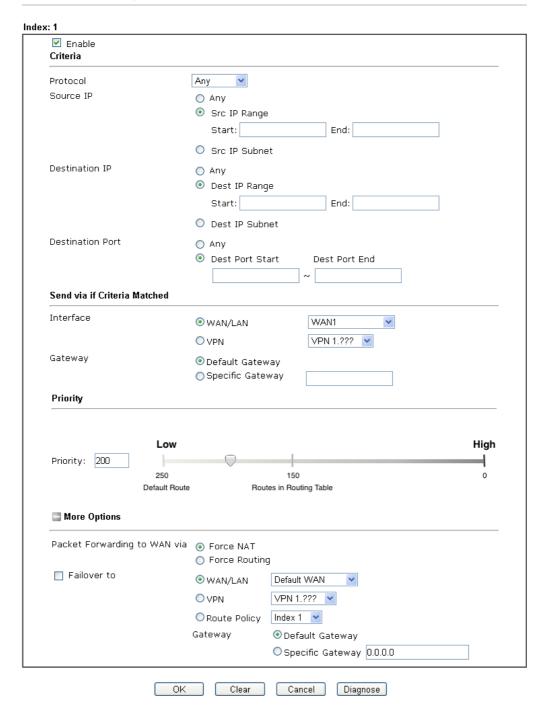


6. If there is no error, click Finish to complete wizard setting.

To use Advance Mode, do the following steps:

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

Load-Balance/Route Policy



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

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable this policy.

Protocol	Use the drop-down menu to choose a proper protocol for the WAN interface.			
	any			
	TCP			
	UDP			
	ICMP			
Source IP	Any - Any IP can be treated as the source IP.			
	Src IP Range - Define a range of IP address as source IP addresses.			
	 Start - Type an address as the starting IP for such profile. 			
	• End - Type an address as the ending IP for such profile.			
	Src IP Subnet - Define a subnet containing IP address and mask address.			
	Network - Type an IP address here.			
	 Mask - Use the drop down list to choose a suitable mask for the network. 			
Destination IP	Any - Any IP can be treated as the destination IP.			
	Dest IP Range - Define a range of IP address as destination IP addresses.			
	 Start - Type an address as the starting IP for such profile. 			
	 End - Type an address as the ending IP for such profile 			
	Dest IP Subnet - Define a subnet containing IP address a mask address.			
	Network - Type an IP address here.			
	 Mask - Use the drop down list to choose a suitable mask for the network. 			
Destination Port	Any - Any port number can be treated as the destination			
	port. Dest Port Start - Type the destination port start for the destination IP.			
	Dest Port End - Type the destination port end for the			
	destination IP. If this field is blank, it means that all the destination ports will be passed through the WAN interface.			
Send to if criteria matched	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.			
	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	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.			
	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.			

More options

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.

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.

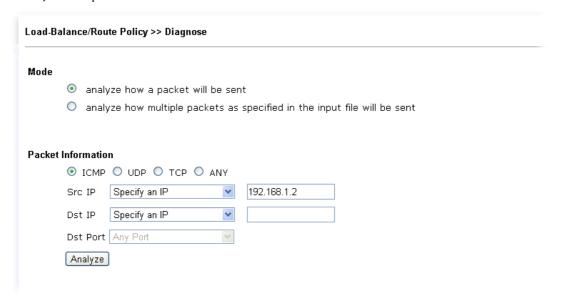
- WAN/LAN Use the drop down list to choose an interface as an auto failover interface.
- VPN Use the drop down list to choose a VPN tunnel as a failover tunnel.
- Route Policy Use the drop down list to choose an existed route policy profile.

Gateway IP - Specific gateway is used only when you want to forward the packets to the desired gateway. Usually, Default Gateway is selected in default.

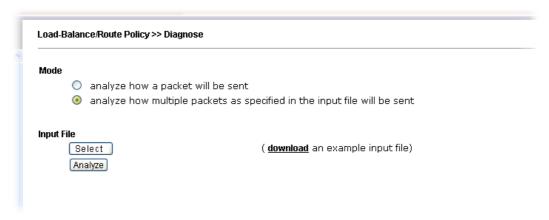
3. When you finish the configuration, please click **OK** to save and exit this page.

II-5-2-2 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.



or



Available settings are explained as follows:

Item	Description				
Mode	Analyze how a packet will be sent - Choose such mode to make Vigor router analyze how a single packet will be sen by a route policy.				
	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.				
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. If required, clic				
	export analysis to export the result as a file.				
Input File	Select - Click the download link to get a blank example				
	file. Then, click such button to select that blank ".csv" fi for saving the result of analysis.				
	Mode				
	analyze how a packet will be sent				
	● ana 下載工作確認 ×				
	Input File diagnose_example_input_file.csv				
	選擇檔案 402 B				
	402 B				
	Analyze 402 B				
	Analyze 儲存至 下載 ▼				
	Analyze 儲存至 下載 下載後開啓 協存 取消				
	Analyze 儲存至 下載 下載後開图 Analyze - Click it to perform the job of analyzing. The				
	Analyze 儲存至 下載 下載後開啓 協存 取消				
	Analyze 儲存至 下載 下載後開图 Analyze - Click it to perform the job of analyzing. The analyzed result will be shown on the page. If required, click				
	Analyze 儲存至 下載 下載後開啓 「本談集階を 「「本談集階を 「本」 Analyze - Click it to perform the job of analyzing. The analyzed result will be shown on the page. If required, clice export analysis to export the result as a file.				
	Analyze				
	Analyze				
	Analyze - Click it to perform the job of analyzing. The analyzed result will be shown on the page. If required, clice export analysis to export the result as a file. Load Balance Route Policy >> Diagnose Mode onalyze how a packet will be sent onalyze how multiple packets as specified in the input file will be sent imput file imput fil				
	Analyze - Click it to perform the job of analyzing. The analyzed result will be shown on the page. If required, clice 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 biput File RESEX + All PREX (download an example input file) Analyzis Analyzis Analyzis Analyzis File Matched Boute Proofice Proof Sec 19 Ost 19 Ost 19 Ost Bort Boute Proofice Proof Sec 19 Ost 19 Ost 19 Ost Bort Boute File Matched Boute				
	Analyze - Click it to perform the job of analyzing. The analyzed result will be shown on the page. If required, clice 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 multiple packet information Register Route Policy Route Register Route				
	Analyze - Click it to perform the job of analyzing. The analyzed result will be shown on the page. If required, clic export analysis to export the result as a file. Loud Balance Poute Policy>> Diagnose Mode O analyze how a packet will be sent O analyze how multiple packets as specified in the input file will be sent. Input File Regul File Analysis (devendoad an example input file) Analysis Perfile Profu Sec IP Dist IP Dist IP Dist Dist Bort Bouts Perfile Profu Sec IP Dist IP Dist IP Dist Dist Bort Bouts No Analysis No A				
	Analyze - Click it to perform the job of analyzing. The analyzed result will be shown on the page. If required, clic export analysis to export the result as a file. Load Balance Route Policy >> Diagnose Mode O analyze how a packet will be sent O analyze how multiple packets as specified in the input file will be sent Input File Input File Registry (desentional an example input file) Profile Proto Ser IP Det 10 10 10 10 10 10 10 10 11 10 1				

Application Notes

A-1 How to Customize a Secure Route between VPN Router and Remote Router by Using Route Policy



Info

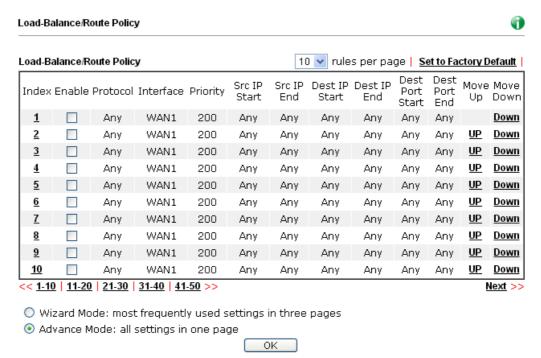
The web user interface will be revised later.

Example 1:

In the following figure, a LAN to LAN VPN tunnel is built between DrayTek VPN router (e.g., Vigor2860 series) and the remote router. Firewall Router can receive all of the traffic coming from remote PC which wants to access into Internet; and send back the packets to Remote Router through VPN Router.

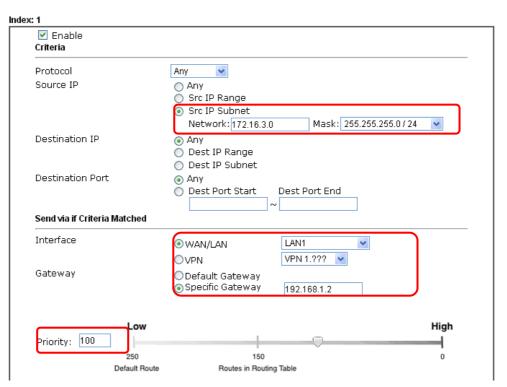


- 1. Establish a VPN tunnel between VPN Router and the Remote Router.
- 2. Change to default route for the router located in Remote Router.
- 3. Access into the web user interface of the router in VPN Router. Then, open Load-Balance / Route Policy>>General Setup and click Advance Mode.



4. Click any Index number link (e.g., 1 in this case). Configure the settings as follows.

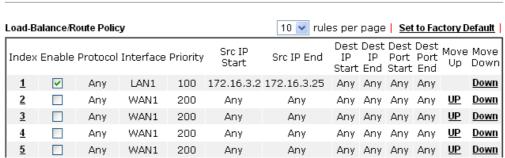
Load-Balance/Route Policy



Now, if you want such route policy will be applied by Vigor router with higher priority, please adjust the value of **Priority** for such route policy. In general, default route is specified with the lowest priority for it value is fixed as "250". And Routes in Routing Table are fixed as "150". You can adjust the value for such route policy with lower value, e.g., 100 to ensure it will be applied to packets transmission with the highest priority.

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

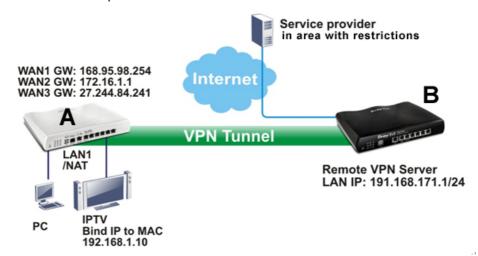




6. To route the packets coming from the Firewall Router back to the remote router, access into the web user interface of the Firewall Router. Then, set "192.168.1.1/24" as the gateway IP address and set "172.16.3.0/24" as the destination IP address.

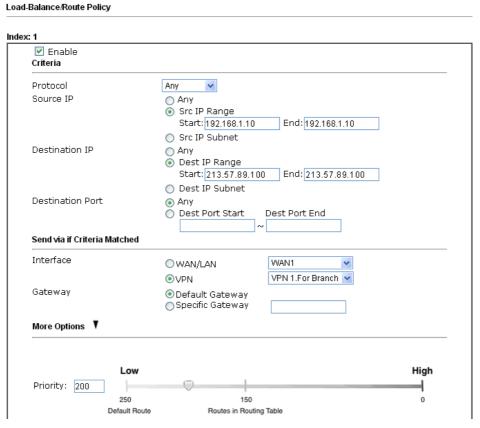
Example 2:

Below shows a scenario that local users behind Vigor router A want to access into a remote service (e.g., YouTube) which is blocked or restricted by local Service Provider in area with restrictions. A policy route can be created by the side of Router A to break through the Internet censorship circumvention.



A VPN tunnel has been established between Router A and router B.

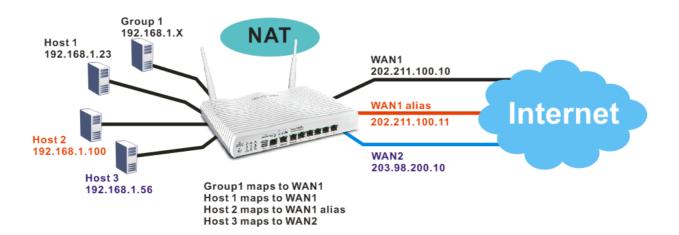
- 1. Access into the web user interface of Router A.
- 2. Open Load-Balance/Route Policy>>General Setup.
- 3. Click any index number (e.g., #1 in this case).
- 4. In the following web page, check Enable; type "192.168.1.10" as Src IP Range; type "213.57.89.100" as the Destination IP for the remote VPN server; and choose VPN as the Interface setting.



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

A-2 How to Setup Address Mapping

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



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

WAN1: 202.211.100.10, WAN1 alias: 202.211.100.11

WAN2: 203.98.200.10

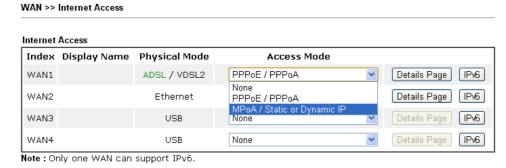
Without address mapping feature, when a NAT host with an IP say "192.168.1.10" sends a packet to the WAN side (or the Internet), the source address of the NAT host will be mapped into either 202.211.100.10 or 203.98.200.10 (which IP or mapping is decided by the internal load balancing algorithm).

With address mapping feature, you can manually configure any host mapping to any WAN interface to fit the request. In the above example, you can configure NAT Host 1 to always map to 202.211.100.10 (WAN1); Host 2 to always map to 202.211.100.11 (WAN1 alias); Hostd 3 always map to 203.98.200.10 (WAN2) and Group 1 to always map to 202.211.100.10 (WAN1).

NAT Address Mapping function lets you specify the outgoing IP address(es) for one internal IP address or a block of internal IP addresses.

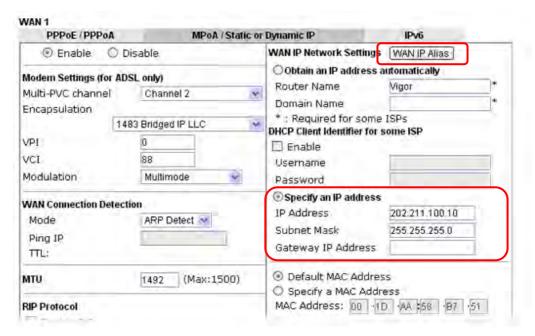
We will take an example to introduce how to make use of this feature.

- 1. Log into the web user interface of Vigor2860.
- Open WAN>>Internet Access. For WAN1, choose MPoA/Static or Dynamic IP as the Access Mode.



Advanced You can configure DHCP client options here.

3. Click the **Details Page** of WAN 1 to open the following page. From the above figure, set main WAN IP address as *202.211.100.10*.



Click the WAN IP Alias button to configure the other IP address which is 202.211.100.11. Make sure Join IP NAT Pool is not checked. Click OK to save the settings.

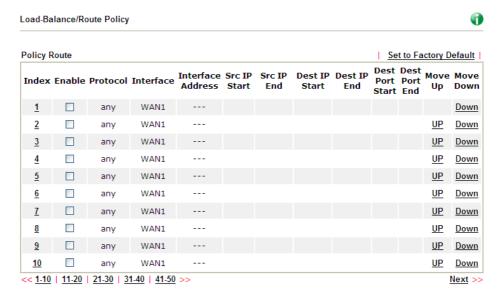
WAN1 IP Alias (Multi-NAT) Index Enable Aux. WAN IP Join NAT IP Pool 1. 202.211.100.10 V 2. V 202.211.100.11 3. 0.0.0.0 4. 0.0.0.0 5. 0.0.0.0 6. 0.0.0.0 7. 0.0.0.0 0.0.0.0 8.

Clear All

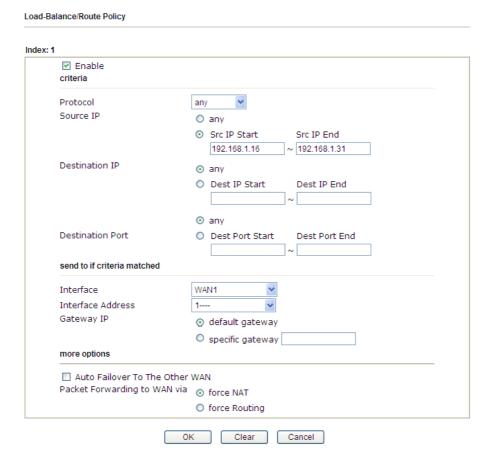
Close

OK

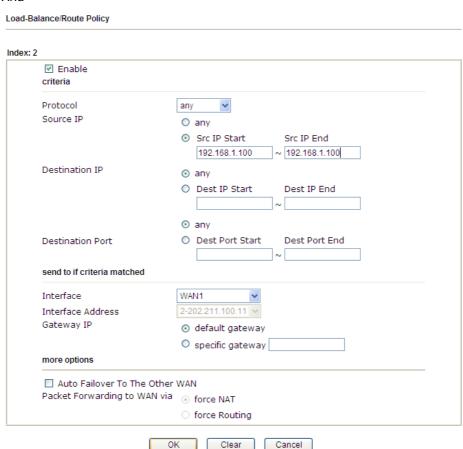
4. After finished configuration for WAN1, open Load-Balance/Route Policy>>General Setup. Choose Advance Mode.



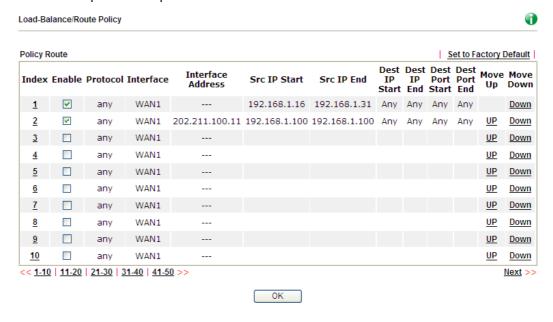
5. Click Index number 1 and 2 to configure the details. After finished the settings, click **OK** to save the settings respectively.



And



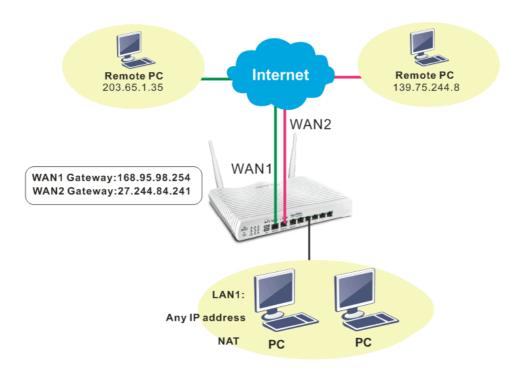
6. Upon completing the above configuration, you have specified the outgoing IP address(es) for some specific computers.



Now, you bind some specific computers to some WAN IP alias for outgoing traffic.

A-3 How to setup Load Balance for Packets?

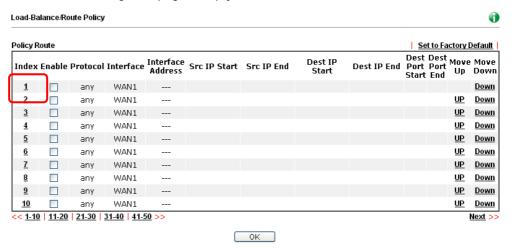
The following figure shows a simple application of load balance. WAN1 and WAN2 can be used to access into Internet. The PC in LAN1 can send the data to the remote PC through the specified WAN1.



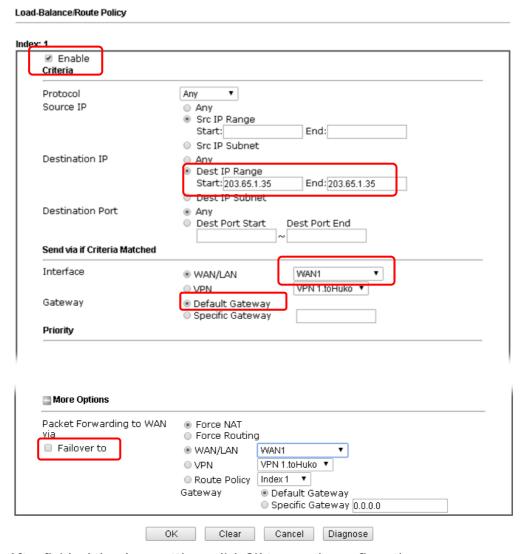
 Access into web user interface of Vigor2860 series. Open Load-Balance/Route Policy>>General Setup.



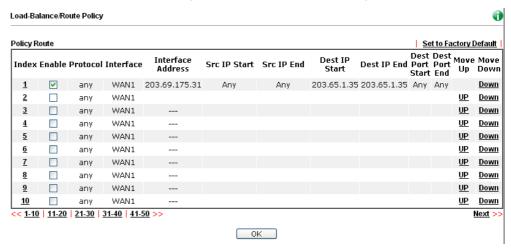
2. From the following web page, simply click index number #1.



3. In the following page, check Enable; set Dest IP Start and Dest IP End with 203.65.1.35 and 203.65.1.35; choose WAN1 as the Interface; click default gateway; do not check Failover to.



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



Now, the packets sent to the remote PC (IP address: 203.65.1.35) will be forced to pass through WAN1.

II-6 LTE

LTE WAN with SIM card can provide convinent Internet access for Vigor router. However, we can't stop thinking about what can Vigor router utilize this SIM card to provide more useful functions for user? Now, we have developed some useful functions for user, such as sending SMS from a router to report router status, rebooting router remotely via SMS with taking security into consideration, and so on.

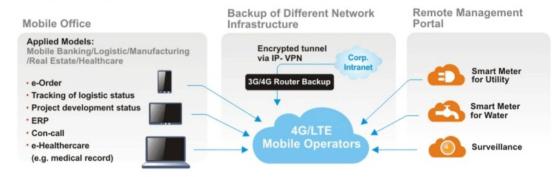
This section can guide you to use the SIM card in LTE WAN to perform SMS related operations.



Info

This function is used for "L" models only.

Service Network



Web User Interface

II-6-1 General Settings

This page allows you to configure general settings for LTE. When SMS Quota Limit is enabled, you can specify the number of SMS quota, actions to perform when quota exceeded, and the period of resetting SMS quota used.

LTE >> General Settings

Quota Limit:	0	SMS	(Current number of SMS sent: 0)
When quota exceeded :	Stop sending SMS		
	Send Mail Alert to A	Administ	rator
Monthly	Custom		
Select the day of a month	n when your SMS quota r	esets.	
SMS quota resets on day	1 v at 00:00 v		

- Note: 1. Please make sure the <u>Time and Date</u> of the router is configured.
 - 2. When quota exceeded, user can choose to stop sending sms or send $\underline{\textbf{e-mail}}$ to administrator.
 - 3. After clicking OK, the counter used will be reset.



Available settings are explained as follows:

Item	Description
Enable SMS Quota Limit	Check the box to enable such feature.
Quota Limit	Specify the maximum number of sending SMS for LTE.
When quota exceeded	There are two actions to be performed when the quota limit is expired.
	Stop sending SMS - If it is checked, no SMS for LTE will be sent after the quota limit is expired.
	Send Mail Alert to Administrator - If it is checkd, a mail alert will be sent to the administrator when the quota limit is expired.
Monthly	This setting is to offer a mechanism of resetting the number of SMS sent record every month.
	SMS quota resets on day XX at XXYou can determine the starting day in one month. The number of SMS sent will be reset.
Custom	This setting allows the user to define the billing cycle according to his request.
	The number of SMS sent will be reset with an interval of cycle duration.
	Custom - Monthly is default setting. If long period or a short period is required, use Custom. The period of reset is between 1 day and 60 days. You can determine the cycle duration by specifying the days and the hours.
	Cycle duration: Specify the days to reset the number of

SMS sent. For example,	7 means the whole cycle is 7
days; 20 means the who	le cycle is 20 days. When the time
is up, the router will re-	set the number of SMS sent
automatically.	

 Today is day XX in the cycle -Specify the day in the cycle duration as the starting point which Vigor router will reset the number of SMS sent. For example, 3 means the third day of the duration cycle.

II-6-2 SMS Inbox

This page will list the received SMS messages in the LTE SIM card. The SMS Inbox table shows the received date, the phone number or sendor ID where this message was from, and the begining of the message content.

Since the data size of one SMS is limited, a long message will be sent by multiple SMS. For the convenience of users, we provide two modes. <u>Simple Mode</u> lists SMS messages in order for received time. <u>Advanced Mode</u> lists SMS in order for real index in the SIM card. Different SIM cards have different capacities. In general, it's around 30 to 40 SMS. Please note that the SIM card can not receive new SMS when all SMS indexes are occupied.

Click the Simple Mode link or the Advanced Mode link below to switch between these two modes.

II-6-2-1 Simple Mode

LTE >> SMS Inbox

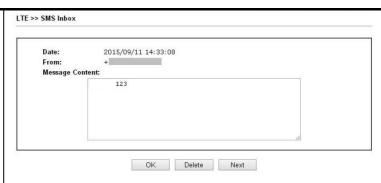
LTE SMS Inbox

Details	Mark as Read	Delete	Date	From	Message
<u>View</u>			2015/10/21 12:03:29	886911520000	
<u>View</u>			2015/10/21 11:31:59	+886905269930	22
<u>View</u>			2015/10/21 11:31:51	+886905269930	11
<u>View</u>			2015/10/21 09:29:39	+886905269930	1
<u>View</u>			2015/10/20 10:15:44	+886988126053	remote reboot 000000 /
<u>View</u>			2015/10/20 10:14:18	+886988126053	remote reboot 000000 /
<u>View</u>			2015/10/20 10:06:49	+886988126053	remote reboot iyt
<u>View</u>			2015/10/20 10:01:01	+886905269930	41
<u>View</u>			2015/10/16 14:13:29	+886988126053	
<u>View</u>			2015/10/16 14:12:46	+886988126053	

Simple Mode: Show SMS messages in order of received dates. **Advanced Mode**: Show SMS in order of indexes in SIM card.

OK

Item	Description
Mark as Read	Those messages in "unread" state are showed in bold text. If you want to change messages into "read" state, select them and click the OK button. Checking the checkbox in title will select all "unread" messages in this page.
Delete	If you want to delete messages, select them and click the OK button. Checking the checkbox in title will select all messages in this page.
Details	If you want to read the full content of the message, click the <u>View</u> link of that message to open the following page. It will change the message into "read" state.

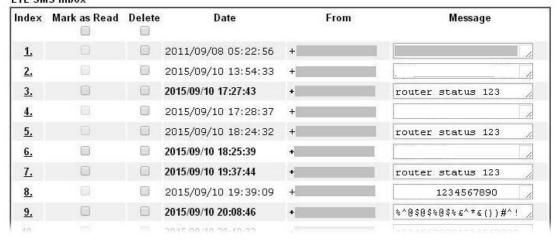


- Message Content Display the full content of the message.
- OK Return to previous page.
- Delete Click it to delete this message and return to previous page.
- Next Click it to see the content of next message.

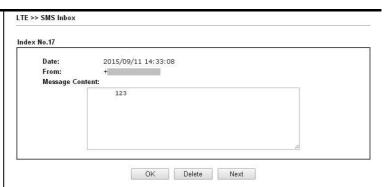
II-6-2-1 Advanced Mode

LTE >> SMS Inbox

LTE SMS Inbox



Item	Description
Mark as Read	Those SMS in "unread" state are shown in bold text. If you want to change SMS into "read" state, select them and click the OK button. Checking the checkbox in title will select all "unread" SMS in this page.
Delete	If you want to delete SMS, select them and click the OK button. Checking the checkbox in title will select all SMS in this page.
Index	If you want to read the full content of the message of the SMS, click the index link of that SMS to open the following page. It will change all SMS of the message into "read" state.



Message Content - Display the full content of the message.

OK - Return to previous page.

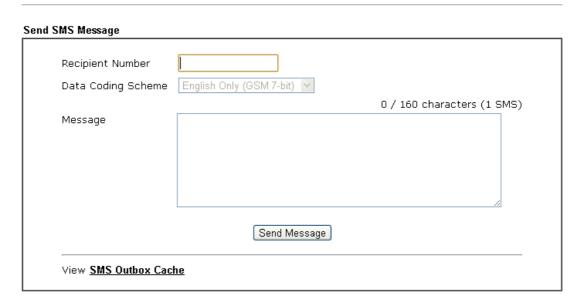
Delete - Click it to delete all SMS of this message and return to previous page.

Next - Click it to see the content of next SMS index.

II-6-3 Send SMS

This page is used to send SMS messages by the LTE SIM card. It also displays the number of SMS required to send the message.

LTE >> Send SMS



Item	Description				
Recipient Number	Type the phone number of the recipient. The format can be an international phone number (+8869123455678) or a general phone number(0912345678).				
Data Coding Scheme	The router will automatically select a suitable Data Coding Scheme according to the current content in Message. GSM 7-bit and UCS-2 are supported.				
Message	Type in the message content to send. The total number of characters that you can type in this field is 1024.				
Send Message	Click it to send this SMS message to the recipient immediately.				
View SMS Outbox Cache	Display the record of SMS messages sent from the Router. LTE >> SMS Outbox Cache				
	LTE SMS O	utbox C	ache		
	Details Delete Date To Message				
	<u>View</u>		2015/10/05 03:12:06	1234567890	555555555555555555555555555555555555555
	<u>View</u>		2015/10/05 03:12:01	1234567890	44444444444444444
	<u>View</u>		2015/10/05 03:11:56	1234567890	333333333333333
	View		2015/10/05 03:11:51	1234567890	22222222222
	<u>View</u>		2015/10/05 03:11:46	1234567890	111111
	<u>View</u>		2015/10/05 03:07:55	1234567890	居易科技於1997年成立,
	View 2015/10/05 03:04:38 1234567890 Test Test Nancy 123				
	Note: Records in Outbox Cache are NOT preserved after replacement of newer records or Router reboot. OK				

II-6-4 Router Commands

This page allows the user to set function to reboot Vigor router remotely and get the router status via SMS.

Get Router Status or Reboot Router via SMS Message



Go to LTE>>Router Commands to get the following page.

eboot on SMS Message			
Enable with Password / PIN			_
Access Control List	List	Phone Number	
	1		
	2		
	3		
router's phone number, follower ply with Router Status Message	d by the pas	sword / PIN if that is enabled.	
Enable with Password / PIN			
Access Control List	List	Phone Number	
	1		
	2		
	3		
Message Contents			
Router Name Route	r Up-Time	☐ Firmware Version ☐ MAC Address	
□WAN1 IP □WAN2	IP	□LTE IP □WAN4 IP	
□WAN1 Data Usage □WAN2	Data Usage	□LTE Data Usage □WAN4 Data Usage	
SMS Number per Status Respons		uter, send a message starting with "router	



Item	Description	
Reboot on SMS Message		
Enable with Password / PIN	To reboot Vigor router remotely via SMS, please check such box and type the password/PIN number (treated as	

	authentication for any mobile phone).
	The password shall be composed by letters, numbers and baseline.
Access Control List	Check the box to type or modify (up to 3) phone numbers.
	The phone number specified here is capable of sending SMS to reboot such Vigor router remotely.
	Note: If such option is enabled, only mobile phones specified here are allowed to send SMS to reboot Vigor router if correct password is given. That is, if it is disabled (unchecked), any mobile phone can send SMS to reboot such Vigor router if correct password is given.
Reply with Router Status Me	essage
Enable with Password / PIN	Users can get the WAN data usage and basic information about Vigor router (e.g., IP address, MAC address) through the mobile phone by entering the password/PIN specified in this field.
	The password shall be composed by letters, numbers and baseline.
Access Control List	Check the box to type or modify (up to 3) phone numbers.
	The phone number specified here is capable of getting related information about Vigor router remotely.
	Note: If such option is enabled, only mobile phones specified here are allowed to obtaine related information about Vigor router if correct password is given. That is, if it is disabled (unchecked), any mobile phone can get the data of Vigor router if correct password is given.
Message Contents	There are several types of message contents for you to select. Choose and check the required item, then Vigor router will offer the status response about that item via SMS.
SMS messages per status response	Display the total number of the type for status response. Display the total number of SMS required to send the status message which contains the current selected Message Contents.

II-6-5 Status

This page will display basic information about the embedded LTE module and the current LTE connection.

LTE >> Status

		<u>Ref</u>	<u>fresh</u>
LTE Mode	em		
	Status:	Operational	
	IMEI:	356318040749422	
	IMSI:	466924200859808	
	Access Tech:	LTE	
	Band:	E-UTRA Op Band 3	
	Operator:	Chunghwa	
	Mobile Country Code:	466	
	Mobile Network Code:	92	
	Location Area Code:	65534	
	Cell ID:	81023501	
	Signal:	-61 dBm	
	Active Channel:	1725	
	Interference with 2.4GHz WLAN:	No	
	Max Channel TX Rate:	50 Mbps	
	Max Channel RX Rate:	100 Mbps	
LTE SMS			
	SMS Centre Number:	+886932400821	
	SMS Service Status:	Ready	
	SMS Loading:	Ready	
	New SMS:	4	

Each item is explained as follows:

Item	Description
Status	LTE WAN status.
IMEI	International Mobile Equipment Identity of the embedded LTE module.
IMSI	International Mobile Subscripber Identity of the LTE SIM card.
Access Tech	Type of LTE connection (CDMA/GSM/WCDMA/LTE/TD-SCDMA).
Band	Band of LTE connection.
Operator	ISP name of LTE connection.
Mobile Country Code / Mobile Network Code / Location Area Code / Cell ID:	Base station information.
Signal	Signal strength of LTE connection.
Active Channel	Frequency of LTE connection.
Interference with 2.4GHz	Whether the current LTE frequency causes interference with 2.4G wireless. If Yes, the interfered 2.4G wireless channels

WLAN	will be indicated.
Max Channel TX Rate / Max Channel RX Rate	Maximum TX/RX link rate of LTE connection.
SMS Centre Number	The phone number for SMS service of the LTE SIM card.
SMS Service status	Whether the SMS service of the LTE SIM card is ready.
SMS Loading	Whether the received SMS messages in the LTE SIM card have been loaded to the Router.
New SMS	The number of unread SMS in SMS Inbox.

Part III Wireless LAN



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 (2.4GHz/5GHz)

This function is used for "n" 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 Vigor2860 wireless series router (with "n", "n-plus" or "ac" 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.

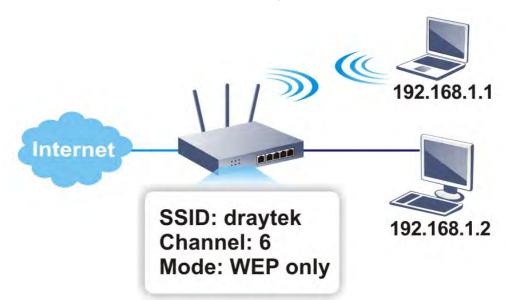
Vigor2860 wireless router is a highly integrated wireless local area network (WLAN) for 5 GHz 802.11ac or 2.4/5 GHz 802.11n WLAN applications. It supports channel operations of 20/40 MHz at 2.4 GHz and 20/40/80 MHz at 5 GHz. Vigor2860 "ac" series router can support data rates up to 1.3 GBps in 802.11ac 80 MHz channels. Vigor2860 "n" 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.



Info

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.



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.

DFS Restrictions

Some of 5GHz channels are DFS channels which are governed radars. Without passing DFS certificate test, we can not open those DFS channels in Vigor router. We are working on DFS certification in Europe and open those channels by releasing new firmware once we receive DFS certification. According to DFS certificate in Europe, we will open channels 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136 and 140.

At present, we will not open DFS channels in the USA because we do not have plan for DFS certification in the USA. Channels 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136 and 140 will be restricted in the USA.

In some countries, there are restrictions on DFS channels as well. We will implement country code to restrict uncertified channels.

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. Besides, the settings will change based on different model of Vigor2860 series. In this case, Vigor2860ac is used as an example.

Wireless Wizard **Host AP Configuration** Wireless 2.4GHz Settings Name: 2860-marketing Mixed(11g+11n) Mode: Channel 8, 2447MHz Channel: Security Key: Wireless 5GHz Settings Use the same SSID and Security Key as above Name: DrayTek2860_5Gmarketing Mode: Mixed (11a+11n) 💌 Channel: Channel 60, 5300MHz ***** Security Key: Note: The host AP configured here will be used for home or internal company use. < Back Next > Finish

Item	Description
Wireless 2.4GHz Setti	ngs
Name	Type the SSID name of this router for wireless 2.4GHz. The default name is defined with DrayTek. Change the name if required.
Mode	At present, the router can connect to 11n Only, 11g Only,

Mixed (11b+11g+1n) Mixed (11a+11n), Mixed (11g+11n), and Mixed (11b+11g+11n) mode. Mixed (11b+11g+11n) Mixed (11a+11n+11ac) stations is multaneously. Use the same SSID and and Security Key as above Mixed (11a+11n) and Mixed (11a+11n+11ac) stations simultaneously. Use the same SSID and and of this router for wireless 5GHz Mode At present, the router can connect to 11a Only, 11n Only (5GHz), Mixed (11a+11n) and Mixed (11a+11n+11ac) stations simultaneously. Channel Means the channel of frequency of the wireless LAN. The default 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.		
default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you. Security Key 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"). Use the same SSID and Security Key as above Wireless 5GHz Settings Name Type the SSID name of this router for wireless 5GHz Mode At present, the router can connect to 11a Only, 11n Only (5GHz), Mixed (11a+11n) and Mixed (11a+11n+11ac) stations simultaneously. Channel Means the channel of frequency of the wireless LAN. The default 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.		Mixed (11b+11g+11n) stations simultaneously. Simply choose Mix (11b+11g+11n) mode. Mixed(11b+11g+11n) 11b Only 11g Only 11n Only (2.4 GHz) Mixed(11b+11g) Mixed(11g+11n)
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"). Use the same SSID and Security Key as above Wireless 5GHz Settings Name Type the SSID name of this router for wireless 5GHz Mode At present, the router can connect to 11a Only, 11n Only (5GHz), Mixed (11a+11n) and Mixed (11a+11n+11ac) stations simultaneously. Channel Means the channel of frequency of the wireless LAN. The default channel is 36. 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.	Channel	default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system
Wireless 5GHz Settings Name Type the SSID name of this router for wireless 5GHz Mode At present, the router can connect to 11a Only, 11n Only (5GHz), Mixed (11a+11n) and Mixed (11a+11n+11ac) stations simultaneously. Channel Means the channel of frequency of the wireless LAN. The default channel is 36. 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.	Security Key	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
Name Type the SSID name of this router for wireless 5GHz Mode At present, the router can connect to 11a Only, 11n Only (5GHz), Mixed (11a+11n) and Mixed (11a+11n+11ac) stations simultaneously. Channel Means the channel of frequency of the wireless LAN. The default channel is 36. 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.	and Security Key as	Check the box to use the same settings configured above.
At present, the router can connect to 11a Only, 11n Only (5GHz), Mixed (11a+11n) and Mixed (11a+11n+11ac) stations simultaneously. Channel Means the channel of frequency of the wireless LAN. The default channel is 36. 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.	Wireless 5GHz Setting	ds
(5GHz), Mixed (11a+11n) and Mixed (11a+11n+11ac) stations simultaneously. Channel Means the channel of frequency of the wireless LAN. The default channel is 36. 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.	Name	Type the SSID name of this router for wireless 5GHz
default channel is 36. 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.	Mode	(5GHz), Mixed (11a+11n) and Mixed (11a+11n+11ac) stations
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.	Channel	default channel is 36. 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
	Security Key	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
Cancel Exit the wireless wizard without saving any changes.		
	Next	"0x321253abcde").

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

Wireless 2.4GHz	z Settings
Enable	Disable
SSID:	DrayTek_Guest
Security Key:	*****
Rate Control:	Enable Upload 30000 kbps Download 30000 kbps
Wireless 5GHz S	Settings
Enable	Disable
Use the sam	ne SSID and Security Key as above
SSID:	DrayTek_5G_Guest
Security Key:	*****
Rate Control:	Enable Upload 30000 kbps Download 30000 kbps
Note: The confi	iqured quest AP will not be able to access the LAN network, VPN
connections, o	r communicate with wireless devices connecting to the router's other APs. ce shall be used for Internet access only.

Item	Description				
Wireless 2.4GHz Setti	Wireless 2.4GHz Settings				
Enable/Disable	Click it to enable or disable settings in this page.				
SSID	Type 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").				
Rate Control	It controls the data transmission rate through wireless connection. Upload - Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps. Download - Type the transmitting rate for data download. Default value is 30,000 kbps.				
Wireless 5GHz Setting	gs				
Enable/Disable	Click it to enable or disable settings in this page.				
Use the same SSID and Security Key as above	Check the box to use the same settings configured above.				
SSID	Type the SSID name of this router. (SSID2)				
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").
Rate Control	It controls the data transmission rate through wireless connection. Upload - Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps. Download - Type the transmitting rate for data download. Default value is 30,000 kbps.
Next	Click it to get into the next setting page.
Cancel	Exit the wireless wizard without saving any changes.

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

Wireless Wizard **Configuration Summary** Wireless 2.4GHz Settings Wireless 5GHz Settings Mode:Mixed(11g+11n) Mode:Mixed (11a+11n) Channel: Channel 8, 2447MHz Channel: Channel 60, 5300MHz Host AP Host AP SSID Name: 2860-marketing SSID Name: DrayTek2860_5Gmarketing Security Key: ********** Security Key: *********** Guest AP Guest AP Status:Enabled Status:Enabled SSID Name:DrayTek_Guest ${\tt SSID Name:DrayTek_5G_Guest}$ Security Key: ********** Security Key: ********** Rate Control: Disabled Rate Control:Disabled Next > < Back Finish Cancel

6. Click Finish to complete the wireless settings configuration.

III-1-2 General Setup

By clicking the Wireless LAN>>General Setup, 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.

ible Wireles	s LAN					
Mode:			Mixed(11b+11g	ı+11n) ▼		
Channel:			Channel 11, 24	62MHz ▼		
Enable F	lide SSID		SSID	Isol	ate Member	Isolate VPN
1		DrayTek				
2 🔲		DrayTek_Gu	est			
3						
4						
to the same	e SSID from	connecting	guration will f to each othe solate the wi	٠.		
to the same The isolate	e SSID from VPN config	connecting uration will i		r. reless traffi	c from VPN c	onnections
to the same The isolate and thus, v	e SSID from VPN config vireless clie	connecting uration will i nts will not	to each othe isolate the wir be able to acc	r. reless traffi	c from VPN c N network u	onnections nder this
to the same The isolate and thus, v setting. Rate Contro	e SSID from VPN config vireless die ol Enabl	connecting uration will i nts will not	to each othe isolate the wi be able to acc Upload	r. reless traffi ess the VP	c from VPN c N network ui <u>Downlo</u>	onnections nder this ad
to the same The isolate and thus, v setting. Rate Contro SSID 1	e SSID from VPN config vireless clie	oconnecting uration will i nts will not	to each other isolate the wire be able to accomplete to accomplete to accomplete to accomplete the second s	r. reless traffi ess the VP	c from VPN c N network u Downlo 30000	onnections nder this ad kbps
The isolate and thus, v setting. Rate Contro SSID 1 SSID 2	e SSID from VPN config vireless die ol Enabl	oconnecting uration will i nts will not	to each other isolate the wire be able to accomplete to accomplete to accomplete to accomplete the beautiful to ac	r. eless traffi ess the VP	pownloo 30000	onnections nder this ad kbps kbps
The isolate and thus, v setting. Rate Control SSID 1 SSID 2 SSID 3	e SSID from VPN config vireless die ol Enabl	ocnnecting uration will i nts will not	Upload 30000 kbp 30000 kbp	r. reless traffi ess the VP	Downlo. 30000 30000	ad kbps kbps kbps
The isolate and thus, v setting. Rate Control SSID 1 SSID 2 SSID 3 SSID 4	e SSID from VPN config vireless die ol Enabl	ocnnecting uration will i nts will not	to each other isolate the wire be able to accomplete to accomplete to accomplete to accomplete the beautiful to ac	r. reless traffi ess the VP	pownloo 30000	onnections nder this ad kbps kbps
The isolate and thus, v setting. Rate Control SSID 1 SSID 2 SSID 3 SSID 4 Note:	e SSID from VPN config vireless clie	a connecting uration will i nts will not	Upload 30000 kbp 30000 kbp	reless traffi ess the VP	Downlo. 30000 30000 30000	ad kbps kbps kbps kbps
The isolate and thus, v setting. Rate Control SSID 1 SSID 2 SSID 3 SSID 4 Note:	e SSID from VPN config vireless clie ol Enable	uration will ints will not	Upload 30000 kbp 30000 kbp	reless traffi ess the VP	Downlo. 30000 30000 30000	ad kbps kbps kbps kbps kbps

OK Cancel

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Mode	For 2.4GHz/LTE: At present, the router can connect to 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.
	Mixed(11b+11g+11n) ✓ 11g Only 11n Only (2.4 GHz) Mixed(11b+11g) Mixed(11g+11n) Mixed(11a+11n 5 GHz) Mixed(11b+11g+11n) Mixed(11a+11n+11ac) Mixed (11a+11n+11ac)
	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.

	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.
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. For 2.4GHz: Channel 6, 2437MHz Channel 1, 2412MHz Channel 3, 2422MHz Channel 3, 2422MHz Channel 4, 2427MHz Channel 4, 2427MHz Channel 5, 2432MHz Channel 5, 2432MHz Channel 6, 2437MHz Channel 6, 2437MHz Channel 7, 2442MHz Channel 7, 2442MHz Channel 19, 2452MHz Channel 10, 2457MHz Channel 10, 2457MHz Channel 11, 2462MHz Channel 11, 2462MHz Channel 165, 5825MHz Channel 165, 5825MHz
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity.
SSID	Means the identification of the wireless LAN. SSID can be any text numbers or various special characters.
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.
Rate Control	It controls the data transmission rate through wireless connection. Upload - Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps. Download - Type the transmitting rate for data download. Default value is 30,000 kbps.
Schedule	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.

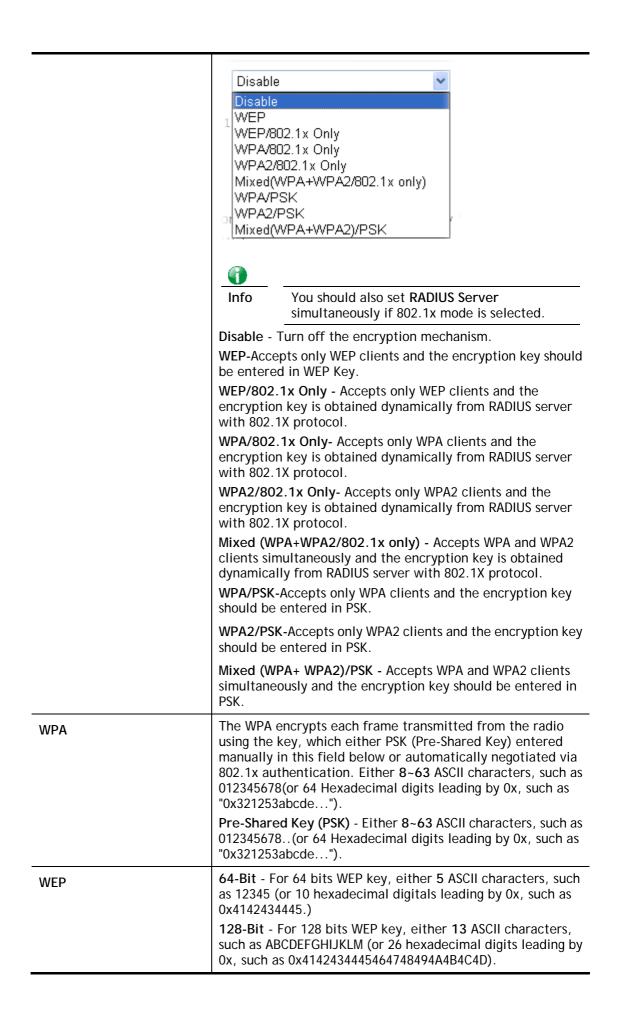


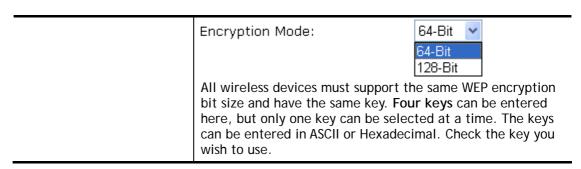
By clicking the Wireless LAN>>Security Settings, a new web page will appear so that you could configure the settings of WPA and WEP.

Wireless LAN(2.4GHz) >> Security Settings

SID 1	SSID 2	SSID 3	SSID 4
Mode:			WEP/802.1x Only
<u>WPA</u>			
	Encryption Mode	: :	TKIP for WPA/AES for WPA2
	Pre-Shared Key	PSK):	******
	Type 8~63 ASCI "cfgs01a2" or	I character or "0x655abcd	or 64 Hexadecimal digits leading by "0x", for example".
WEP			
	Encryption Mode	! :	64-Bit 🔻
	® Key 1:		*******
	○ Key 2 :		*******
	○ Key 3 :		*******
	○ Key 4 :		*******
Note:			
Please	configure the <u>RA</u>	DIUS Server if	f 802.1x is used.
			lease insert 5 ASCII characters or 10 Hexadecimal "AB312" or "0x4142333132".
	8 bit WEP key cor leading by "0x".	nfigurations, (please insert 13 ASCII characters or 26 Hexadecimal

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



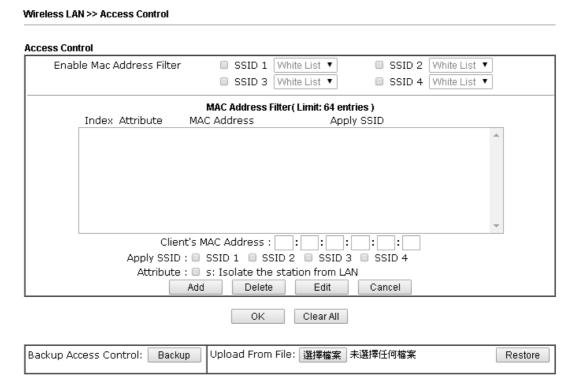


After finishing all the settings here, please click **OK** to save the configuration.

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.



Item	Description
Enable Mac Address Filter	Select to enable the MAC Address filter for wireless LAN identified with SSID 1 to 4 respectively. All the clients (expressed by MAC addresses) listed in the box can be grouped under different wireless LAN. For example, they can be grouped under SSID 1 and SSID 2 at the same time if you check SSID 1 and SSID 2.
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.

Apply SSID	After entering the client's MAC address, check the box of the SSIDs desired to insert this MAC address into their access control list.
Attribute	s: Isolate the station from LAN - select to isolate the wireless connection of the wireless client of the MAC address from LAN.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.
OK	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.

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

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.





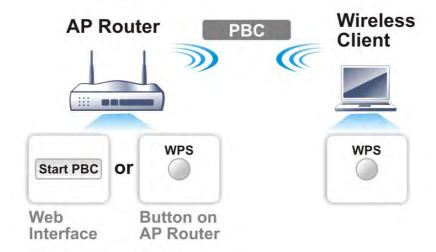
Info

WPS is available for the wireless station with WPS supported.

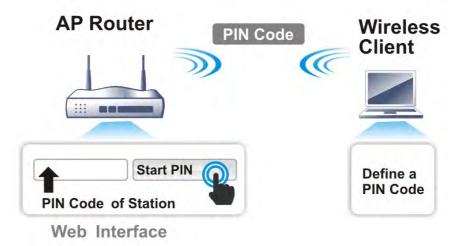
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for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

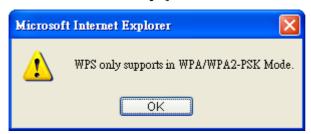
• On the side of Vigor 2860 series which served as an AP, press WPS button once on the front panel of the router or click Start PBC on web configuration interface. On the side of a station with network card installed, press Start PBC button of network card.



• 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(2.4GHz) >> WPS (Wi-Fi Protected Setup)

☑ Enable WPS 🗘

Wi-Fi Protected Setup Information

WPS Status	Configured
SSID	DrayTek_2860_130
Authentication Mode	Mixed(WPA+WPA2)/PSK

Device Configure

Configure via Push Button	Start PBC
Configure via Client PinCode	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.

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

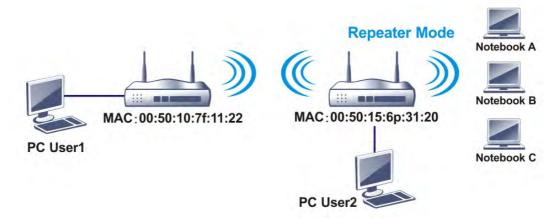
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- 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:

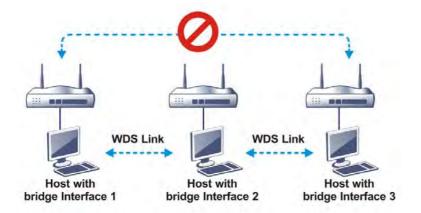


The application for the WDS-Repeater mode is depicted as below:



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

Mode: Bridge	Bridge
mode.	Enable Peer MAC Address
Security:	
Disable	
O DISUBLE O WEP O Pre-Shared Rey	
WEP:	
Use the same WEP key set in $\ \underline{\text{\bf Security Settings}}.$	Note: Disable unused links to get better
	_ performance.
Pre-shared Key:	Repeater
Type:	Enable Peer MAC Addess
○ WPA	
Key : *********	
Note: WPA and WPA2 are not compatible with	
DrayTek WPA.	
Type 8~63 ASCII characters or 64 hexadecimal	
digits leading by "0x", for example "cfgs01a2" or "0x655abcd".	Access Point Function:
	⊙ Enable ○ Disable
	Status:
	Send "Hello" message to peers.
	Link Status
	Note: The status is valid only when the peer also supports this function.

Item	Description
Mode	Choose the mode for WDS setting. 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.

	Disable Disable Bridge Repeater
Security	There are three types for security, Disable , WEP and Pre-shared key . The setting you choose here will make the following WEP or Pre-shared key field valid or not. Choose one of the types for the router.
WEP	Check this box to use the same key set in Security Settings page. If you did not set any key in Security Settings page, this check box will be dimmed.
Pre-shared Key	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	If you choose Bridge as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Yet please disable the unused link to get better performance. If you want to invoke the peer MAC address, remember to check Enable box in the front of the MAC address after typing.
Repeater	If you choose Repeater as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Similarly, if you want to invoke the peer MAC address, remember to check Enable box in the front of the MAC address after typing.
Access Point Function	Click Enable to make this router 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 \mathbf{OK} to save the configuration.

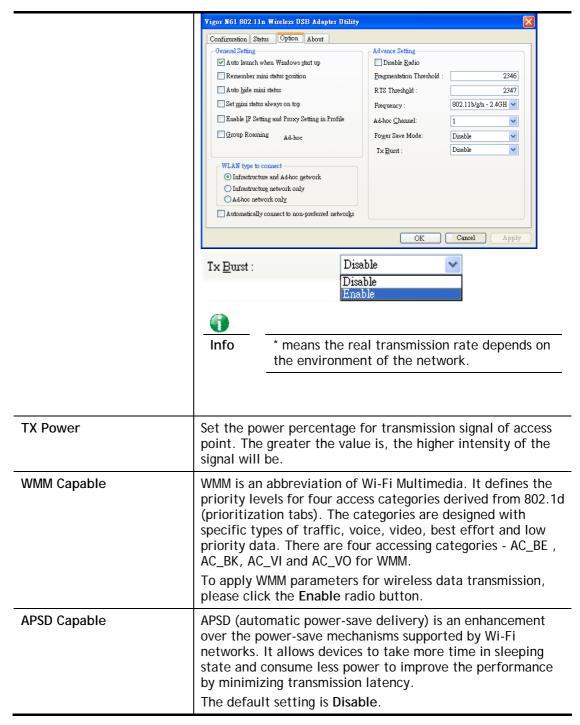
III-1-7 Advanced Setting

This page allows users to set advanced settings such as operation mode, channel bandwidth, guard interval, and aggregation MSDU for wireless data transmission.

T Physical Mode	
Operation Mode	Mixed Mode Green Field
Channel Bandwidth	O 20 ⊙ 20/40
Guard Interval	O long auto
Aggregation MSDU(A-MSDU)	O Disable O Enable
Long Preamble	⊙ Disable ○ Enable
Packet-OVERDRIVE TM TX Burst	Disable Enable
	ОК
/ireless LAN(5GHz) >> Advanced S	etting
hysical Mode	
Operation Mode	Mixed Mode Green Field
Channel Bandwidth	O 20 O 20/40 O 20/40/80
Guard Interval	O long auto
Aggregation MSDU(A-MSDU)	O Disable 💿 Enable
Number of Spatial Streams(NSS)	○ 1 ⊙ 2 ○ 3
	OK
fireless LAN >> Advanced Setting	
T Physical Mode	
Operation Mode	Mixed Mode Green Field
operación mode	○ 20 ● 20/40
Channel Bandwidth	20 9 20/10
Channel Bandwidth Guard Interval	○ long ● auto
Channel Bandwidth Guard Interval Aggregation MSDU(A-MSDU)	○ long ● auto ● Enable ○ Disable
Channel Bandwidth Guard Interval Aggregation MSDU(A-MSDU) Long Preamble	long autoEnable DisableEnable Disable
Channel Bandwidth Guard Interval Aggregation MSDU(A-MSDU) Long Preamble Packet-OVERDRIVE TM TX Burst	long autoEnable DisableEnable DisableEnable Disable
Channel Bandwidth Guard Interval Aggregation MSDU(A-MSDU) Long Preamble	long autoEnable DisableEnable Disable

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- the router will use 20Mhz for data transmission and receiving between the AP and the stations.
	20/40 - the router will use 20Mhz or 40Mhz for data transmission and receiving according to the station capability. Such channel can increase the performance for data transit.
	20/40/80 - the router will use 20Mhz, 40Mhz or 80Mhz for data transmission and receiving according to the station capability. Such channel can increase the performance for data transit.
Guard Interval	It is to assure the safety of propagation delays and reflections for the sensitive digital data. If you choose auto as guard interval, the AP router will choose short guard interval (increasing the wireless performance) or long guard interval for data transmit based on the station capability.
Aggregation MSDU	Aggregation MSDU can combine frames with different sizes. It is used for improving MAC layer's performance for some brand's clients. The default setting is Enable .
Number of Spatial Streams (NSS)	Setup Number of Spatial Stream for Vigor2860ac and Vigor2860Vac.
	Default value is 2 and connection rate could reach 1.3GBps.
Long Preamble	This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. Click Enable to use Long Preamble if needed to communicate with this kind of devices.
Packet-OVERDRIVE	This feature can enhance the performance in data transmission about 40%* more (by checking 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. 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).



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(2.4GHz) >> Station Control SSID 1 SSID 2 SSID 3 SSID 4

SSID 1	SSID 2	SSID 3	SSID 4	
SSID		DrayTek		
Enable				
Connec	tion Time	1 hour	~	
Reconn	ection Time	1 day	~	
Display a	All Station Contro	<u>ll List</u>		
WEB Po	rtal Setup			

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



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, type 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.
WEB Portal Setup	Click it to access in to LAN>>Web Portal Setup page for modifying the settings if required.

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

III-1-9 AP Discovery

Vigor router can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of this router can be found. Please click **Scan** to discover all the connected APs.

Access Point List Index BSSID Channel RSSI SSID Authentication Scan See Statistics. Add to WDS Settings: AP's MAC address Add to Bridge Repeater

Note:

- 1. During the scanning process (\sim 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:

Wireless LAN(2.4GHz) >> Access Point Discovery

Item	Description
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button.
Statistics	It displays the statistics for the channels used by APs. Wireless LAN >> Site Survey Statistics Recommended channels for usage:1 2 3 4 5 6 7 8 9 10 11 12 13 AP number v.s. Channel Channel Cancel
Add to	If you want the found AP applying the WDS settings, please type in the AP's MAC address on the bottom of the page and click Bridge or Repeater. Next, click Add to. Later, the MAC address of the AP will be added to Bridge or Repeater field of WDS settings page.

III-1-10 Station List

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

Refresh Status Codes: C: Connected, No encryption. E: Connected, WEP. P: Connected, WPA. A: Connected, WPA. B: Blocked by Access Control. N: Connecting. F: Fail to pass WPA/PSK authentication.					General	Advance
Status Codes: C: Connected, No encryption. E: Connected, WEP. P: Connected, WPA. A: Connected, WPA2. B: Blocked by Access Control. N: Connecting.	Index	Status	MAC Address	Asso	ciated with	
Status Codes: C: Connected, No encryption. E: Connected, WEP. P: Connected, WPA. A: Connected, WPA2. B: Blocked by Access Control. N: Connecting.						^
Status Codes: C: Connected, No encryption. E: Connected, WEP. P: Connected, WPA. A: Connected, WPA2. B: Blocked by Access Control. N: Connecting.						
Status Codes: C: Connected, No encryption. E: Connected, WEP. P: Connected, WPA. A: Connected, WPA2. B: Blocked by Access Control. N: Connecting.						
Status Codes: C: Connected, No encryption. E: Connected, WEP. P: Connected, WPA. A: Connected, WPA2. B: Blocked by Access Control. N: Connecting.						
Status Codes: C: Connected, No encryption. E: Connected, WEP. P: Connected, WPA. A: Connected, WPA2. B: Blocked by Access Control. N: Connecting.						
Status Codes: C: Connected, No encryption. E: Connected, WEP. P: Connected, WPA. A: Connected, WPA2. B: Blocked by Access Control. N: Connecting.						~
C: Connected, No encryption. E: Connected, WEP. P: Connected, WPA. A: Connected, WPA2. B: Blocked by Access Control. N: Connecting.			Refresh			
E: Connected, WEP. P: Connected, WPA. A: Connected, WPA2. B: Blocked by Access Control. N: Connecting.	Status Code	s:				
P: Connected, WPA. A: Connected, WPA2. B: Blocked by Access Control. N: Connecting.						
A: Connected, WPA2. B: Blocked by Access Control. N: Connecting.						
B: Blocked by Access Control. N: Connecting.						
N: Connecting.						
F: Fail to pass WPA/PSK authentication.	N: Connect	ing.				
	F: Fail to pa	ass WPA/PSK authe	ntication.			
		ee i umitui '				
Add to Access Control:	Add to Acce	33 Control				

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.



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.

Part IV 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.



U

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

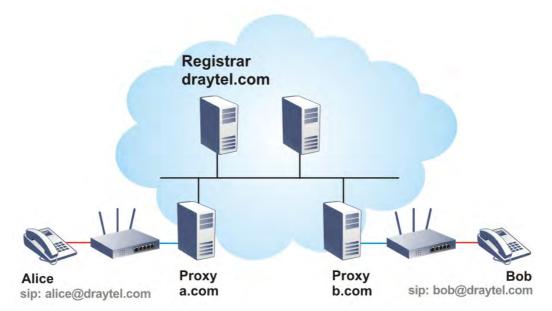
Some fields may be optional in different use. In general, "host" refers to a domain. The "userinfo" includes the user field, the password field and the @ sign following them. This is very similar to a URL so some may call it "SIP URL". SIP supports peer-to-peer direct calling and also calling via a SIP 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.

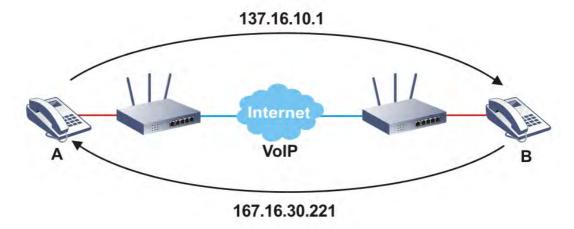
If you both register to the same SIP Registrar, then it will be illustrated as below:



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 using 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.

Our 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

VI-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>>VolP Wizard.



2. The screen of VolP Wizard will be shown as follows.

VoIP Wizard Set VoIP service provider domain VoIP service provider draytel.org draytel.org (63 char max). 5060 SIP Port Set Account quickly Phone 1 (default mapping to Account 1) Account Number/Name (63 char max). (63 char max). Password Phone 2 (default mapping to Account 2) ☑ use the same Account as phone1 Account Number/Name (63 char max). Password (63 char max). < Back | Next > Finish Cancel

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 - Type the account number/name registered to your ISP. Password - Type 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.

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!

VI-1-2 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.

VoIP >> DialPlan Setup		
DialPlan Configuration		
	Phone Book	
	<u>Digit Map</u>	
	Call Barring	
	<u>Regional</u>	
	PSTN Setup	
Secure Phone configuration		
	☑ Enable Secure Phone (ZRTP+SRTP)	
	☑ Enable SAS Voice Prompt	
	OK	

Available settings are explained as follows:

Item	Description
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.

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.



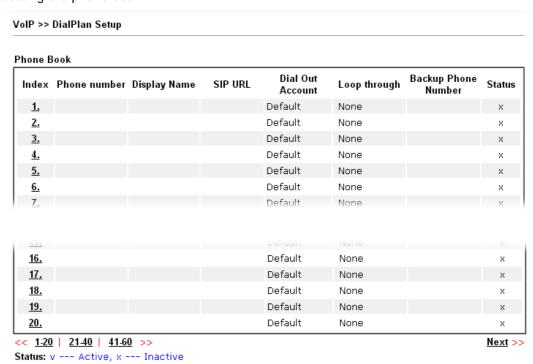
Info

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.

VI-1-1-1 Phone Book

VoIP >> DialPlan Setup

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 total 60 index entries in the phonebook for you to store all your friends and family members' SIP addresses. Loop through and Backup Phone Number will be displayed if you are using Vigor2860 series for setting the phone book.



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

Phone Book Index No. 1 ☑ Enable Phone Number Display Name Polly SIP URL 1112 @ fwd.pulver.com Dial Out Account Default 💌 PSTN 🕶 Loop through None Backup Phone Number 0K Clear Cancel

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.
Loop through	Choose PSTN to enable loop through function. None None PSTN
Backup Phone Number	When the VoIP phone obstructs or the Internet breaks down for some reasons, the backup phone will be dialed out to replace the VoIP phone number. At this time, the phone call will be changed from VoIP phone into PSTN call according to the loop through direction chosen. Note that, during the phone switch, the blare of phone will appear for a short time. And when the VoIP phone is switched into the PSTN phone, the telecom co. might charge you for the connection fee. Please type in backup phone number for this VoIP phone setting.

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

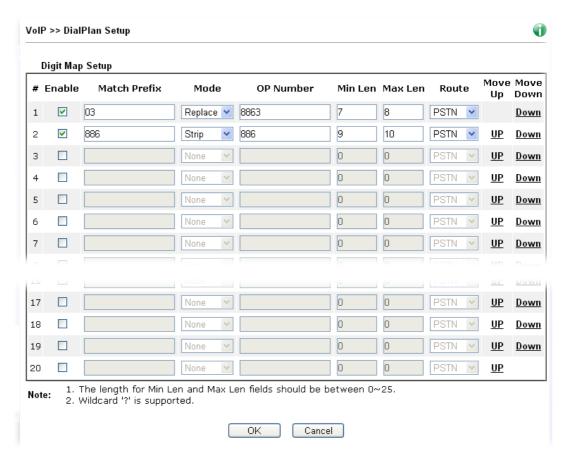


Info

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.

VI-1-1-2 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.



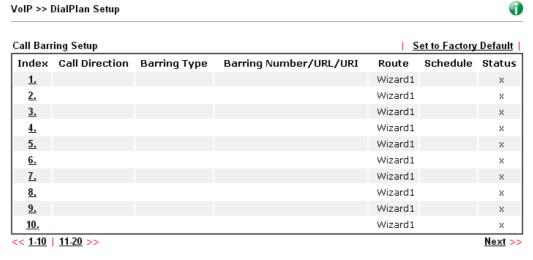
Item	Description
Enable	Check this box to invoke this setting.
Match Prefix	It is used to match with the number you dialed and may be modified by the action (add, strip or replace) with the OP Number.
Mode	None - No action.
	Add - When you choose this mode, the OP number will be added before the match prefix number for calling out through the specific route.
	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.
	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 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 "88631111111" and sent to

	SIP server.
	Mode
	Replace V None Add Strip Replace
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.

VI-1-1-3 Call Barring

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



Advanced: <u>Block Anonymous</u> <u>Block Unknown Domain</u> <u>Block IP Address</u> Click any index number to display the dial plan setup page.

VoIP >> DialPlan Setup

Call Barring Index No. 1 ✓ Enable Call Direction Barring Type Specific URI/URL Route Index(1-15) in Schedule Setup Note: Wildcard '?' is supported.

Cancel

ΟK

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. IN VIN OUT IN & OUT
Barring Type	Determine the type of the VoIP phone call, URI/URL or number. Specific URI/URL Specific URI/URL Specific 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.

Additionally, you can set advanced settings for call barring such as **Block Anonymous**, **Block Unknown Domain** or **Block IP Address**. Simply click the relational links to open the web page.

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.

Call Barring Block Anonymous Route	VoIP >> DialPlan Setup	
Route		
Index(1-15) in Schedule Setup , , , , , , , , , , , , , , , , , , ,		
Note:Block the incoming calls which do not have the caller ID. OK Cancel OR DialPlan Setup	Route	☐ Phone1 ☐ Phone2
OK Cancel OR Block Unknown Domain - this function can block incoming calls (through Phone port) from the control also can be done be an preconfigured schedules. VolP >> DialPlan Setup Call Barring Block Unknown Domain Route Phone1 Phone2 Index(1-15) in Schedule Setup , , , , , , , , , , , , , , , , , , ,	Index(1-15) in <u>Schedule</u> Setup	, , , , , , , , , , , , , , , , , , , ,
or Block Unknown Domain - this function can block incoming calls (through Phone port) from the cognized domain that is not specified in SIP accounts. Such control also can be done bath preconfigured schedules. VoIP >> DialPlan Setup Call Barring Block Unknown Domain Route Phone1 Phone2 Index(1-15) in Schedule Setup , , , , , , , , , , , , , , , , , , ,	Note: Block the incoming calls which do not have t	the caller ID.
nrecognized domain that is not specified in SIP accounts. Such control also can be done ban preconfigured schedules. VoIP >> DialPlan Setup Call Barring Block Unknown Domain Route Phone1 Phone2 Index(1-15) in Schedule Setup , , , , , , , , , , , , , , , , , , ,	ОК	Cancel
Route Phone1 Phone2 Index(1-15) in Schedule Setup , , , , , , , , , , , , , , , , , , ,	n preconfigured schedules.	n SIP accounts. Such control also can be done based
Route Phone1 Phone2 Index(1-15) in Schedule Setup , , , , , , , , , , , , , , , , , , ,	Call Parring Plack Hoknown Damain	
Index(1-15) in Schedule Setup , , , , , , , , , , , , , , , , , , ,		Dhono1 Dhono2
Note: If the domain of the incoming call is different from the domain found in SIP accounts, the call should be blocked. OK Cancel OR Cancel		Filone Filonez
OK Cancel OK Cancel OR Block IP Address - this function can block incoming calls (through Phone port) coming from address. Such control also can be done based on preconfigured schedules. VoIP >> DialPlan Setup Call Barring Block IP Address Route Phone 1 Phone 2	, , ,	t from the domain found in SID accounts the call should
or Block IP Address - this function can block incoming calls (through Phone port) coming from address. Such control also can be done based on preconfigured schedules. VoIP >> DialPlan Setup Call Barring Block IP Address Route		them the deman read in our decounts, the can should
P address. Such control also can be done based on preconfigured schedules. VolP >> DialPlan Setup Call Barring Block IP Address Route	OK_	Cancel
P address. Such control also can be done based on preconfigured schedules. VoIP >> DialPlan Setup Call Barring Block IP Address Route		
Call Barring Block IP Address Route		
Route Phone1 Phone2	VoIP >> DialPlan Setup	
Think!	Call Barring Block IP Address	
Index(1-15) in <u>Schedule</u> Setup , , , ,	Route	Phone1 Phone2
	Index(1-15) in <u>Schedule</u> Setup	
Note: The incoming calls by means of IP dialing (e.g. #192*168*1*1#) should be blocked.	Note:The incoming calls by means of IP dialing (e.	g.#192*168*1*1#) should be blocked.
OK Cancel		

VI-1-1-4 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 Enable Regional Set to Factory Default Last Call Return [Miss]: *69 *14 Last Call Return [In]: *12 Last Call Return [Out]: *72 Call Forward [All] [Act]: Call Forward [Deact]: *73 +number+# *90 *92 Call Forward [Busy] [Act]: Call Forward [No Ans] [Act]: +number+# +number+# Do Not Disturb [Act]: Do Not Disturb [Deact]: *78 +# *79 +# *67 Hide caller ID [Act]: +# Hide caller ID [Deact]: *68 +# Call Waiting [Act]: *56 +# Call Waiting [Deact]: *57 +# Block Anonymous [Act]: *77 +# Block Anonymous [Deact]: *87 +# Block Unknow Domain +# Block Unknow Domain [Act]: *40 *04 +# [Deact]: Block IP Calls [Act]: *50 Block IP Calls [Deact]: *05 +# +# *60 Block Last Calls [Act]: +#

OK

Cancel

Available settings are explained as follows:

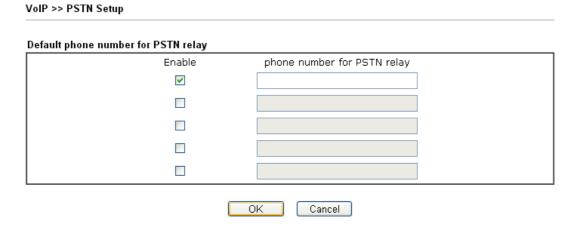
Item	Description
Enable Regional	Check this box to enable this function.
Last Call Return [Miss]	Sometimes, people might miss some phone calls. Please dial number typed in this field to know where the last phone call comes from and call back to that one.
Last Call Return [In]	You have finished an incoming 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 filed 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.

VI-1-1-5 PSTN Setup

Some emergency phone (e.g., 911) or special phone cannot be dialed out by using VoIP and can be called out through PSTN line only. To solve this problem, this page allows you to set five sets of PSTN number for dialing without passing through Internet. Check the Enable box to make the PSTN number available for dial whenever you need and type the number in the field of phone number for PSTN relay.

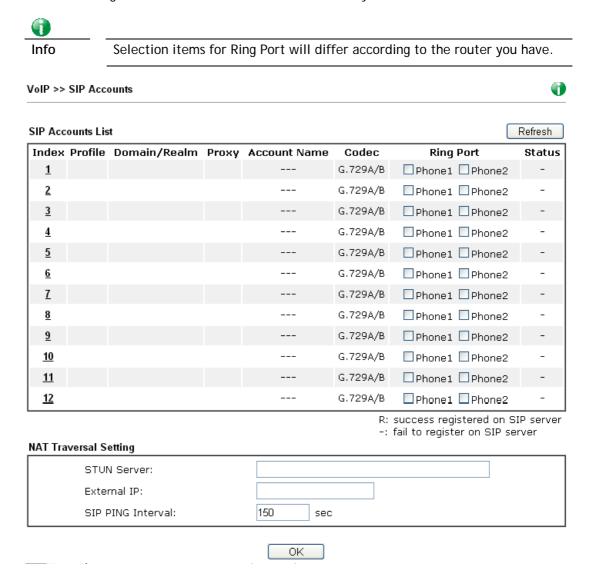


After finishing all the settings here, please click **OK** to save the configuration.

VI-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.



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.
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.

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

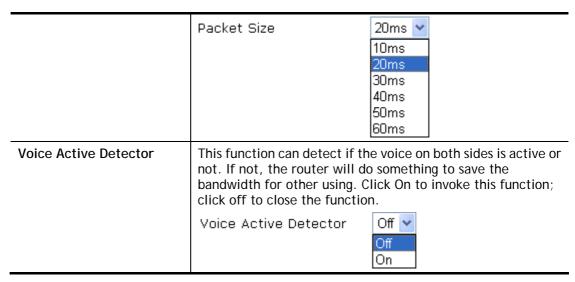
VoIP >> SIP Accounts

Profile Name	(11 char max.)
Register via	None 💌 🗆 Call without Registration
SIP Port	5060
Domain/Realm	(63 char max.)
Proxy	(63 char max.)
🔲 Act as outbound pro	×y
Display Name	(23 char max.)
Account Number/Name	(63 char max.)
Authentication ID	(63 char max.)
Password	(63 char max.)
Expiry Time	1 hour 💌 3600 sec
NAT Traversal Support	None 💌
Call Forwarding	Disable 💌
SIP URL	
Time Out	30 sec
Ring Port	Phone1 Phone2
Ring Pattern	1 🕶
Prefer Codec	G.729A/B (8Kbps) 🔻 🗌 Single Codec
Packet Size	20ms 🕶
Voice Active Detector	Off 💌

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. None None Auto WAN1 WAN2 WAN3 WAN4 LANWPN PVC/MLAN
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., nat.draytel.org:5065)
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	If the router (e.g., broadband router) you use connects to internet by other device, you have to set this function for your necessity.
	NAT Traversal Support None Stun Manual Nortel
	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	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. Disable Always Busy No Answer Busy or No Answer
	SIP URL - Type in the SIP URL (e.g., aaa@draytel.org or abc@iptel.org) as the site for call forwarded. Time Out - Set the time out for the call forwarding. The default setting is 30 sec.
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. Ring Pattern 1 2 3 4 5 6
Prefer Codec	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. 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. G.729A/B (8Kbps) G.711MU (64Kbps) G.729A/B (8Kbps) G.729A/B (8Kbps) G.729A/B (8Kbps) G.726_32 (32kbps) Single Codec - If the box is checked, only the selected Codec will be applied.
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.

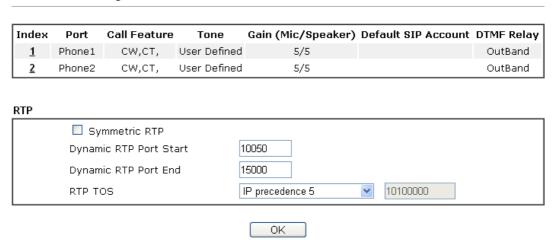


After finishing all the settings here, please click **OK** to save the configuration.

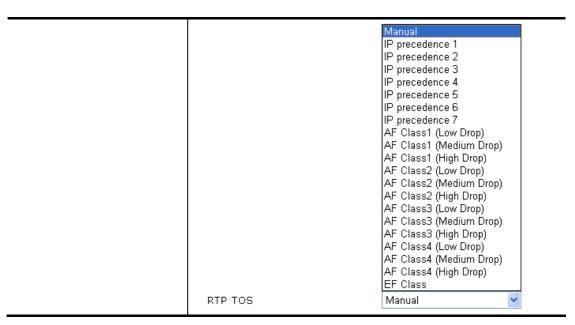
VI-1-4 Phone Settings

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



Item	Description
Phone List	Port - there are two phone ports provided here for you to configure. Phone1/Phone2 allows you to set general settings for PSTN phones.
	Call Feature - A brief description for call feature will be shown in this field for your reference.
	Tone - Display the tone settings that configured in the advanced settings page of Phone Index. Gain - Display the volume gain settings for Mic/Speaker that configured in the advanced settings page of Phone Index.
	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.
	DTMF Relay - Display DTMF mode that configured in the advanced settings page of Phone Index.
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.



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.

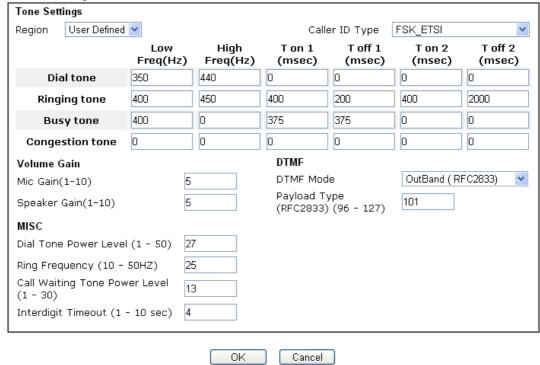
VoIP >> Phone Settings Phone1 Call Feature Default SIP Account v Hotline Play dial tone only when account registered Session Timer sec T.38 Fax Function Error Correction Mode REDUNDANCY V DND(Do Not Disturb) Mode Index(1-15) in Schedule Setup: Note: Action and Idle Timeout settings will be ignored. Index(1-60) in Phone Book as Exception List: CLIR (hide caller ID) ✓ Call Waiting ✓ Call Transfer ΟK Cancel Advanced

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.

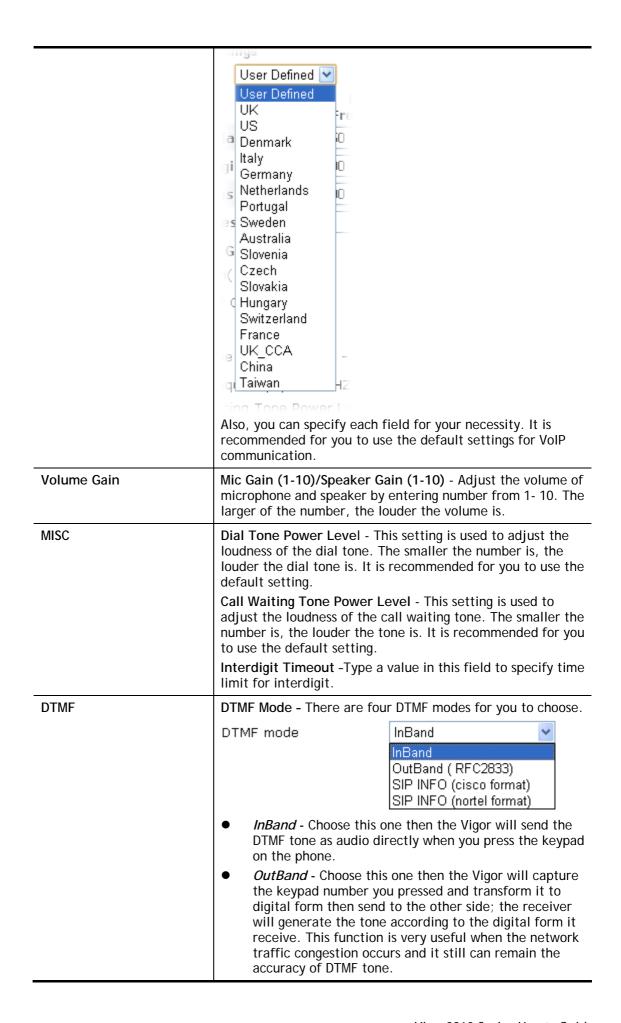
	Error Correction Mode - choose a mode for error correction.
DND (Do Not Disturb) mode	Set a period of peace time without disturbing by VoIP phone call. During the period, the one who dial in will listen busy tone, yet the local user will not listen any ring tone.
	Index (1-15) in Schedule - Enter the 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.

Advance Settings >> Phone 1



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.

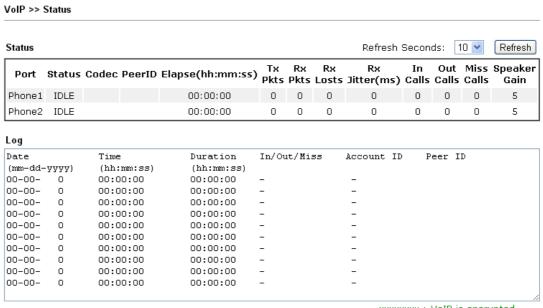


• SIP INFO- Choose this one then the Vigor will capture the DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message.

Payload Type (rfc2833) - Type a number from 96 to 127, the default value was 101. This setting is available for the OutBand (RFC2833) mode.

VI-1-5 Status

From this page, you can find codec, connection and other important call status for each port.



xxxxxxxx : VoIP is encrypted. xxxxxxxx : VoIP isn't encrypted.

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.
	Refresh Seconds: 10 \(\frac{10}{5} \) 10 \(\frac{10}{30} \)
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 Losts	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.

Part V 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.

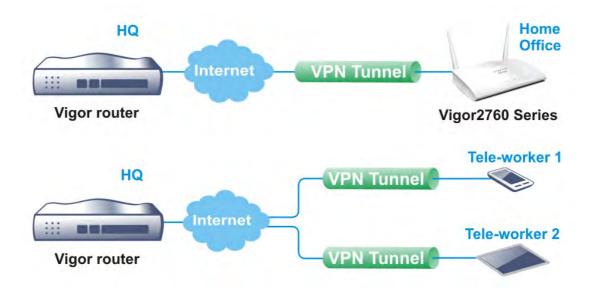
A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is 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

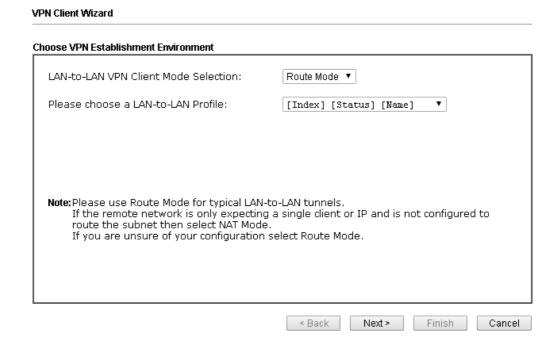


Web User Interface

V-1-1 VPN Client Wizard

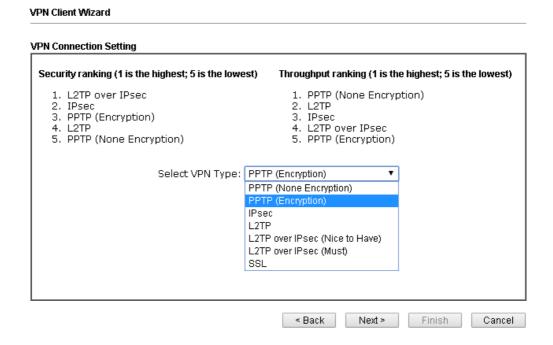
Such wizard is used to configure VPN settings for VPN client. Such wizard will guide to set the LAN-to-LAN profile for VPN dial out connection (from server to client) step by step.

1. Open Wizards>>VPN Client Wizard. The following page will appear.



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. Route Mode NAT Mode
Please choose a LAN-to-LAN Profile	There are 32 VPN profiles for users to set. [Index] [Status] [Name] 1

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



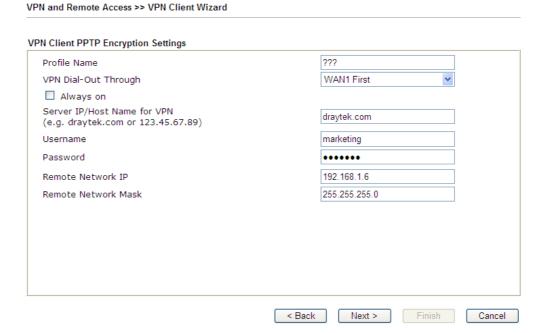
In this page, you have to select suitable VPN type for the VPN client profile. There are six types provided here. Different type will lead to different configuration page. After making the choices for the client profile, please click Next. You will see different configurations based on the selection(s)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



Info

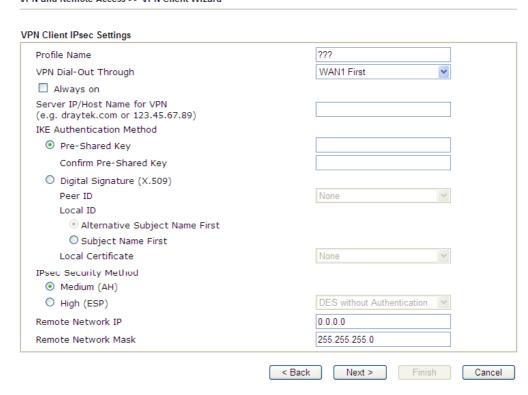
The following descriptions for VPN Type are based on the Route Mode specified in LAN-to-LAN Client Mode Selection.

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



When you choose IPsec, you will see the following graphic:

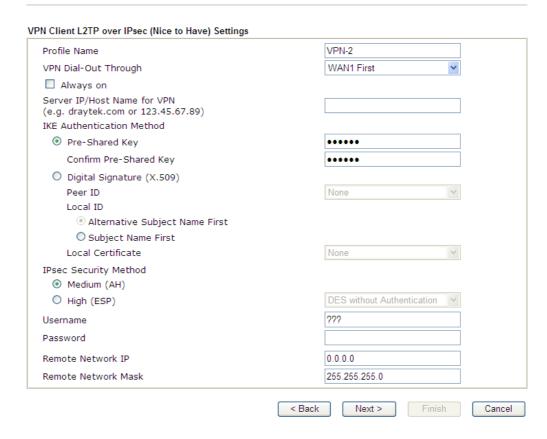
VPN and Remote Access >> VPN Client Wizard



When you choose SSL, you will see the following graphic:

VPN Client Wizard **VPN Connection Setting** Security ranking (1 is the highest; 5 is the lowest) Throughput ranking (1 is the highest; 5 is the lowest) 1. L2TP over IPsec 1. PPTP (None Encryption) 2. IPsec 3. PPTP (Encryption) 4. L2TP 2. L2TP 3. IPsec 4. L2TP over IPsec 5. PPTP (Encryption) 5. PPTP (None Encryption) Select VPN Type: PPTP (Encryption) PPTP (None Encryption) IPsec L2TP L2TP over IPsec (Nice to Have) L2TP over IPsec (Must) SSL < Back Next > Cancel Finish

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



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

???
WAN1 First ▼
WAN1 First
WAN1 Only WAN1 only: Only establish VPN if WAN2 down WAN2 First WAN2 Only WAN2 only: Only establish VPN if WAN1 down LTE First LTE Only WAN4 First WAN4 Only
WAN1 First/ WAN2 First /WAN3 First/WAN4/LTE First-While connecting, the router will use WAN1/WAN2/WAN3/WAN4/LTE as the first channel for VPN connection. If WAN1/WAN2/WAN3/WAN4/LTE fails, the router will use another WAN interface instead.
WAN1 Only /WAN2 Only/WAN3 Only/WAN4/ LTE Only - While connecting, the router will use WAN1/WAN2/WAN3/WAN4/LTE 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.
Check to enable router always keep VPN connection.
Type the IP address of the server or type the host name for such VPN profile.
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.
Click 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.
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.
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.

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 user 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 password is limited to 11 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 type the network mask (according to the real location of the remote host) for building VPN connection.

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

VPN and Remote Access >> VPN Client Wizard

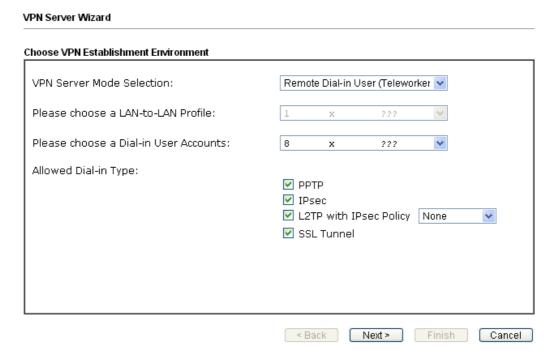
Please confirm your settings LAN-to-LAN Index: 20 Profile Name: VPN-2 VPN Connection Type: L2TP over IPsec (Nice to Have) VPN Dial-Out Through: WAN1 First Always on: Server IP/Host Name: 172.16.3.8 IKE Authentication Method: Pre-Shared Key AH-SHA1 IPsec Security Method: Remote Network IP: 0.0.0.0 Remote 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. O Do another VPN Client Wizard setup. O View more detailed configurations. < Back Next > Finish Cancel

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.

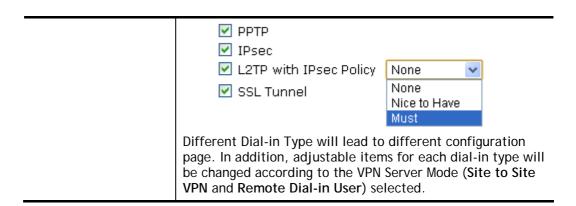
V-1-2 VPN Server Wizard

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.



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).



2. 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/SSL, you will see the following graphic:

VDN Sorver Mitzard

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

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

VPN Server Wizard

VPN Authentication Setting	
Profile Name	???
PPTP / L2TP / L2TP over IPsec / SSL Tunnel Auth	nentication
Username	???
Password	
IPsec / L2TP over IPsec Authentication	
Confirm Pre-Shared Key	
Digital Signature (X.509)	
Peer ID	None ▼
Local ID	
• Alternative Subject Name First	
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
	< Back Next > Finish Cancel

When you check IPsec, you will see the following graphic:

VPN Server Wizard **VPN Authentication Setting** Profile Name 222 IPsec / L2TP over IPsec Authentication ☑ Pre-Shared Key Confirm Pre-Shared Key ☐ Digital Signature (X.509) Peer ID None Local ID Alternative Subject Name First OSubject Name First Peer IP/VPN Client IP Peer ID Site to Site Information Remote Network IP 0.0.0.0 255.255.255.0 Remote Network Mask < Back Next > Finish Cancel

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	Type the pre-shared key again for confirmation.
Digital Signature	Check the box of Digital Signature to invoke this function.
(X.509)	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	Type the WAN IP address or VPN client IP address for the remote client.
Peer ID	Type the ID name for the remote client.
. 661 15	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 type the network mask (according to the real location of the remote host) for building VPN connection.

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

VPN Server Wizard

Please Confirm Your Settings

VPN Environment: Site to Site VPN (LAN-to-LAN) Index: Profile Name: ??? Username: Allowed Service: PPTP+L2TP with IPsec Policy Peer IP/VPN Client IP: Peer ID: 456 Remote Network IP: 172.16.3.56 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	Click this radio button to set another profile of VPN Server

< Back Next > Finish Cancel

Server Wizard Setup	through VPN Server Wizard.
	Click this radio button to access VPN and Remote Access>>LAN to LAN for viewing detailed configuration.
configuration	Access>>LAN to LAN for viewing detailed configuration.

V-1-3 Remote Access Control

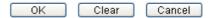
Enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should disable the VPN service of Vigor Router to allow VPN tunnel pass through, as well as the appropriate NAT settings, such as DMZ or open port.

Open VPN and Remote Access>>Remote Access Control.

Remote Access Control Setup

Enable PPTP VPN Service
Enable L2TP VPN Service
Enable SSL VPN Service
Enable SSL VPN Service

Note: To allow VPN pass-through to a separate VPN server on the LAN, disable any services above that use the same protocol and ensure that NAT <u>Open Ports</u> or <u>Port Redirection</u> is also configured.



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

V-1-4 PPP General Setup

VPN and Remote Access >> PPP General Setup

This submenu only applies to PPP-related VPN connections, such as PPTP, L2TP, L2TP over IPsec.

PPP/MP Protocol		PPP Authentication Methods
Dial-In PPP Authentication PAI	P/CHAP/MS-CHAP/MS-CHAPv2 💌	☑ Remote Dial-in User ☑ RADIUS
Dial-In PPP Encryption(MPPE)	tional MPPE	✓ AD/LDAP
Mutual Authentication	(PAP) O Yes 💿 No	PPTP LDAP Profile
Username		▼ TACACS+
Password IP Address Assignment for Dial-In Users		Note: Please select 'PAP Only 'Dial-In PPP Authentication', if you want to use AD/LDAP or TACACS+ for PPP Authentication.
(When DHCP Disable:		TACACO IN TIT Addiction
Assigned IP start LA	•	Note: Default priority is Remote Dial-in User -> RADIUS -> AD/LDAP -> TACACS+.
LA	N 2 192.168.2.250	RADIOS -> AD/LDAP -> TACACS+.
LA	N 3 192.168.3.200	While using Radius or LDAP Authentication: Assign IP from subnet: LAN1
LA	N 4 192.168.4.200	Assign Ir Holl Subhet.
LA	N 5 192.168.5.200	
LA	N 6 192.168.6.200	

Item	Description
Dial-In PPP Authentication	PAP Only - elect this option to force the router to authenticate dial-in users with the PAP protocol. 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.
Dial-In PPP Encryption (MPPE)	Optional MPPE - This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit "no MPPE encrypted packets". Otherwise, the MPPE encryption scheme will be used to encrypt the data. 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	The Mutual Authentication function is mainly used to

(PAP)	communicate with other routers or clients who need bi-directional authentication in order to provide stronger security, for example, Cisco routers. So you should enable this function when your peer router requires mutual authentication. You should further specify the User Name and Password of the mutual authentication peer. The length of the name/password is limited to 23/19 characters.	
Assigned IP Start	Enter a start IP address for the dial-in PPP connection. You should choose an IP address from the local private network. For example, if the local private network is 192.168.1.0/255.255.255.0, you could choose 192.168.1.200 as the Start IP Address. You can configure up to four start IP addresses for LAN1 ~ LAN6.	
PPP Authentication Methods	Select the method(s) to be used for authentication in PPP connection. PPP Authentication Methods Remote Dial-in User RADIUS AD/LDAP	
PPTP LDAP Profile	Configured LDAP profiles will be listed under such item. Simply check the one you want to enable the PPP authentication by LDAP server profiles. However, if there is no profile listed, simply click the link of PPTP LDAP Profile to create/add some new LDAP profiles you want.	
While using Radius or LDAP Authentication	If PPP connection will be authenticated via RADIUS server or LDAP profiles, it is necessary to specify the LAN profile for the dial-in user to get IP from. Assign IP from subnet: LAN1 LAN2 LAN3 LAN4 LAN5 LAN6 DMZ	

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 Setu	ıp
VDN IVE/ID Co Coto	
VPN IKE/IPsec General Setup	TO Client (LAN)
Dial-in Set up for Remote Dial-in users and D	ynamic IP Client (LAN to LAN).
IKE Authentication Method	
Certificate for Dial-in	None 🕶
Pre-Shared Key	
Pre-Shared Key	
Confirm Pre-Shared Key	
IPsec Security Method	
✓ Medium (AH)	
Data will be authentic, but will no	ot be encrypted.
High (ESP) ✓ DES ✓ 3DES	✓ AES
Data will be encrypted and authe	entic.
	OK Cancel

Item	Description
IKE Authentication Method	This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPsec-related VPN connections such as L2TP over IPsec and IPsec tunnel. There are two methods offered by Vigor router for you to authenticate the incoming data coming from remote dial-in user, Certificate (X.509) and Pre-Shared

	Key.
	Certificate for Dial-in -Choose one of the local certificates from the drop down list.
	Pre-Shared Key- Specify a key for IKE authentication.
	Confirm Pre-Shared Key- Retype the characters to confirm the pre-shared key.
	Note: Any packets from the remote dial-in user which does not match the rule defined in VPN and Remote Access>>Remote Dial-In User will be applied with the method specified here.
IPsec Security Method	Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.
	High (ESP) - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

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.

VPN and Remote Access >> IPsec Peer Identity

K509 Peer ID A	ccounts:			Set to Factor	ry Default
Index	Name	Status	Index	Name	Status
<u>1.</u>	???	X	<u>17.</u>	???	X
<u>2.</u>	???	X	<u>18.</u>	???	X
<u>3.</u>	???	X	<u>19.</u>	???	X
<u>4.</u>	???	X	<u>20.</u>	???	X
<u>5.</u>	???	X	<u>21.</u>	???	X
<u>6.</u>	???	X	<u>22.</u>	???	X
<u>7.</u>	???	X	<u>23.</u>	???	X
<u>8.</u>	???	X	<u>24.</u>	???	X
<u>9.</u>	???	X	<u>25.</u>	???	X
<u>10.</u>	???	X	<u>26.</u>	???	X
<u>11.</u>	???	X	<u>27.</u>	???	X
<u>12.</u>	???	X	<u>28.</u>	???	X
<u>13.</u>	???	X	<u>29.</u>	???	X
<u>14.</u>	???	X	<u>30.</u>	???	X
<u>15.</u>	???	X	<u>31.</u>	???	X
<u>16.</u>	???	X	<u>32.</u>	???	X

Item	Description
Set to Factory Default	Click it to clear all indexes.
Index	Click the number below Index to access into the setting page

	of IPsec Peer Identity.
Name	Display the profile name of that index.

Click each index to edit one peer digital certificate. There are three security levels of digital signature authentication: Fill each necessary field to authenticate the remote peer. The following explanation will guide you to fill all the necessary fields.

Profile Index : 4	
Profile Name ???	
☑ Enable this account	
Accept Any Peer ID	
Accept Subject Alternative Name	
Type	Domain Name 🕶
Domain Name	
Accept Subject Name	
Country (C)	
State (ST)	
Location (L)	
Orginization (O)	
Orginization Unit (OU)	
Common Name (CN)	
Email (E)	

Available settings are explained as follows:

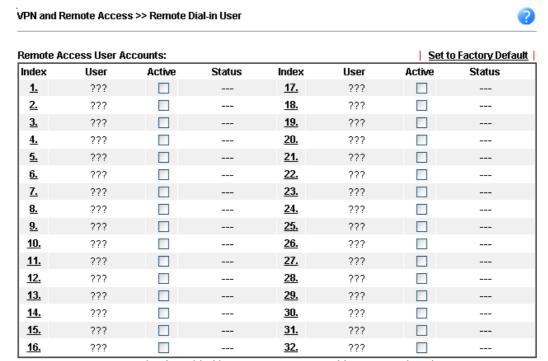
Item	Description
Profile Name	Type the name of the profile. The maximum length of the name you can set is 32 characters.
Enable this account	Check it to enable such account profile.
Accept Any Peer ID	Click to accept any peer regardless of its identity.
Accept Subject Alternative Name	Click to check 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 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.



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

OK Cancel

Available settings are explained as follows:

Item	Description
Set to Factory Default	Click to clear all indexes.
Index	Click the number below Index to access into the setting page of Remote Dial-in User.
User	Display the username for the specific dial-in user of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.
Active	Check the box to activate such profile.
Status	Display the access state of the specific dial-in user. The symbol V and X represent the specific dial-in user to be active and inactive, respectively.

Click each index to edit one remote user profile. Each Dial-In Type requires you to fill the different corresponding fields on the right. If the fields gray out, it means you may leave it untouched. The following explanation will guide you to fill all the necessary fields.

Index No. 1	
User account and Authentication Enable this account Idle Timeout Allowed Dial-In Type	Username ??? Password(Max 19 char) Enable Mobile One-Time Passwords(mOTP) PIN Code Secret
 ✓ PPTP ✓ IPsec Tunnel ✓ L2TP with IPsec Policy None ✓ SSL Tunnel ✓ Specify Remote Node Remote Client IP 	IKE Authentication Method ☑ Pre-Shared Key IKE Pre-Shared Key ☑ Digital Signature(X.509) None ▼
or Peer ID Netbios Naming Packet Pass Block Multicast via VPN Pass Block (for some IGMP,IP-Camera,DHCP Relayetc.)	IPsec Security Method
Subnet LAN 1 ▼ Assign Static IP Address 0.0.0.0	
ОК	Clear Cancel

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.	
Allowed Dial-In Type	PPTP - Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.	
	IPsec Tunnel - Allow the remote dial-in user to make an IPsec VPN connection through Internet.	
	L2TP with IPsec Policy - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below:	
	 None - Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection. 	
	 Nice to Have - Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. 	
	 Must -Specify the IPsec policy to be definitely applied on the L2TP connection. 	
	SSL Tunnel - Allow the remote dial-in user to make an SSL VPN connection through Internet.	
	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).	
	Uncheck the checkbox means the connection type you select above will apply the authentication methods and security	

methods in the general settings. Netbios Naming Packet -Pass - Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. Block - When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel. Multicast via VPN - Some programs might send multicast packets via VPN connection. Pass - Click this button to let multicast packets pass through the router. Block - This is default setting. Click this button to let multicast packets be blocked by the router. 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. 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. Enable Mobile One-Time Passwords (mOTP) - Check this box to make the authentication with mOTP function. PIN Code - Type the code for authentication (e.g., 1234). Secret - Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6). 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** This group of fields is applicable for IPsec Tunnels and L2TP Method 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. This group of fields is a must for IPsec Tunnels and L2TP with **IPsec Security Method** 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.

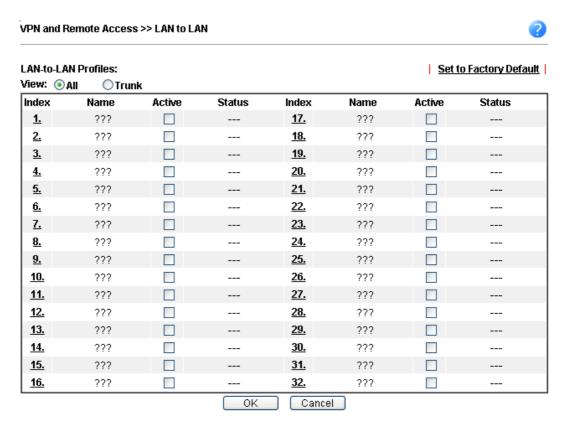
After finishing all the settings here, please click **OK** to save the configuration.

V-1-8 LAN to LAN

Here you can manage LAN-to-LAN connections by maintaining a table of connection profiles. You may set parameters including specified connection direction (dial-in or dial-out), connection peer ID, connection type (VPN connection - including PPTP, IPsec Tunnel, and L2TP by itself or over IPsec) and corresponding security methods, etc.

The router supports up to 32 VPN tunnels simultaneously. The following figure shows the summary table.

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



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

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

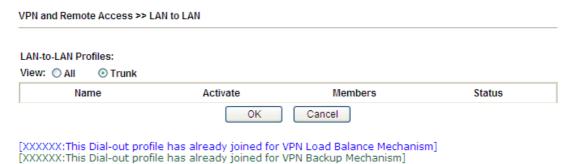
[XXXXXX:This Dial-out profile does not join for VPN TRUNK]

The following shows profiles joined into VPN Load Balance and VPN Backup mechanism.



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

If there is no profile joined yet, this page will be shown as follows:



Available settings are explained as follows:

Item	Description
View	All - Click it to display the LAN to LAN profiles. Trunk - Click it to display the Trunk profiles.
Set to Factory Default	Click to clear all indexes.
Name	Indicate the name of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.
Active	V - means the profile has been enabled. X - means the profile has not been enabled.
Status	Indicate the status of individual profiles. The symbol V and X represent the profile to be active and inactive, respectively.

To edit each profile:

1. Click each index to edit each profile and you will get the following page. Each LAN-to-LAN profile includes 4 subgroups. If the fields gray out, it means you may leave it untouched. The following explanations will guide you to fill all the necessary fields.

Profile Index: 1 1. Common Settings Profile Name Call Direction ○ Both ● Dial-Out ○ Dial-in toHuko Always on Enable this profile Idle Timeout second(s) VPN Dial-Out Through Enable PING to keep IPsec tunnel alive PING to the IP WAN1 First Netbios Naming Packet Pass Block (for some IGMP,IP-Camera,DHCP Relay..etc.) 2. Dial-Out Settings Type of Server I am calling Username rd6_draytek ○ PPTP Password(Max 15 char) IPsec Tunnel PPP Authentication PAP/CHAP/MS-CHAP/MS-CHAPv2 ▼ L2TP with IPsec Policy None VJ Compression SSL Tunnel ● On ○ Off Server IP/Host Name for VPN. IKE Authentication Method (such as draytek.com or 123.45.67.89) Pre-Shared Key vpn.draytek.com IKE Pre-Shared Key Server Port (for SSL Tunnel): 443 Digital Signature(X.509) Peer ID None Local ID Alternative Subject Name First Subject Name First Local Certificate None • IPsec Security Method Medium(AH) High(ESP) 3DES with Authentication Advanced Index(1-15) in Schedule Setup:

Item	Description	
Common Settings	Profile Name - Specify a name for the profile of the LAN-to-LAN connection.	
	Enable this profile - Check here to activate this profile.	
	VPN Dial-Out Through - Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only.	
	 WAN1 First/ WAN2 First/ WAN3 First /WAN4/LTE First- While connecting, the router will use WAN1/WAN2/WAN3/WAN4/LTE as the first channel for VPN connection. If WAN1/WAN2/WAN3/WAN4/LTE fails, the router will use another WAN interface instead. 	
	 WAN1 Only /WAN2 Only/WAN 3 Only/WAN 4/LTE Only- While connecting, the router will use WAN1/WAN2/WAN3/WAN4/LTE 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.

Netbios Naming Packet

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

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

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

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

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

Always On-Check to enable router always keep VPN connection.

Idle Timeout: The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.

Enable PING to keep alive - This function is to help the router to determine the status of IPsec VPN connection, especially useful in the case of abnormal VPN IPsec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address.

Enable PING to keep alive is used to handle abnormal IPsec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial. Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer 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).

PING to the IP - Enter the IP address of the remote host that located at the other-end of the VPN tunnel.

Dial-Out Settings

Type of Server I am calling - PPTP - Build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server.

 $\ensuremath{\mathsf{IPsec}}$ Tunnel - Build an $\ensuremath{\mathsf{IPsec}}$ VPN connection to the server through Internet.

L2TP with IPsec Policy - Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below:

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.

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 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.

Index(1-15) - Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in Applications >> Schedule setup. The default setting of this field is blank and the function will always work.

3. Dial-In Settings

Allowed Dial-In Type		Usern	ame	???
		Passw	ord(Max 11 char)	
		VJ Cor	mpression	● On ○ Off
🗷 L2TP with IPsec Poli	cy None ▼		U4! B.O -4! J	
✓ SSL Tunnel			thentication Method -Shared Kev	
Specify Remote VPN Gateway Peer VPN Server IP		IKE Pi	re-Shared Key gital Signature(X.50	09)
- Board ID			 cal ID	
or Peer ID) Alternative Subje) Subject Name Firs	
		IPsec 9	Security Method	
		Me	dium(AH)	
		High(E	SP) 🕜 DES 🗹	3DES ₪ AES
4. GRE Settings				
	function GRE over IPsec			
■ Logical Traffic My GRE IP			Peer GRE IP	
5. TCP/IP Network Settings				
My WAN IP	0.0.0.0	RIP Di	rection	Disable ▼
Remote Gateway IP	0.0.0.0		irst subnet to rem	ote network, you have
Remote Network IP	172.16.2.0	to do		Davida 🔻
Remote Network Mask	255.255.255.0		umu idad o	Route •
Local Network IP	172.17.11.0	U IPS	sec VPN with the S	ame Subnets
Local Network Mask	255.255.255.0	 □ ch	ange default route	e to this VPN tunnel (
	More		ingle WAN support	,
	OK CI	ear	Cancel	

Item	Description	
Dial-In Settings	Allowed Dial-In Type - Determine the dial-in connection with different types.	
	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: 	
	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.	

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 methods on the right side.

If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings.

Username - 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.

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.

VJ Compression - VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select PPTP or L2TP with or without IPsec policy above.

IKE Authentication Method - This group of fields is applicable for IPsec Tunnels and L2TP with IPsec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPsec tunnel either with or without specify the IP address of the remote node.

- 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.
 - 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.

IPsec Security Method - This group of fields is a must for IPsec Tunnels and L2TP with IPsec Policy when you specify the remote node.

- Medium- Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.
- High- Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

GRE over IPsec Settings

Enable IPsec Dial-Out function GRE over IPsec: Check this box to verify data and transmit data in encryption with GRE over IPsec packet after configuring IPsec Dial-Out setting. Both ends must match for each other by setting same virtual IP address for communication.

Logical Traffic: Such technique comes from RFC2890. Define logical traffic for data transmission between both sides of

VPN tunnel by using the characteristic of GRE. Even hacker can decipher IPsec encryption, he/she still cannot ask LAN site to do data transmission with any information. Such function can ensure the data transmitted on VPN tunnel is really sent out from both sides. This is an optional function. However, if one side wants to use it, the peer must enable it, too.

My GRE IP: Type the virtual IP for router itself for verified by peer.

Peer GRE IP: Type the virtual IP of peer host for verified by router.

TCP/IP Network Settings

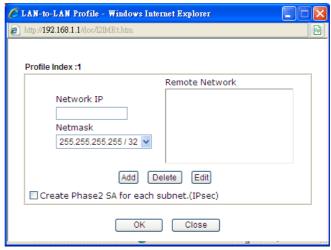
My WAN IP -This field is only applicable when you select PPTP or L2TP with or without IPsec policy above. The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.

Remote Gateway IP - This field is only applicable when you select PPTP or L2TP with or without IPsec policy above. The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.

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.



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.

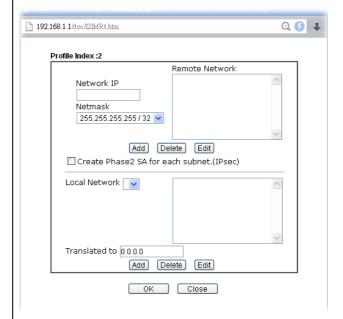
After checking the box of IPSec VPN with the Same subnet, the options under TCP/IP Network Settings will be changed as shown below:



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.

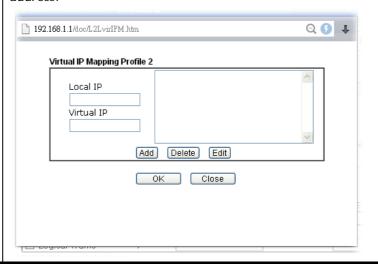
Advanced - Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.



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.



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

V-1-9 VPN Trunk Management

VPN trunk includes four features - VPN Backup, VPN load balance, GRE over IPsec, and Binding tunnel policy.

Features of VPN TRUNK — VPN Backup Mechanism

VPN TRUNK Management is a backup mechanism which can set multiple VPN tunnels as backup tunnel. It can assure the network connection not to be cut off due to network environment blocked by any reason.

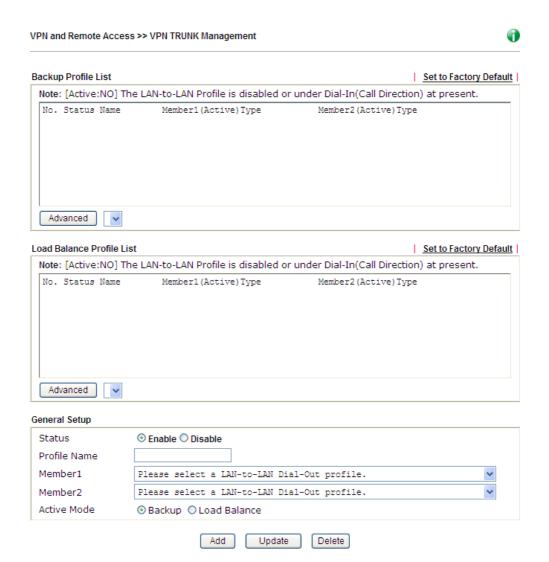
- VPN TRUNK-VPN Backup mechanism can judge abnormal situation for the environment of VPN server and correct it to complete the backup of VPN Tunnel in real-time.
- VPN TRUNK-VPN Backup mechanism is compliant with all WAN modes (single/multi)
- Dial-out connection types contain IPsec, PPTP, L2TP, L2TP over IPsec and ISDN (depends on hardware specification)
- The web page is simple to understand and easy to configure
- Fully compliant with VPN Server LAN Site Single/Multi Network
- Mail Alert support, please refer to System Maintenance >> SysLog / Mail Alert for detailed configuration
- Syslog support, please refer to System Maintenance >> SysLog / Mail Alert for detailed configuration
- Specific ERD (Environment Recovery Detection) mechanism which can be operated by using Telnet command

VPN TRUNK-VPN Backup mechanism profile will be activated when initial connection of single VPN tunnel is off-line. Before setting VPN TRUNK -VPN Backup mechanism backup profile, please configure at least two sets of LAN-to-LAN profiles (with fully configured dial-out settings) first, otherwise you will not have selections for grouping Member1 and Member2.

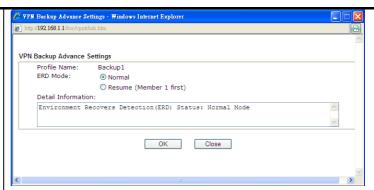
Features of VPN TRUNK — VPN Load Balance Mechanism

VPN Load Balance Mechanism can set multiple VPN tunnels for using as traffic load balance tunnel. It can assist users to do effective load sharing for multiple VPN tunnels according to real line bandwidth. Moreover, it offers three types of algorithms for load balancing and binding tunnel policy mechanism to let the administrator manage the network more flexibly.

- Three types of load sharing algorithm offered, Round Robin, Weighted Round Robin and Fastest
- Binding Tunnel Policy mechanism allows users to encrypt the data in transmission or specified service function in transmission and define specified VPN Tunnel for having effective bandwidth management
- Dial-out connection types contain IPsec, PPTP, L2TP, L2TP over IPsec and GRE over IPsec
- The web page is simple to understand and easy to configure
- The TCP Session transmitted by using VPN TRUNK-VPN Load Balance mechanism will not be lost due to one of VPN Tunnels disconnected. Users do not need to reconnect with setting TCP/UDP Service Port again. The VPN Load Balance function can keep the transmission for internal data on tunnel stably



Item	Description
Backup Profile List	Set to Factory Default - Click to clear all VPN TRUNK-VPN Backup mechanism profile.
	No - The order of VPN TRUNK-VPN Backup mechanism profile.
	Status - "v" means such profile is enabled; "x" means such profile is disabled.
	Name - Display the name of VPN TRUNK-VPN Backup mechanism profile.
	Member1 - Display the dial-out profile selected from the Member1 drop down list below.
	Active - "Yes" means normal condition. "No" means the state might be disabled or that profile currently is set with Dial-in mode (for call direction) in LAN-to-LAN.
	Type - Display the connection type for that profile, such as IPsec, PPTP, L2TP, L2TP over IPsec (NICE), L2TP over IPsec(MUST) and so on.
	Member2 - Display the dial-out profile selected from the Member2 drop down list below.
	Advanced - This button is available only when LAN to LAN profile (or more) is created.



Detailed information for this dialog, see later section - Advanced Load Balance and Backup.

Load Balance Profile List

Set to Factory Default - Click to clear all VPN TRUNK-VPN Load Balance mechanism profile.

No - The order of VPN TRUNK-VPN Load Balance mechanism profile.

Status - "v" means such profile is enabled; "x" means such profile is disabled.

Name - Display the name of VPN TRUNK-VPN Load Balance mechanism profile.

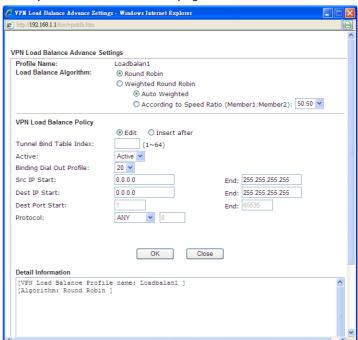
Member1 - Display the dial-out profile selected from the Member1 drop down list below.

Active - "Yes" means normal condition. "No" means the state might be disabled or that profile currently is set with Dial-in mode (for call direction) in LAN-to-LAN.

Type - Display the connection type for that profile, such as IPsec, PPTP, L2TP, L2TP over IPsec (NICE), L2TP over IPsec (MUST) and so on.

Member2 - Display the dial-out profile selected from the Member2 drop down list below.

Advanced - This button is only available when there is one or more profiles created in this page.



Detailed information for this dialog, see later section - Advanced Load Balance and Backup.

General Setup

Status- After choosing one of the profile listed above, please click Enable to activate this profile. If you click Disable, the selected or current used VPN TRUNK-Backup/Load Balance mechanism profile will not have any effect for VPN tunnel.

Profile Name- Type a name for VPN TRUNK profile. Each profile can group two VPN connections set in LAN-to-LAN. The saved VPN profiles in LAN-to-LAN will be shown on Member1 and Member2 fields. The length of the name is limited to 11 characters.

Member 1/Member2 - Display the selection for LAN-to-LAN dial-out profiles (configured in VPN and Remote Access >> LAN-to-LAN) for you to choose for grouping under certain VPN TRUNK-VPN Backup/Load Balance mechanism profile.

- No Index number of LAN-to-LAN dial-out profile.
- Name Profile name of LAN-to-LAN dial-out profile.
- Connection Type Connection type of LAN-to-LAN dial-out profile.
- VPN ServerIP (Private Network) VPN Server IP of LAN-to-LAN dial-out profiles.

Active Mode - Display available mode for you to choose. Choose Backup or Load Balance for your router.

Add - Add and save new profile to the backup profile list. The corresponding members (LAN-to-LAN profiles) grouped in such new VPN TRUNK - VPN Backup mechanism profile will be locked. The profiles in LAN-to-LAN will be displayed in red. VPN TRUNK - VPN Load Balance mechanism profile will be locked. The profiles in LAN-to-LAN will be displayed in blue

Update - Click this button to save the changes to the **Status** (Enable or Disable), profile name, member1 or member2.

Delete - Click this button to delete the selected VPN TRUNK profile. The corresponding members (LAN-to-LAN profiles) grouped in the deleted VPN TRUNK profile will be released and that profiles in LAN-to-LAN will be displayed in black.

Time for activating VPN TRUNK — VPN Backup mechanism profile

VPN TRUNK - VPN Backup mechanism will be activated automatically after the initial connection of single VPN Tunnel off-line. The content in Member1/2 within VPN TRUNK - VPN Backup mechanism backup profile is similar to dial-out profile configured in LAN-to-LAN web page. VPN TRUNK - VPN Backup mechanism backup profile will process and handle everything unless it is off-line once it is activated.

Time for activating VPN TRUNK — VPN Load Balance mechanism profile

After finishing the connection for one tunnel, the other tunnel will dial out automatically within two seconds. Therefore, you can choose any one of members under VPN Load Balance for dialing out.

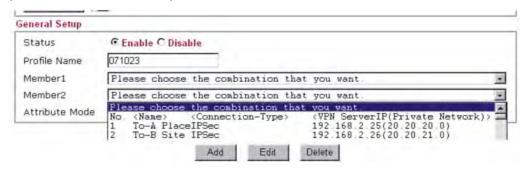
Time for activating VPN TRUNK —Dial-out when VPN Load Balance Disconnected

For there is one Tunnel created and connected successfully, to keep the load balance effect between two tunnels, auto-dial will be executed within two seconds.

To close two tunnels of load balance after connecting, please click **Disable** for **Status** in **General Setup** field.

How can you set a VPN TRUNK-VPN Backup/Load Balance mechanism profile?

- First of all, go to VPN and Remote Access>>LAN-to-LAN. Set two or more LAN-to-LAN profiles first that will be used for Member1 and Member2. If you do not set enough LAN-to-LAN profiles, you cannot operate VPN TRUNK VPN Backup /Load Balance mechanism profile management well.
- Access into VPN and Remote Access>>VPN TRUNK Management.
- 3. Set one group of VPN TRUNK VPN Backup/Load Balance mechanism backup profile by choosing Enable radio button; type a name for such profile (e.g., 071023); choose one of the LAN-to-LAN profiles from Member1 drop down list; choose one of the LAN-to-LAN profiles from Member2 drop down list; and click Add at last.



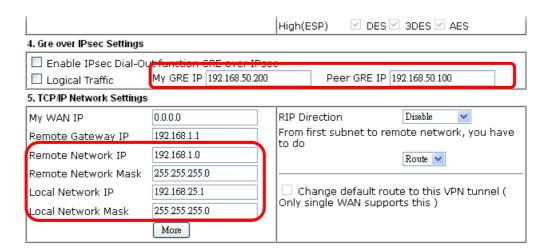
4. Take a look for LAN-to-LAN profiles. Index 1 is chosen as Member1; index 2 is chosen as Member2. For such reason, LAN-to-LAN profiles of 1 and 2 will be expressed in red to indicate that they are fixed. If you delete the VPN TRUNK - VPN Backup/Load Balance mechanism profile, the selected LAN-to-LAN profiles will be released and expressed in black.

LAN-to-LAN Profiles:

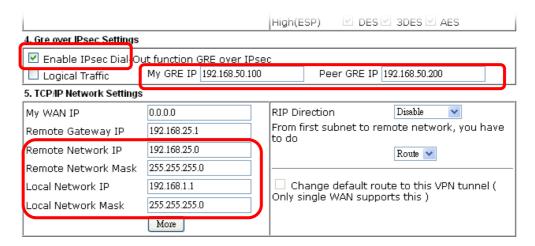


How can you set a GRE over IPsec profile?

- 1. Please go to LAN to LAN to set a profile with IPsec.
- If the router will be used as the VPN Server (i.e., with virtual address 192.168.50.200).
 Please type 192.168.50.200 in the field of My GRE IP. Type IP address (192.168.50.100) of the client in the field of Peer GRE IP. See the following graphic for an example.



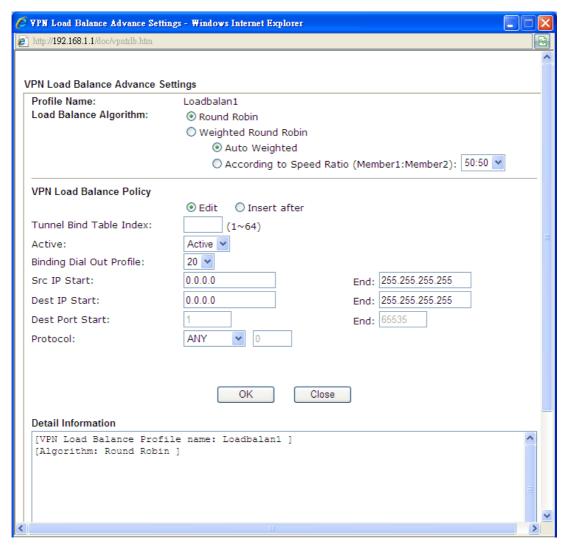
3. Later, on peer side (as VPN Client): please type 192.168.50.100 in the field of My GRE IP and type IP address of the server (192.168.50.200) in the field of Peer GRE IP.



Advanced Load Balance and Backup

After setting profiles for load balance, you can choose any one of them and click Advance for more detailed configuration. The windows for advanced load balance and backup are different. Refer to the following explanation:

Advanced Load Balance



Item	Description
Profile Name	List the load balance profile name.
Load Balance Algorithm	Round Robin - Based on packet base, both tunnels will send the packet alternatively. Such method can reach the balance of packet transmission with fixed rate.
	Weighted Round Robin -Such method can reach the balance of packet transmission with flexible rate. It can be divided into Auto Weighted and According to Speed Ratio. Auto Weighted can detect the device speed (10Mbps/100Mbps) and switch with fixed value ratio (3:7) for packet transmission. If the transmission rate for packets on both sides of the tunnels is the same, the value of Auto Weighted should be 5.5. According to Speed Ratio allows user to adjust suitable rate manually. There are 100 groups of rate ratio for Member1:Member2 (range from 1:99 to 99:1).
VPN Load Balance Policy	Below shows the algorithm for Load Balance.
	Edit - Click this radio button for assign a blank table for configuring Binding Tunnel.
	Insert after - Click this radio button to adding a new binding tunnel table.

Tunnel Bind Table Index- 128 Binding tunnel tables are provided by this device. Specify the number of the tunnel for such Load Balance profile.

Active - In-active/Delete can delete this binding tunnel table. Active can activate this binding tunnel table.

Binding Dial Out Index - Specify connection type for transmission by choosing the index (LAN to LAN Profile Index) for such binding tunnel table.

Scr IP Start /End- Specify source IP addresses as starting point and ending point.

Dest IP Start/End - Specify destination IP addresses as starting point and ending point.

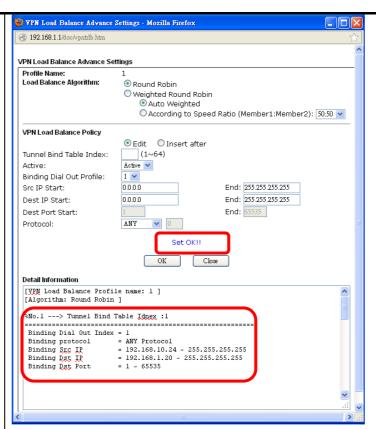
Dest Port Start /End- Specify destination service port as starting point and ending point.

Protocol - Any means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here, such binding tunnel table can be established for TCP Service Port/UDP Service Port/ICMP/IGMP specified here.

TCP means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and TCP Service Port also fits the number here, such binding tunnel table can be established. UDP means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and UDP Service Port also fits the number here, such binding tunnel table can be established. TCP/UPD means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and TCP/UDP Service Port also fits the number here, such binding tunnel table can be established. ICMP means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and ICMP Service Port also fits the number here, such binding tunnel table can be established. IGMP means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and IGMP Service Port also fits the number here, such binding tunnel table can be established. Other means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here with different TCP Service Port/UDP Service Port/ICMP/IGMP, such binding tunnel table can be established.

Detail Information

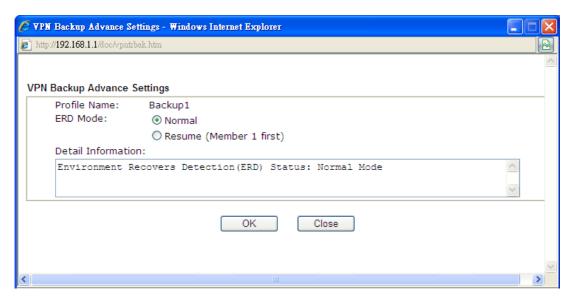
This field will display detailed information for Binding Tunnel Policy. Below shows a successful binding tunnel policy for load balance:



To configure a successful binding tunnel, you have to:

Type Binding Src IP range (Start and End) and Binding Des IP range (Start and End). Choose TCP/UDP, IGMP/ICMP or Other as Binding Protocol.

Advanced Backup

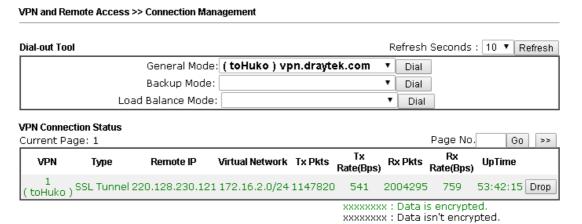


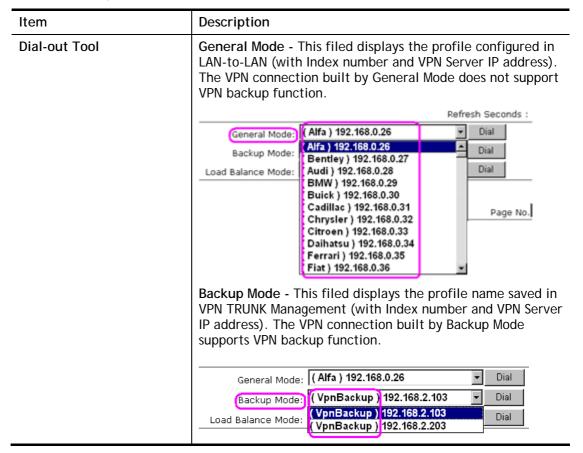
Item	Description	
Profile Name	List the backup profile name.	
ERD Mode	ERD means "Environment Recovers Detection".	
	Normal - choose this mode to make all dial-out VPN TRUNK	

	backup profiles being activated alternatively. Resume - when VPN connection breaks down or disconnects, Member 1 will be the top priority for the system to do VPN connection.
Detail Information	This field will display detailed information for Environment Recovers Detection.

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.





Dial - Click this button to execute dial out function.
Refresh Seconds - Choose the time for refresh the dial information among 5, 10, and 30.
Refresh - Click this button to refresh the whole connection status.

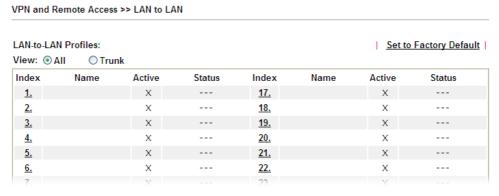
Application Notes

A-1 How to Build a LAN-to-LAN VPN Between Remote Office and Headquarter via IPsec Tunnel (Main Mode)

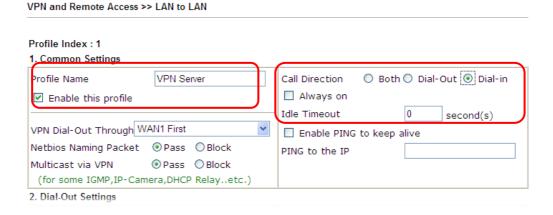


Configuration on Vigor Router for Head Office

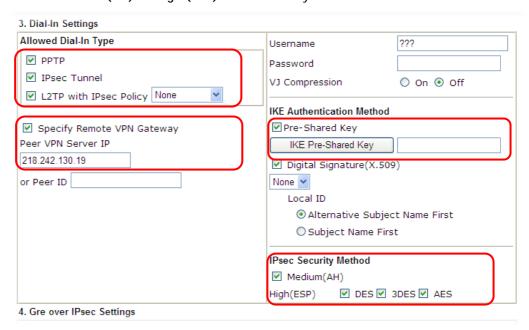
- 1. Log into the web user interface of Vigor router.
- 2. Open VPN and Remote Access>>LAN to LAN to create a LAN-to-LAN profile. The following settings are for a permanent VPN connection.



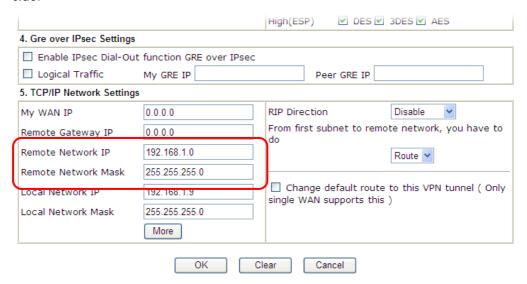
3. Click any index number to open the configuration page. Type a name which is easy for identification for such profile (in this case, type *VPN Server*), and check the box of **Enable This Profile**. For Vigor router will be set as a **server**, the call direction shall be set as **Dial-in** and set 0 as **Idle Timeout**.



4. Now navigate to the next section, Dial-In Settings to check PPTP, IPsec Tunnel and L2TP boxes. Check the box of Specify Remote... and type the Peer VPN Server IP (e.g., 218.242.130.19 in this case). Press the IKE Pre-Shared Key button to set the PSK; and select Medium (AH) or High (ESP) as the security method.



5. Continue to navigate to the TCP/IP Network Settings for setting the LAN IP for remote side.



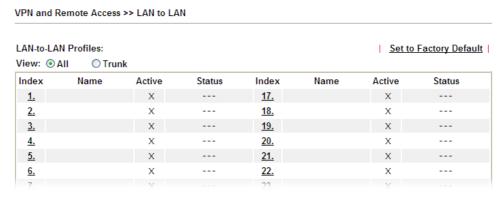
- 6. Click **OK** to save the settings.
- 7. Open VPN and Remote Access>>Connection Management to check the dial-in connection status (from branch office).



xxxxxxxx : Data isn't encrypteu.

Configuration on Vigor Router for Branch Office

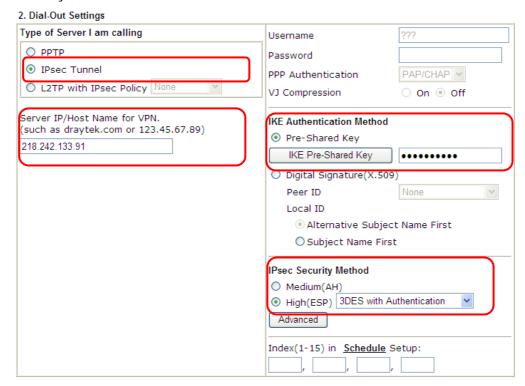
- Log into the web user interface of Vigor router. 1.
- 2. Open VPN and Remote Access>>LAN to LAN to create a LAN-to-LAN profile. The following settings are for a permanent VPN connection.



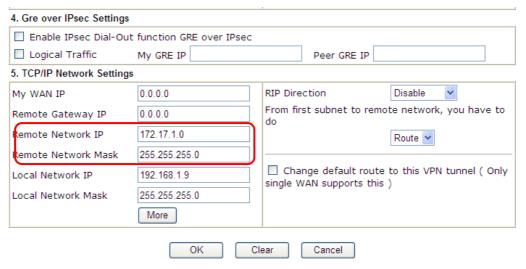
Click any index number to open the configuration page. Type a name which is easy for 3. identification for such profile (in this case, type VPN Client), and check the box of Enable This Profile. For such Vigor router will be set as a client, the call direction shall be set as Dial-out. Check the box of Always on for a permanent VPN connection.



4. Now navigate to the next section, Dial-Out Settings to select the IPsec Tunnel service and type the remote server IP/host name (e.g., 218.242.133.91, in this case). Press the IKE Pre-Shared Key button to set the PSK; and select Medium (AH) or High (ESP) as the security method.



5. Continue to navigate to the TCP/IP Network Settings for setting the LAN IP for the remote side.



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

7. Open VPN and Remote Access>>Connection Management to check the dial-in connection status (from head office).



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.

SSL VPN
General Setup
SSL Web Proxy
SSL Application
User Account
User Group
Online User Status

Web User Interface

V-2-1 General Setup

This page determines the general configuration for SSL VPN Server and SSL Tunnel.

SSL VPN >> General Setup	
SSL VPN General Setup	
Port	443 (Default: 443)
Server Certificate	self-signed 💌

Note: The settings will act on all SSL applications.

Please go to $\underline{\text{System Maintenance}} > \underline{\text{Management}}$ to enable SSLv3.0 .



Available settings are explained as follows:

Item	Description
Port	Such port is set for SSL VPN server. It will not affect the HTTPS Port configuration set in System Maintenance>>Management . In general, the default setting is 443.
Server Certificate	When the client does not set any certificate, default certificate will be used for HTTPS and SSL VPN server. Choose any one of the user-defined certificates from the drop down list if users set several certificates previously. Otherwise, choose Self-signed to use the router's built-in default certificate. The default certificate can be used in SSL VPN server and HTTPS Web Proxy.

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

V-2-2 SSL Web Proxy

SSL Web Proxy will allow the remote users to access the internal web sites over SSL.

SSL VPN >> SSL Web Proxy

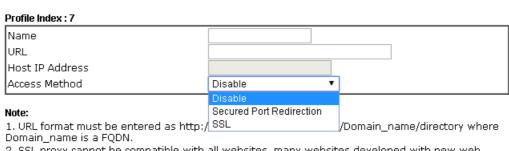
SSL Web Prox	y Servers Profiles:	<u> </u>	Set to Factory Default
Index	Name	URL	Active
<u>1.</u>			Х
<u>2.</u>			X
<u>3.</u>			X
<u>4.</u>			X
<u>5.</u>			X
<u>6.</u>			X
<u>7.</u>			X
<u>8.</u>			X
<u>9.</u>			X
10.			X

Each item is explained as follows:

Item	Description
Name	Display the name of the profile that you create.
URL	Display the URL.
Active	Display current status (active or inactive) of such profile.

Click number link under Index filed to set detailed configuration.

SSL VPN >> SSL Web Proxy



2. SSL proxy cannot be compatible with all websites, many websites developed with new web coding technology may not work with proxy mode. We suggest using SSL Tunnel when SSL proxy is not working.



Item	Description
Name	Type name of the profile. The length of the name is limited to 15 characters.
URL	Type the address (function variation or IP address) or path of the proxy server.
Host IP Address	If you type function variation as URL, you have to type corresponding IP address in this filed. Such field must match with URL setting.

Access Method

There are three modes for you to choose.

Disable - the profile will be inactive. If you choose **Disable**, all the web proxy profile appeared under VPN remote dial-in web page will disappear.

Secured Port Redirection - such technique applies private port mapping to random WAN port. There are two restrictions for proxy web server for such selection: 1) it is only used for WAN to LAN access, the web server must be configured behind vigor router; 2) web server gateway must be indicated to vigor router. In addition, users must execute "Connect" manually in SSL Client Portal page.

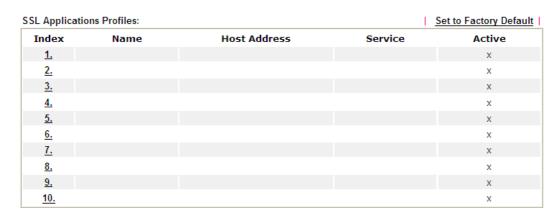
 $\ensuremath{\mathsf{SSL}}$ - if you choose such selection, web proxy over SSL will be applied for VPN.

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

V-2-3 SSL Application

It provides a secure and flexible solution for network resources, including VNC (Virtual Network Computer) /RDP (Remote Desktop Protocol) /SMB, to any remote user with access to Internet and a web browser.

SSL VPN >> SSL Application



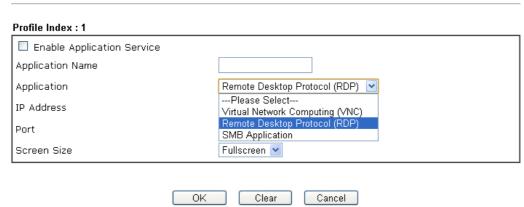
Each item is explained as follows:

Item	Description
Name	Display the application name of the profile that you create.
Host Address	Display the IP address for VNC/RDP or SMB path.
Service	Display the type of the service selected, e.g., VNC/RDP/SMB.
Active	Display current status (active or inactive) of the selected profile.

To create a new SSL application profile:

- 1. Click number link under Index filed to set detailed configuration.
- 2. The following page will appear.

SSL VPN >> SSL Application



Item	Description
Enable Application	Check the box to enable such profile.

Server	
Application Name	Type a name for such application. The length of the name is limited to 23 characters.
Application	There are three types offered for you to create an application profile.
	Virtual Network Computing (VNC) - It allows you to access and control a remote PC through VNC protocol.
	Remote Desktop Protocol (RDP) - It allows you to access and control a remote PC through RDP protocol.
	SMB Application - It allows you to access and control a remote PC through SMB service.
IP Address	If you choose VNC or RDP, you have to type the IP address for this protocol.
Port	If you choose VNC or RDP, you have to specify the port used for this protocol. The default setting is 5900.
Idle Timeout	If you choose VNC, you have to specify the time for disconnecting the SSL VPN tunnel.
Scaling	If you choose VNC, you have to choose the percentage (100%, 80%, 60%) for such application.
Screen Size	If you choose RDP, you have to choose the screen size for such application.
SMB Path	If you choose SMB, you have to specify the path of the SMB service.

- 3. Enter the required information.
- 4. After finished the above settings, click \mathbf{OK} to save the configuration.

SSL VPN >> SSL Application

SL Applicatio	ns Profiles:		1	Set to Factory Default
Index	Name	Host Address	Service	Active
<u>1.</u>	VNC_1	192.168.1.51:5900	VNC	V
<u>2.</u>				Х
<u>3.</u>				X

V-2-4 User Account

With SSL VPN, Vigor2860 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, Vigor2860 series allows up to 16 simultaneous incoming users.

For SSL VPN, identity authentication and power management are implemented through deploying user accounts. Therefore, the user account for SSL VPN must be set together with remote dial-in user web page. Such menu item will guide to access into VPN and Remote Access>>Remote Dial-in user.

SSL VPN >> Remote Dial-in User

Index	User	Active	Status	Index	User	Active	Status
<u>1.</u>	???	Ш		<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>	???		

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



Click each index to edit one remote user profile.

SSL VPN >> Remote Dial-in User

User account and Authentication	Username	???
Enable this account	Password(Max 19 char)	
Idle Timeout 300 second(s)	☐ Enable Mobile One-Tim	e Passwords(mOTP)
Allowed Dial-In Type	PIN Code	
✓ PPTP	Secret	<u> </u>
☑ IPsec Tunnel		
☑ L2TP with IPsec Policy None ☑	IKE Authentication Method	
✓ SSL Tunnel	✓ Pre-Shared Key	
	IKE Pre-Shared Key	
Specify Remote Node	Digital Signature(X.509))
Remote Client IP	None 🐣	
	IPsec Security Method	
or Peer ID	✓ Medium(AH)	
Netbios Naming Packet Pass Block		BDES 🗹 AES
Multicast via VPN Pass • Block	Local ID (optional)	
(for some IGMP,IP-Camera,DHCP Relayetc.)		
Subnet		
LAN 1 🕶		
Assign Static IP Address		
0.0.0.0		

Item	Description
User account and	Enable this account - Check the box to enable this function.
Authentication	Idle Timeout- If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.
	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.
	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.
	Enable Mobile One-Time Passwords (mOTP) - Check this box to make the authentication with mOTP function.
	PIN Code - Type the code for authentication (e.g, 1234).
	Secret - Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).
Allowed Dial-In Type	PPTP - Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.
	IPSec Tunnel - Allow the remote dial-in user to make an IPSec VPN connection through Internet.
	L2TP with IPSec Policy - Allow the remote dial-in user to

Item	Description	
	make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below:	
	 None - Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. 	
	 Nice to Have - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VP connection becomes one pure L2TP connection. 	
	Must -Specify the IPSec policy to be definitely applied on the L2TP connection.	
	SSL Tunnel - It allows the remote dial-in user to make an SSL VPN Tunnel connection through Internet, suitable for the application through network accessing (e.g., PPTP/L2TP/IPSec)	
	If you check this box, the function of SSL Tunnel for this account will be activated immediately.	
	Specify Remote Node - Check the checkbox to specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode). If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings.	
	Netbios Naming Packet	
	 Pass - Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. 	
	 Block - When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel. 	
	Multicast via VPN - Some programs might send multicast packets via VPN connection.	
	 Pass - Click this button to let multicast packets pass through the router. 	
	Block - This is default setting. Click this button to let multicast packets be blocked by the router.	
Subnet	Chose one of the subnet selections for such VPN profile.	
	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 specify the IP address of the remote node.	
	Pre-Shared Key - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key.	
	Digital Signature (X.509) - Check the box of Digital Signature to invoke this function and Select one 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.	

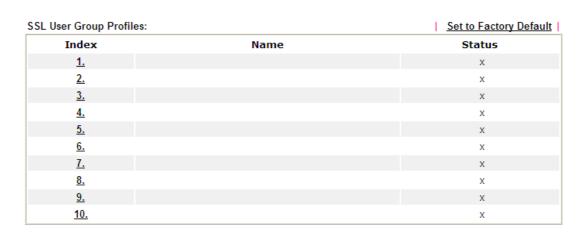
Item	Description
	Medium-Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it.
	High-Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
	Local ID - Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.

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

V-2-5 User Group

There are 10 user group profiles which can be created for authentication by LDAP server. Such profiles will be used by applications such as User Management, VPN and etc.

SSL VPN >> User Group



Each item is explained as follows:

Item	Description
Set to Factory Default	Click to clear all indexes.
Index	Display the number of the client which connecting to FTP server.
Name	Display the name of the group profile.

Click any index number link to open the following page for detailed configuration.

SSL VPN >> User Group Index No. 10 Enable **Group Name Access Authority** SSL Web Proxy SSL Application **Authentication Methods** Local User DataBase Available User Accounts Selected User Accounts 1-alpha_huang 2-dni >> _ · · · RADIUS ■ TACACS+ LDAP / Active Directory ΟK Clear Cancel

Available settings are explained as follows:

Item	Description	
Enable	Check this box to enable such profile.	
Group Name	Type a name for such profile. The length of the name is limited to 23 characters.	
Access Authority	Specify the authority for such profile. At present, Vigor router allows you to create SSL Web Proxy and SSL Application profiles used for SSL VPN. The available profiles will be displayed here for you to select. Access Authority SSL Web Proxy Game_APP	
Authentication Methods	It can determine the authentication method used for such profile. Local User DataBase - The system will do the authentication by using the user defined account profiles (in VPN and Remote Access>>Remote Dial-In User). The enabled profiles will be listed in the Available User Account on the left box. To add a profile into a group, simply choose the one from the left box and click the >> button. It will be displayed in the Selected User Account on the right box. For detailed information about configuring the profile setting, refer to Objects Setting>>IP Group. RADIUS - The RADIUS server will do the authentication by using the username and password TACACS+ - The TACACS+ will do the authentication by using the username and password. LDAP / Active Directory - If it is checked, the LDAP / AD server will do the authentication by using the username, password, information stated on the selected profiles. If the above three options are enabled, the system will do the authentication based on them in sequence.	

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

V-2-6 Online User Status

If you have finished the configuration of SSL Web Proxy (server), users can find out corresponding settings when they access into **DrayTek SSL VPN portal** interface.





Next, users can open SSL VPN>> Online Status to view logging status of SSL VPN.

SSL VPN >> Online User Status



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.	

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.

Below shows the menu items for Certificate Management.

Certificate Management Local Certificate Trusted CA Certificate Certificate Backup

Web User Interface

V-3-1 Local Certificate

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify
			View Delete
			View Delete
			View Delete

Note

- 1. Please setup the "System Maintenance $>> \underline{\text{Time and Date}}$ " correctly before signing the local certificate.
- 2. The Time Zone MUST be setup correctly!!

GENERATE IMPORT REFRESH

Available settings are explained as follows:

Item	Description	
Generate	Click this button to open Generate Certificate Request window.	
	Type in all the information that the window requests. Then click Generate again.	
Import	Click this button to import a saved file as the certification information.	
Refresh	Click this button to refresh the information listed below.	
View	Click this button to view the detailed settings for certificate request.	
Delete	Click this button to delete selected name with certification information.	

GENERATE

Click this button to open Generate Certificate Signing Request window. Type in all the information that the window request such as certificate name (used for identifying different certificate), subject alternative name type and relational settings for subject name. Then click GENERATE again.

Generate Certificate Signing Request Certificate Name Subject Alternative Name IP Address Type **Subject Name** Country (C) State (ST) Location (L) Organization (O) Organization Unit (OU) Common Name (CN) Email (E) RSA V **Key Type** 1024 Bit 💌 Key Size Generate



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



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.

Import X509 Local Certificate Upload Local Certificate Select a local certificate file. Certificate file: Browse. Click Import to upload the local certificate. Import Cancel Upload PKCS12 Certificate Select a PKCS12 file. PKCS12 file: Browse. Password: Click Import to upload the PKCS12 file. Cancel Upload Certificate and Private Key Select a certificate file and a matchable Private Key. Certificate file: Browse. Key file: Browse. Password: Click Import to upload the local certificate and private key. Cancel Import

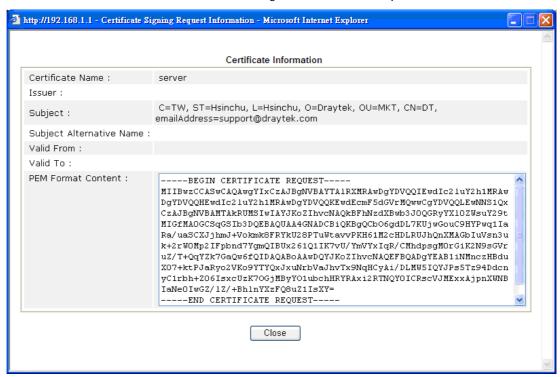
Item	Description		
Upload Local Certificate	It allows users to import the certificate which is generated by Vigor router and signed by CA server.		
	If you have done well in certificate generation, the Status of the certificate will be shown as "OK".		
	Import X509 Local Certificate Congratulation! Local Certificate has been imported successfully. Please click Back to view the certificate.		
	X509 Local Certificate Configuration		
	Name Subject Status Modify		
	draytekdemo /O=Draytek/OU=Draytek Sales/ OK View Delete		
	View Delete		
	GENERATE IMPORT REFRESH		
Upload PKCS12 Certificate	It allows users to import the certificate whose extensions are usually .pfx or .p12. And these certificates usually need passwords.		
	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.		
Upload Certificate and Private Key	It is useful when users have separated certificates and private keys. And the password is needed if the private key is encrypted.		

REFRESH

Click this button to refresh the information listed below.

View

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





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 Root CA
Trusted CA-1			View Delete
Trusted CA-2			View Delete
Trusted CA-3			View Delete

Note:

- 1. Please setup the "System Maintenance $>> \underline{\text{Time and Date}}$ " correctly before you try to generate a RootCA!!
- 2. The Time Zone MUST be setup correctly!!



Creating a RootCA

Click Create Root CA 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.

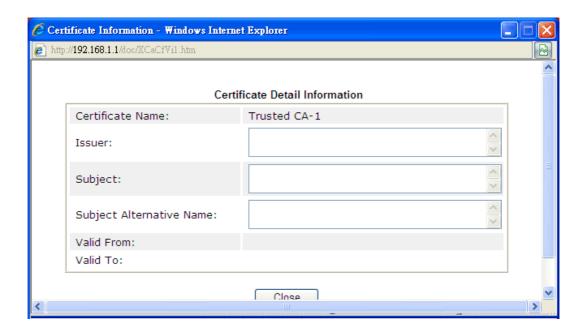
Generate Root CA Root CA Certificate Name Subject Alternative Name Туре IP Address ΙP Subject Name Country (C) State (ST) Location (L) Organization (O) Organization Unit (OU) Common Name (CN) Email (E) RSA 🔻 Key Type Key Size 1024 Bit 🔻 Generate

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.



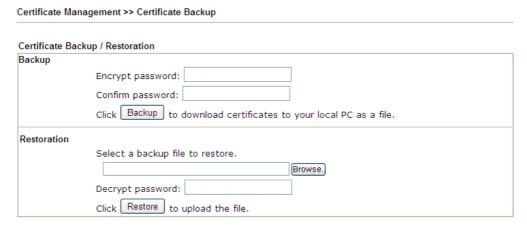
For viewing each trusted CA certificate, click **View** to open the certificate detail information window. If you want to delete a CA certificate, choose the one and click **Delete** to remove all the certificate information.



V-3-3 Certificate Backup

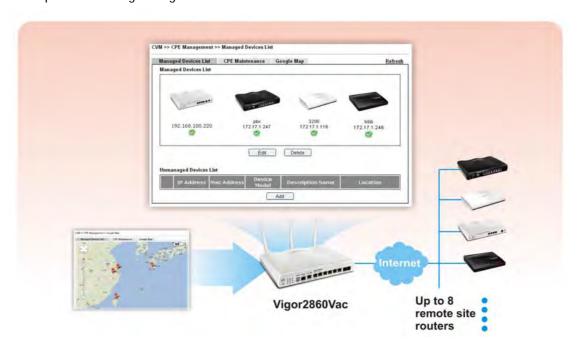
Local certificate and Trusted CA certificate for this router can be saved within one file. Please click **Backup** on the following screen to save them. If you want to set encryption password for these certificates, please type characters in both fields of **Encrypt password** and **Confirm password**.

Also, you can use **Restore** to retrieve these two settings to the router whenever you want.



V-4 Central VPN Management

Vigor2860 can build virtual private network (VPN) between itself and any other TR-069 CPE by the function of central VPN management. In addition, it can be treated as a server (called CVM server) which can manage TR-069 CPE for periodical firmware upgrade, configuration backup and restoring configuration.



Web User Interface

Central VPN Management menu can manage the CPE connected through WAN only.



V-4-1 General Setup

This page is used to configure settings which will be used by the clients to register to such Vigor router. Click **General Settings** and **IPsec VPN Settings** to configure the basic settings for CVM mechanism.

V-4-1-1 General Settings

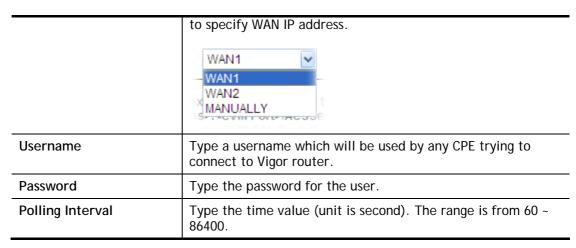
To enable the CVM feature, the first thing you have to do is enabling CVM port or CVM SSL Port.

CVM >> General Setup

General Settings	IPsec VPN Settings	
CVM SSL Port:	8443	
CVM Port:	8000	
WAN IP for Remote C	onnection: WAN1	✓ /
• '	.CSServer/services/ACSServ	et"
Username:	acs	
Password:	•••••	
Polling Interval:	600	Seconds
2. If you choose to us	feature, one of the Port MU se CVM Port, the data betwo Itext, and could be revealed	een CVM Server & CPE Client will

0K

Item	Description
CVM SSL Port	Check the box to enable the port setting. Type the port number in the box.
CVM Port	Check the box to enable the port setting. Type the port number in the box.
WAN IP for Remote Connection	For Vigor router can manage only the client from WAN interface, therefore you have to specify which interface will be used for such function. If you choose MANUALLY, you have

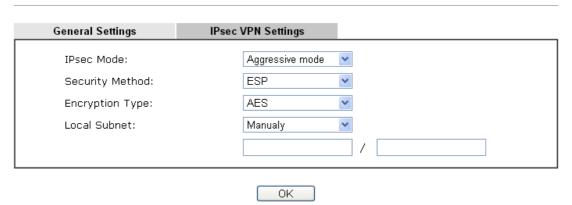


After finishing all the settings here, please click **OK** to save the configuration.

V-4-1-2 IPsec VPN Settings

Central VPN management is operated through IPsec VPN connection.

CVM >> General Setup



Available settings are explained as follows:

Item	Description
IPsec Mode	Choose Aggressive or Main as the IPsec Mode.
Security Method	Choose one of the following methods (AH or ESP) for the security of data transmission. For example, choose AH to specify the IPsec protocol for the Authentication Header protocol. The data will be authenticated but not be encrypted.
Encryption Type	Choose one of the selections as the encryption type.
Local Subnet	Type the IP address and subnet mask of local host.

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

V-4-2 CPE Management

All the CPEs managed by Vigor2860 series can be seen with icons from this page.

Before using such feature, make sure the CVM port has been enabled and configured properly.



V-4-2-1 Managed Device List

This page allows you to manage the CPEs connected to Vigor2860 series.

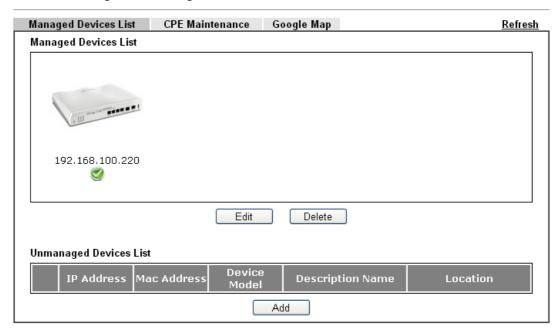
Page without CPE connected

CVM >> CPE Management >> Managed Devices List

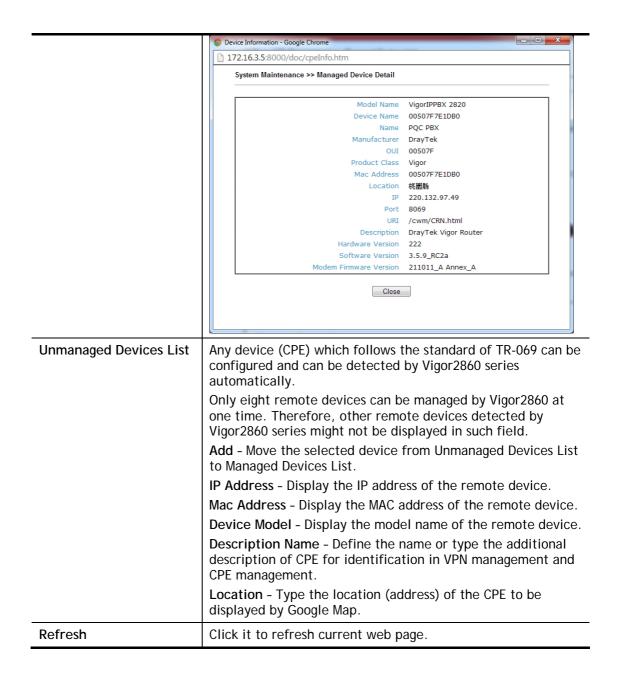


Page with CPE connected

CVM >> CPE Management >> Managed Devices List



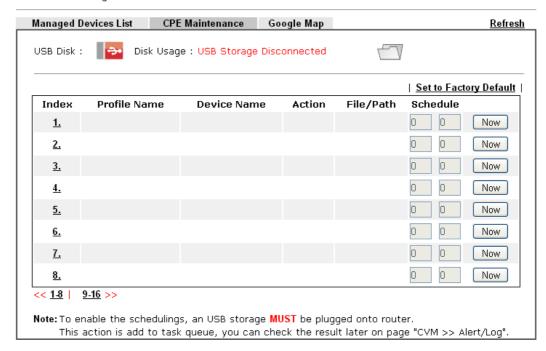
Item	Description
Managed Devices List	This area displays device icons (up to 8) for the CPE managed by Vigor2860 series.
	Edit - To modify the name and location of specific CPE, click the one you want and click the Edit button. A pop up window will appear. Simply change the name and/or location manually.
	№ Device Information - Mozilla Firefox
	(a) 192.168.1.1/doc/cpeInfo.htm
	. System Maintenance >> Edit Device Information
	Model Name Vigor2850
	Device Name 00507F7D9D00
	Name Kate_local_Y2850
	Manufacturer DrayTek
	OUI 00507F
	Product Class Vigor Mac Address 00507F7D9D00
	Location No. 26, Fu Road, HS Ci
	IP 192.168.30.12
	Port 8069
	URI /cwm/CRN.html
	Description DrayTek Vigor Router
	Hardware Version 104
	Software Version 3.6.3
	Modem Firmware Version 211801_A Annex_A
	OK
	Delete - To disconnect the management of any CPE, click the CPE icon you want and click the Delete button.
	Double-clicking the CPE icon also can pop up the Managed Device Detail window. However, you cannot modify any data
	on the window.



V-4-2-2 CPE Maintenance

This area displays all the profiles which are created for applying to the managed device. This page can help the administrator to do maintenance jobs like firmware upgrade, configuration backup, configuration restoration and etc.

CVM >> CPE Management >> CPE Maintenance



Item	Description
Refresh	Click it to refresh current page.
USB Disk	USB Disk: - It means a USB disk connecting to Vigor2860.
	USB Disk: - It means no USB disk connecting to Vigor2860.
Disk Usage	Disk Usage: 1084MB / 2009MB - When a USB disk connects to Vigor2860, the disk usage and the disk capacity will be displayed in such field.
	Disk Usage: USB Storage Disconnected - When there is no USB disk connecting to Vigor2860, such message will be displayed in this field.
	Click the icon to see the content inside the USB disk.
Set to Factory Default	Click to clear all indexes.
Index	Display the number of the profile that you can edit.
Profile Name	Display the name of the maintenance profile.
Device Name	Display the name of the managed CPE that the maintenance profile will apply to.

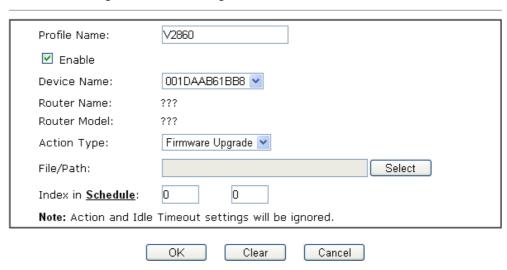
Action	Display the action that managed CPE shall accept.
File/Path	Display the location of the file you want to save, restore or upgrade for CPE.
Schedule	Display the schedule profiles selected for such profile.
Now	The action will be performed for the selected CPE immediately.

How to add a new Maintenance Profile

Follow the steps below to create a new maintenance profile.

- 1. Click any index number link, e.g., Index 1.
- 2. The Maintenance dialog appears.

Central VPN Management >> CPE Management >> Maintanance Profile





Info

When restoring configuration to a CPE, make sure the configuration file you selected was backup from this CPE before. Because restoring from another device's configuration file may cause serious problem (e.g., Both devices have different ISP username/ password. Restoring configuration from one CPE to the other will cause Internet connection not being online)..

Available parameters are listed as follows:

Item	Description
Profile Name	Type the name of the maintenance profile.
Enable	Check it to enable such profile.
Device Name	The drop down list will display all the CPE devices detected by Vigor2860 series. Choose the one which will be applied with such new created profile.
Action Type	 There are three actions for you to choose for such profile. Config Backup - It means such profile will be used for configuration backup of the selected CPE. Config Restore - It means such profile will be used for restoring the configuration of the selected CPE.

	Info When restoring configuration to a CPE, make sure the configuration file you selected was backup from this CPE before. Because restoring from another device's configuration file may cause serious problem (e.g., Both devices have different ISP username/ password. Restoring configuration from one CPE to the other will cause Internet connection not being online).
	Firmware Upgrade - It means such profile will be used for firmware upgrade.
File/Path	Click Select to locate the file you want to save, restore or upgrade for CPE.
Index in Schedule	Vigor2860 series will perform the specified action to the selected CPE based on the schedule configured here. Specify one or two schedule profiles (represented by number) here.

- 3. Enter all the settings and click **OK**.
- 4. A new maintenance profile has been created.

V-4-2-3 Google Map

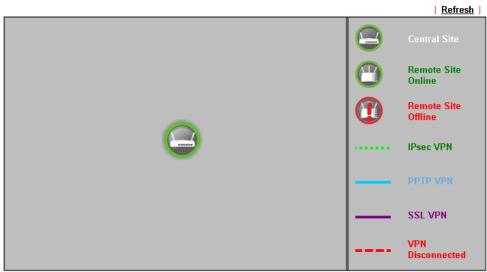
To display the **location** of the managed CPE with a bird's eye view, open **Central VPN Management**>>CPE **Management** and click the tab of **Google Map**.



V-4-3 VPN Management

An easy and quick method is offered to configure VPN settings for building VPN connection automatically between Vigor2860 series (treated as VPN server) and other Vigor router (treated as CPE device, i.e., VPN client).

CVM >> VPN Management



Note: CVM SSL LAN-to-LAN dial-up might fail with the CPE of old version firmware. Please update the remote CPE to the latest version.



Available parameters are listed as follows:

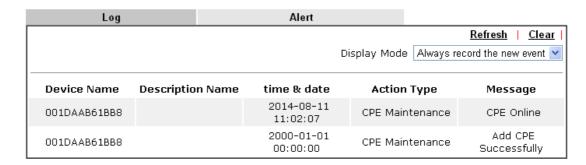
Item	Description
CPE VPN Connection List	
VPN	Display the name of the LAN-to-LAN profile. It is generated automatically when you click the PPTP/IPsec/Advanced button to build the VPN connection between Vigor2860 and remote CPE.
Туре	Display the dial-in type and the authentication method.
Remote IP	Display the IP address of the remote CPE and the interface.
Virtual Network	Display the IP address and subnet mask of Vigor2860 series.
Tx Pkts	Display the number of the transmitted packets.
Tx Rate(Bps)	Display the number of the transmitted rate.
Rx Pkts	Display the number of the received packets.
Rx Rate(Bps)	Display the number of the received rate.
UP Time	Display the connection time of such VPN.

Once the device is managed (controlled) by Vigor2860 series, it will be displayed on such screen automatically. If not, refer to sections "How to manage the CPE (router) through Vigor2860?" for more detailed information.

V-4-4 Log & Alert

This page offers brief information to identify the CPE connected to Vigor2860 series.

CVM >> Log & Alert



Available settings are explained as follows:

Item	Description
Display Mode	Choose the mode you want to display the related information on the following table.
	• Stop record when fulls - when the capacity of CVM log is full, the system will stop recording.
	 Always record the new event - only the newest events will be recorded by the system.
Device Name	Display the name of the managed CPE.
Description Name	Display the brief explanation for the managed CPE.
Time & date	Display the time and date that the managed CPE scanned by Vigor2860 series.
Action Type	Display the action that Vigor2860 series will perform for the managed CPE.
Message	Display the information for each event.

The Alert page offers brief information to identify the CPE connected to Vigor2860 series.

Application Notes

A-1 CVM Application - How to manage the CPE (router) through Vigor2860 series?

To manage CPEs through Vigor2860 series, you have to set URL on CPE first and set username and password for Vigor2860 series. For this section, we use Vigor2850 series as the example. All the CPE configuration will be done through Vigor2850 series.

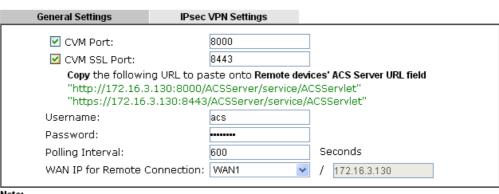
Configure CVM Settings on Vigor2860 series

- 1. Access into the web user interface of Vigor2860 series.
- 2. Open Central VPN Management>>General Setup.



3. In the following page, check the boxes for CVM Port and CVM SSL Port to enable the port setting. Type the values for CVM Port, CVM SSL Port, Username, and Password respectively. Remember the values configured in this page.

CVM >> General Setup



Note:

To enable the CVM feature, one of the Port MUST be Enabled!

ΟK

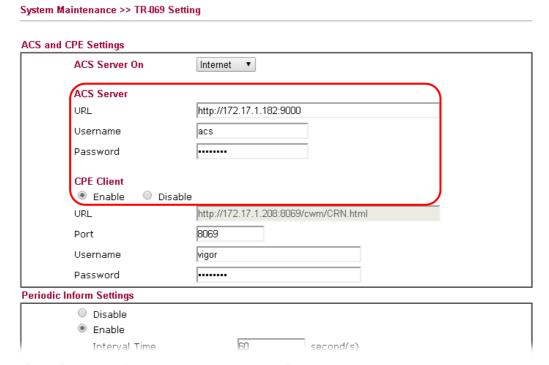
Click **OK** to save the settings.

Configure Settings on CPE

- 1. In the end of the CPE, access into the web user interface of the CPE (e.g., Vigor2850 series). Open a web browser (for example, IE, Mozilla Firefox or Netscape) and type http://192.168.1.1.
- 2. Open System Maintenance >> TR-069.

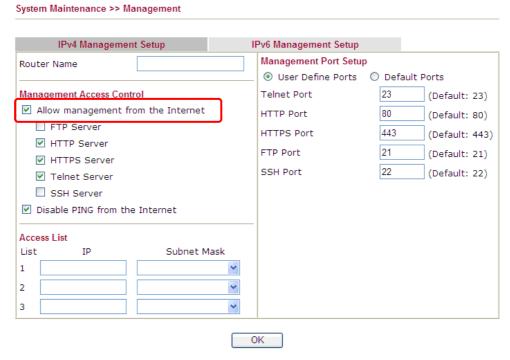


3. In the field of ACS Server, type the URL (IP address with port number) of Vigor2860 series and type the same Username and Password defined on the page of Central VPN Management>>General Setup in Vigor2860 series. Then, click Enable for CPE Client and then click OK to save the settings.

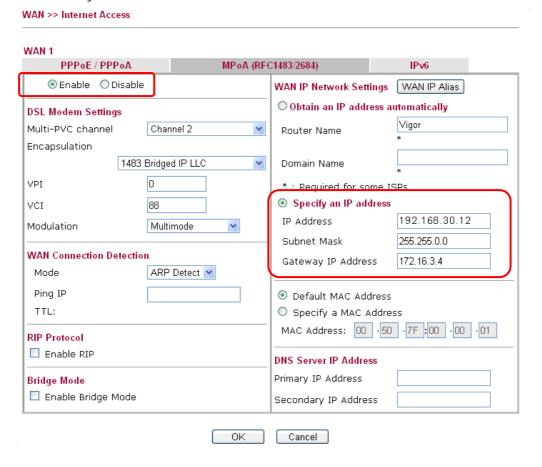


4. Open System Maintenance>>Management Setup.

5. Check Allow management from the Internet to set management access control and click OK.



- 6. Open WAN>>Internet Access. Use the drop down list of Access Mode on WAN1 to select MPoA (RFC1483/2684). Then, click Details Page.
- 7. Click **Specify an IP address**. Type correct WAN IP address, subnet mask and gateway IP address for your CPE. Then click **OK**.



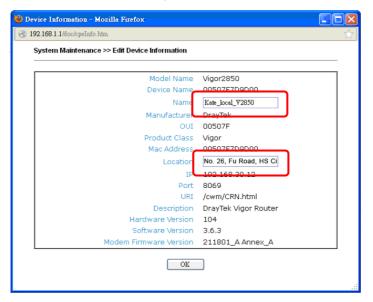


Info

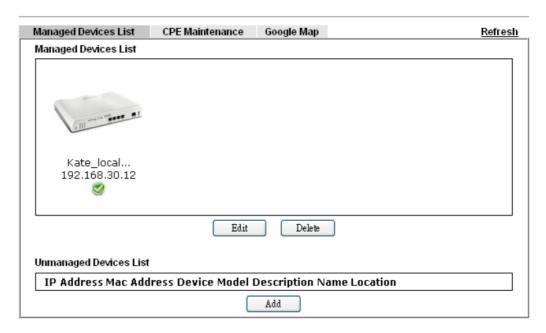
Reboot the CPE device and re-log into Vigor2860 series. CPE which has registered to Vigor2860 series will be captured and displayed on the page of Central VPN Management>>CPE Management.

Check CPE Maintenance Page

- 1. Return to the web user interface of Vigor2860 series.
- 2. Open Central VPN Management>>VPN Management. Now there is one CPE displayed on the field of Unmanaged Devices List.
- 3. Choose the one (Vigor2850) from Unmanaged Devices List and click **Add**. The following dialog will be popped up. Type the name and the location of the router respectively. Click **OK** to save the configuration.



4. The selected CPE will be moved and displayed on Managed Devices List which means it is controlled / managed by Vigor2860 series from now on.



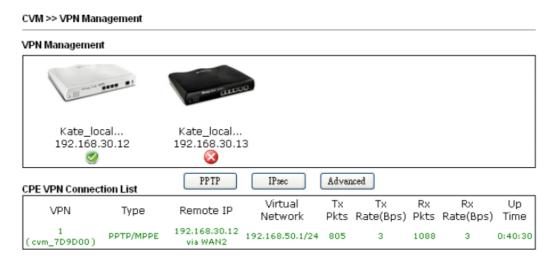
A-2 CVM Application - How to build the VPN between remote devices and Vigor2860 series?

When a remote device is managed by Vigor2860 series, it is easy to build VPN between these two devices.

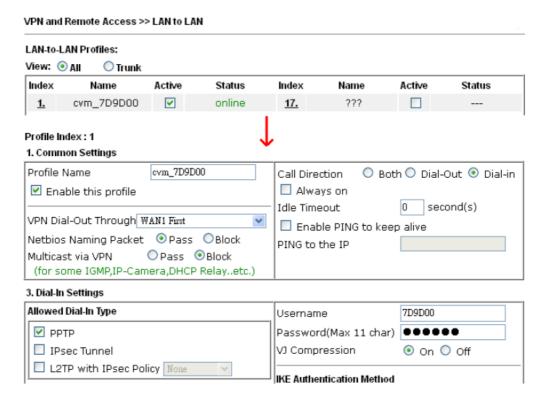
- 1. Access into the web user interface of Vigor2860 series.
- 2. Open Central VPN Management>>CPE Management.



- 3. Click the device icon (marked with) and click the PPTP/IPsec button.
- 4. Wait for a moment. If VPN is built successfully, related information will be displayed on CPE VPN Connection List.



5. A LAN to LAN profile for such VPN will be generated automatically. You can access into VPN and Remote Access>>LAN to LAN of the remote device for viewing the detailed information.



Note: The profile name is created automatically by the system. Do not modify any value in such page to avoid VPN error.

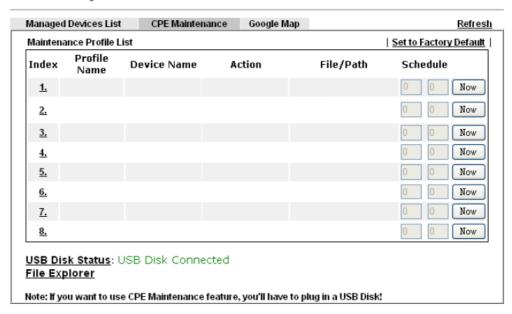
A-3 CVM Application - How to upgrade CPE firmware through Vigor2860 series?

Download the newest firmware from your Draytek website to USB Storage Disk for the device (e.g., Vigor2850) managed by Vigor2860 series.

Vigor2850, as an example, is chosen for Vigor2860 to perform the CPE firmware upgrade remotely in this case.

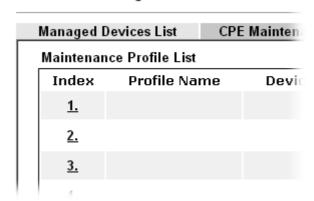
- 1. Plug in USB storage disk onto Vigor2860 series via USB interface. Make sure the USB disk has been installed correctly, otherwise, the firmware upgrade will not be successful.
- Access into web user interface of Vigor2860 series. Open Central VPN Management>>CPE Management and click the CPE Maintenance tab.

CVM >> CPE Management >> CPE Maintenance



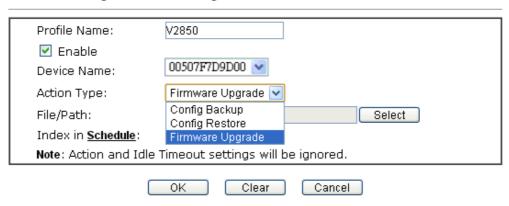
3. Click any index number link, e.g., Index 1.

CVM >> CPE Management >> CPE Maintenan



4. The Maintenance profile dialog appears.

Central VPN Management >> CPE Management >> Maintanance Profile



In the field of Profile Name, type a name for such maintenance profile; check Enable; and choose the one you want to perform firmware upgrade from Device Name drop down list. From the Action Type, choose Firmware Upgrade. Type the file/path of the newest firmware or click Select to locate it. Specify the Schedule profile. At last, click **OK**.

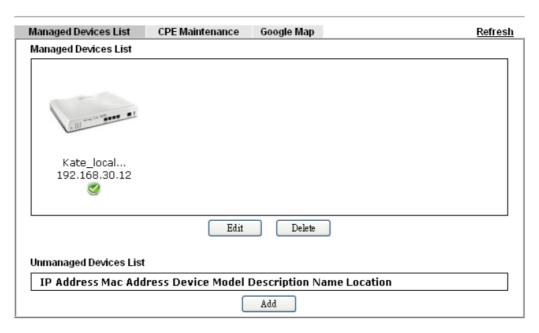
5. Now, a new maintenance profile has been created.

CVM >> CPE Management >> CPE Maintenance

Managed	Devices List	CPE Maintenance	Google Map		Refresi
Maintenance Profile List Set to Factory Default			Set to Factory Default		
Index	Profile Name	Device Name	Action	File/Path	Schedule
<u>1.</u>	V2850	00507F7D900	Firmware Upgrade		1 0 Now
<u>2.</u>					0 0 Now
<u>3.</u>					0 0 Now
<u>4.</u>					0 0 Now
<u>5.</u>					0 0 Now
<u>6.</u>					0 0 Now
<u>7.</u>					0 0 Now
<u>8.</u>					0 0 Now
USB Disk Status: USB Disk Connected File Explorer					
Note: If you want to use CPE Maintenance feature, you'll have to plug in a USB Disk!					

- 6. Click **Now** to perform the firmware upgrade immediately for Vigor2850.
- 7. Wait for several minutes for firmware upgrade.

8. Then check the device information for the managed device if the firmware upgrade is successful or not. Click Managed Devices List.



Click the icon of Vigor2850 and click **Edit** and view the software version. Another way to check if the firmware upgrade is completed or not, simply open **Central VPN Management>>Log & Alert**.

Part VI Security



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.

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:

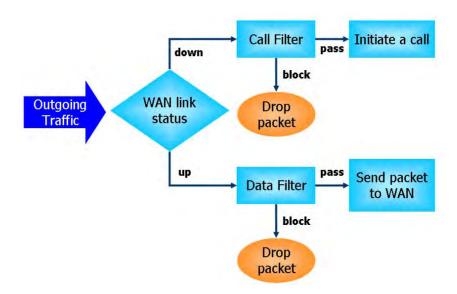
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

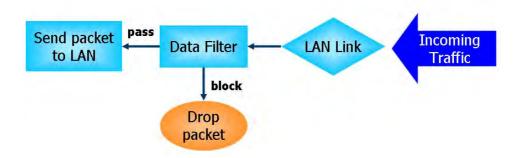
IP Filters

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
- 2. UDP flood attack
- 3. ICMP flood attack
- 4. Port Scan attack
- 5. IP options
- 6. Land attack
- 7. Smurf attack
- 8. Trace route

- 9. SYN fragment
- 10. Fraggle attack
- 11. TCP flag scan
- 12. Tear drop attack
- 13. Ping of Death attack
- 14. ICMP fragment
- 15. Unassigned Numbers

Web User Interface

Below shows the menu items for Firewall.



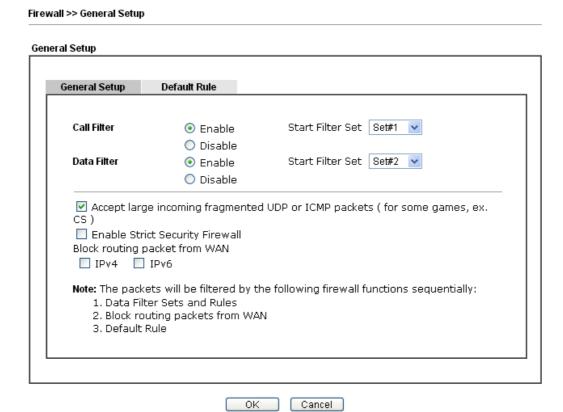
VI-1-1 General Setup

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.



Available settings are explained as follows:

14	Description
Item	Description
	'

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

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.

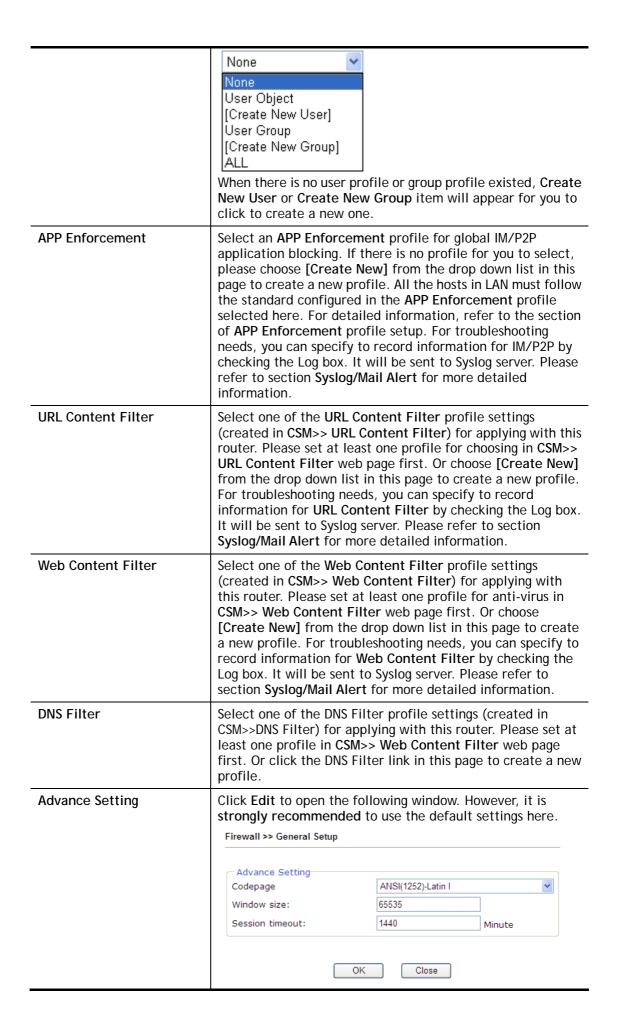
Firewall >> General Setup General Setup General Setup Default Rule Actions for default rule: Application Action/Profile Syslog Filter Pass ▼ **Sessions Control** 174 / 60000 **Quality of Service** None <u>User Management</u> None **APP Enforcement** None **URL Content Filter** None • Web Content Filter None **DNS Filter** None Advance Setting Edit

OΚ

Cancel

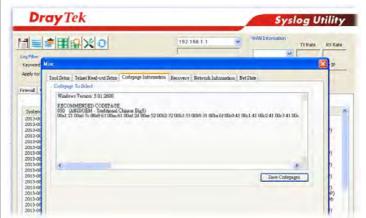
Available settings are explained as follows:

Item	Description	
Filter	Select Pass or Block for the packets that do not match with the filter rules.	
	Filter Pass Pass Block	
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.	
Quality of Service	Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later. None Class 1 Class 2 Class 3 Default	
User Management	Such item is available only when Rule-Based is selected in User Management>>General Setup. The general firewall rule will be applied to the user/user group/all users specified here.	



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.

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



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

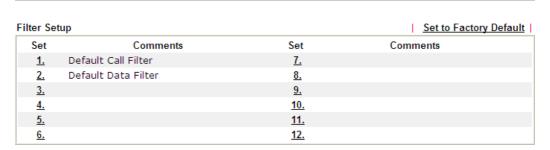
Session timeout - Setting timeout for sessions can make the best utilization of network resources.

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



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



Available settings are explained as follows:

Item	Description
Filter Rule	Click a button numbered (1 ~ 7) to edit the filter rule. Click the button will open Edit Filter Rule web page. For the detailed information, refer to the following page.
Active	Enable or disable the filter rule.
Comment	Enter filter set comments/description. Maximum length is 23-character long.
Move Up/Down	Use Up or Down link to move the order of the filter rules.
Next Filter Set	Set the link to the next filter set to be executed after the current filter run. Do not make a loop with many filter sets.

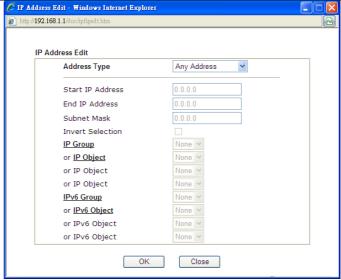
To edit Filter Rule, click the Filter Rule index button to enter the Filter Rule setup page.

Filter Set 1 Rule 1

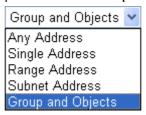
Check to enable the Filter Rul	le	
Comments:	Block NetBios	
Index(1-15) in Schedule Setup:		
Clear sessions when schedule ON:	■ Enable	
Direction:	LAN/DMZ/RT/VPN -> WAN	▼
Source IP:	Any	Edit
Destination IP:	Any	Edit
Service Type:	TCP/UDP, Port: from 137~139 to any	Edit
Fragments:	Don't Care ▼	
Application	Action/Profile	Syslog
Filter:	Block Immediately ▼	
Branch to Other Filter Set:	None ▼	
Sessions Control	0 / 60000	
MAC Bind IP	Non-Strict ▼	
Quality of Service	None ▼	
<u>User Management</u>	None ▼	
APP Enforcement:	None ▼	
<u>URL Content Filter</u> :	None ▼	
Web Content Filter:	None ▼	
DNS Filter	None ▼	
Advance Setting	Edit	

Available settings are explained as follows:

Item	Description	
Check to enable the Filter Rule	Check this box to enable the filter rule.	
Comments	Enter filter set comments/description. Maximum length is 14-character long.	
Index(1-15)	Set PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in Applications >> Schedule setup. The default setting of this field is blank and the function will always work.	
Clear sessions when schedule ON	Check this box to clear the sessions when the above schedule profiles are applied.	
Direction	Set the direction of packet flow. It is for Data Filter only. For the Call Filter, this setting is not available since Call Filter is only applied to outgoing traffic. LAN/RT/VPN -> WAN LAN/RT/VPN -> WAN WAN -> LAN/RT/VPN LAN/RT/VPN -> LAN/RT/VPN Note: RT means routing domain for 2nd subnet or other LAN.	
Source/Destination IP	Click Edit to access into the following dialog to choose the source/destination IP or IP ranges.	



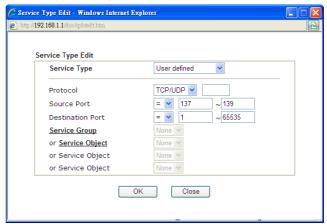
To set the IP address manually, please choose Any Address/Single Address/Range Address/Subnet Address as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose Group and Objects as the Address Type.



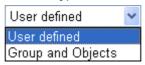
From the IP Group drop down list, choose the one that you want to apply. Or use the IP Object drop down list to choose the object that you want.

Service Type

Click **Edit** to access into the following dialog to choose a suitable service type.



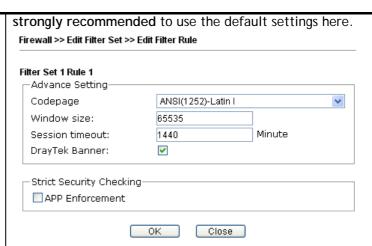
To set the service type manually, please choose **User defined** as the Service Type and type them in this dialog. In addition, if you want to use the service type from defined groups or objects, please choose **Group and Objects** as the Service Type.



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

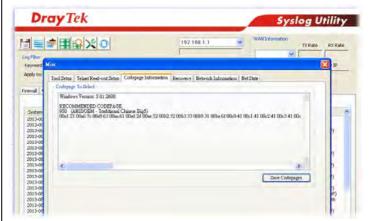
S (O o ir t	Source/Destination Port - (=) - when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type. (!=) - when the first and last value are the same, it indicates all the ports except the port defined
(o in ty	(=) - 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 ype. (!=) - when the first and last value are the same, it indicates all the ports except the port defined
o ir ty	one port; when the first and last values are different, it indicates a range for the port and available for this service type. (!=) - when the first and last value are the same, it indicates all the ports except the port defined
-	ndicates all the ports except the port defined
ir	nere; 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
Š	orofile. Service Group/Object - Use the drop down list to choose the one that you want.
	Specify the action for fragmented packets. And it is used for Data Filter only.
	Don't care -No action will be taken towards fragmented backets.
L	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 o contain a complete header.
	Specifies the action to be taken when packets match the rule.
	Block Immediately - Packets matching the rule will be dropped immediately.
	Pass Immediately - Packets matching the rule will be passed mmediately.
ti	Block If No Further Match - A packet matching the rule, and hat does not match further rules, will be dropped.
	Pass If No Further Match - A packet matching the rule, and hat does not match further rules, will be passed through.
b b w	oranch to the specified filter set. Select 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.
ti	The number typed here is the total sessions of the packets hat do not match the filter rule configured in this page. The default setting is 60000.
c	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. No-Strict - no limitation.
F	Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later.

	None None Class 1 Class 2 Class 3 Default
User Management	Such item is available only when Rule-Based is selected in User Management>>General Setup. The general firewall rule will be applied to the user/user group/all users specified here. None None
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 from the drop down list in this page to create a new profile.
Advance Setting	Click Edit to open the following window. However, it is



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

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



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

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

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

The requested Web page has been blocked by Web Content Filter.

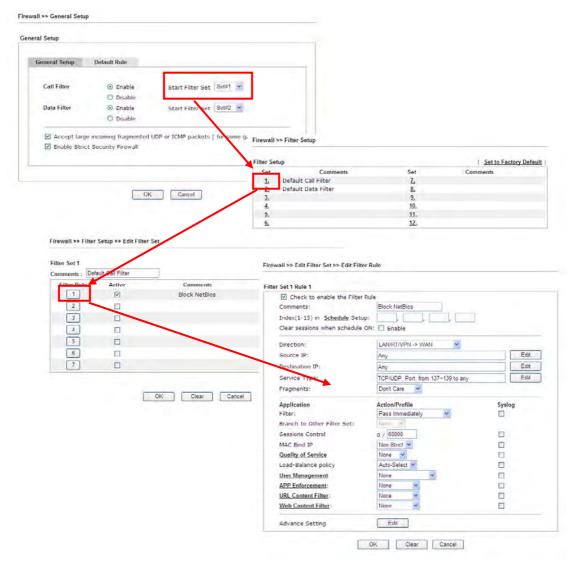
Please contact your system administrator for further information.

[Powered by Draytek]

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 on of two IP filters: call filter or data filter. You may preset 12 call filters and data filters in Filter Setup and even link them in a serial manner. Each filter set is composed by 7 filter rules, which can be further defined. After that, in General Setup you may specify one set for call filter and one set for data filter to execute first.



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.

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

Firewall >> DoS defense Setup DoS defense Setup Enable DoS Defense Select All Enable SYN flood defense 2000 Threshold packets / sec 10 Timeout sec packets / sec Threshold 2000 ☐ Enable UDP flood defense Timeout 10 sec Threshold Enable ICMP flood defense 250 packets / sec Timeout 10 sec packets / sec Threshold 2000 Enable Port Scan detection Block IP options Block TCP flag scan ■ Block Land ■ Block Tear Drop Block Smurf Block Ping of Death ☐ Block trace route ■ Block ICMP fragment Block SYN fragment Block Unassigned Numbers Block Fraggle Attack

Clear All

Cancel

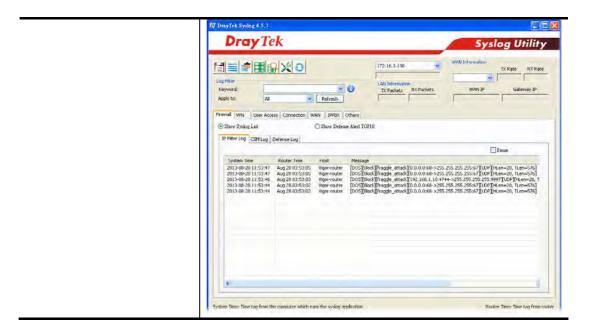
OΚ

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	Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent TCP SYN packets for a period defined in Timeout. The goal for this is prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor router. By default, the threshold and timeout values are set to 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.
Enable UDP flood defense	Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent UDP packets for a period defined in Timeout. The default setting for threshold and timeout are 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.
Enable ICMP flood defense	Check the box to activate the ICMP flood defense function. Similar to the UDP flood defense function, once if the Threshold of ICMP packets from Internet has exceeded the defined value, the router will discard the ICMP echo requests coming from the Internet.
	The default setting for threshold and timeout are 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.
Enable PortScan detection	Port Scan attacks the Vigor router by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the port-scanning Threshold rate, the Vigor router will send out a warning.
	By default, the Vigor router sets the threshold as 2000 packets per second. That means, when 2000 packets per second received, they will be regarded as "attack event".
Block IP options	Check the box to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messagesetc. An eavesdropper outside might learn the details of your private networks.
Block Land	Check the box to enforce the Vigor router to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.
Block Smurf	Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.
Block trace route	Check the box to enforce the Vigor router not to forward any trace route packets.
Block SYN fragment	Check the box to activate the Block SYN fragment function. The Vigor router will drop any packets having SYN flag and more fragment bit set.
Block Fraggle Attack	Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked.
	Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.

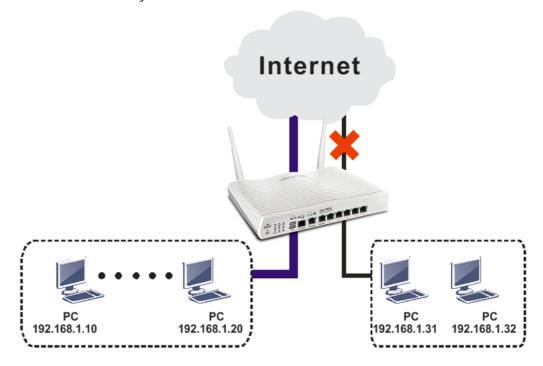
Block TCP flag scan	Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include <i>no flag scan</i> , FIN without ACK scan, SYN FINscan, Xmas scan and full Xmas scan.	
Block Tear Drop	Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.	
Block Ping of Death	Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.	
Block ICMP Fragment	Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.	
Block Unassigned Numbers	Check the box to activate the Block Unknown Protocol function. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and reject this kind of packets.	
Warning Messages	We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client.	
	All the warning messages related to DoS Defense will be sent to user and user can review it through Syslog daemon. Look for the keyword DoS in the message, followed by a name to indicate what kind of attacks is detected. System Maintenance >> SysLog / Mail Alert Setup	
	SysLog / Mail Alert Setup SysLog Access Setup Penable Syslog Save to: Syslog Save to: Syslog Save to: Syslog Save to: SMTP Server SMTP Port 25 Mail To Return-Path Authentication User Name Password Enable syslog message: Firewall Log Viser Access Log Winner Access Lo	
	OK Clear	



Application Notes

A-1 How to Configure Certain Computers Accessing to Internet

We can specify certain computers (e.g., $192.168.1.10 \sim 192.168.1.20$) 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.

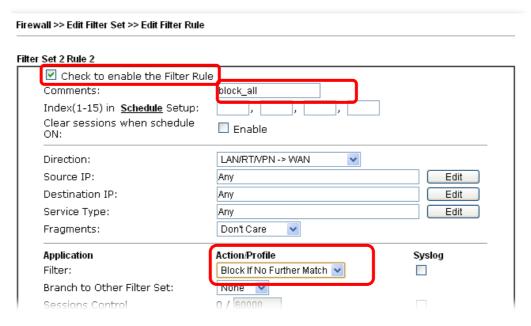


The way we can use is to set two rules under Firewall. For Rule 1 of Set 2 under Firewall>>Filter Setup is used as the default setting, we have to create a new rule starting from Filter Rule 2 of Set 2.

- 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.

irewall >> Filter S	Setup			
ilter Setup			Set to	Factory Default
Set	Comments	Set	Comments	
Defaul	t Call Filter	<u>7.</u>		
	t Data Filter	<u>8.</u>		
3.		<u>9.</u>		
<u>4.</u> <u>5.</u>		<u>10.</u>		
		<u>11.</u>		
<u>6.</u>		<u>12.</u>		
ilter Se 2 Commet s: Def	Setup >> Edit Filter Set			
Filter Rule	Active	Comments	Mo∨e Up	Move Down
	✓	xNetBios -> DNS		<u>Down</u>
2			<u>UP</u>	<u>Down</u>
3			<u>UP</u>	<u>Down</u>
4			UP	Down

Check the box of Check to enable the Filter Rule. Type the comments (e.g., block_all).
 Choose Block If No Further Match for the Filter setting. Then, click OK.

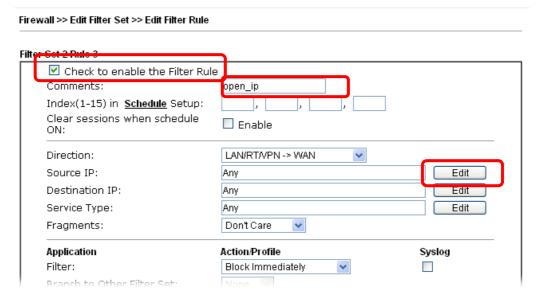




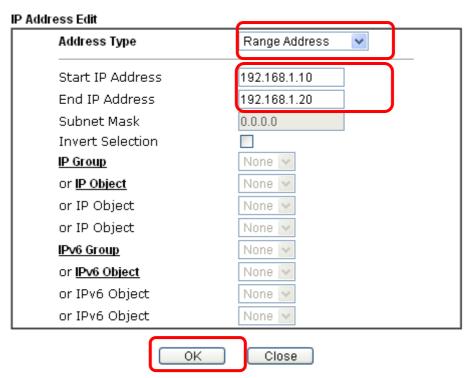
Info

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.

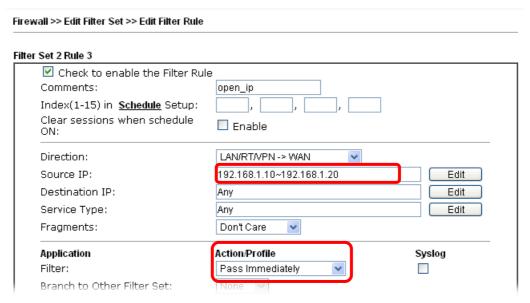
- 4. Next, set another rule. Just open Firewall>>Filter Setup. Click the Set 2 link and choose the Filter Rule 3 button.
- 5. Check the box of Check to enable the Filter Rule. Type the comments (e.g., open_ip). Click the Edit button for Source IP.



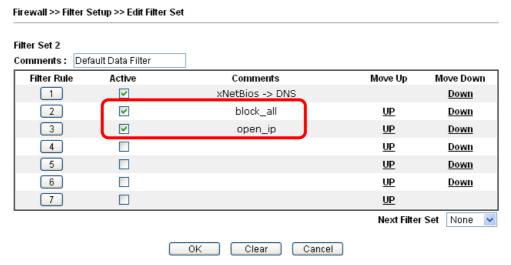
6. A dialog box will be popped up. Choose Range Address as Address Type by using the drop down list. Type 192.168.1.10 in the field of Start IP, and type 192.168.1.20 in the field of End IP. Then, click OK to save the settings. The computers within the range can access into the Internet.



7. 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.



8. Both filter rules have been created. Click **OK**.



Now, all the settings are configured well. Only the computers with the IP addresses within $192.168.1.10 \sim 192.168.1.20$ can access to Internet.

VI-2 Central Security Management (CSM)

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 misusage during office hour or prevent unknown security leak. It is similar situation for corporation towards peer-to-peer applications since file-sharing can be convenient but insecure at the same time. To address these needs, we provide CSM functionality.

URL Content Filter

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

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

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

Web Content Filter

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

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



Info

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

Web User Interface

CSM
APP Enforcement Profile
APPE Signature Upgrade
URL Content Filter Profile
Web Content Filter Profile
DNS Filter Profile

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 License	<u>Activate</u>
[Status:Not Activated]	

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

Available settings are explained as follows:

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

Click the number under Index column for settings in detail.

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

Below shows the items which are categorized under IM.



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.
Adv	A button under Enable check box allows you to open a pop up window to specify activity for that APP.

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

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

CSM >> APP Enforcement Profile

Profile Index : 1 Profile Name:

IM P2P Protocol OTHERS

Select All Clear All

Select	All Clear All				
	Protocol				
Enable	APP Name	Version	Note		
	DB2		DB2 is a relational database management system (RDBMS) offered by IBM.		
	DNS		Domain Name System (DNS) protocol is used to translate easily memorized domain names to numerical IP addresses needed for the purpose of locating computer services and devices worldwide.		
	FTP		File Transfer Protocol (FTP) is used to transfer files from one host to another host over networks.		
	НТТР	1.1	Hypertext Transfer Protocol (HTTP) is the data communication protocol for the World Wide Web.		
	IMAP	4.1	Internet message access protocol (IMAP) is a protocol for e-mail retrieval.		
	IRC	2.4.0	Internet Relay Chat (IRC) is a protocol for live interactive Internet text messaging (chat), synchronous conferencing and file sharing.		
	Informix		Informix is a relational database management system (RDBMS) offered by IBM.		
	MSSQL		Microsoft SQL Server is a relational database management system.		
	MySQL		MySQL is an open source relational database management system.		
	NNTP		The Network News Transfer Protocol (NNTP) is a protocol used for transporting Usenet news articles between news servers and for reading and posting articles by end user client applications.		

The items categorized under P2P -----

CSM >> APP Enforcement Profile

Profile Index: 1 Profile Name:

IM	P2P	Protocol	OTHERS	
Select A	II Clear All			
			BitTorrent	
Enable	APP Name	Version	Note	
	BitTorrent		The encrypted connection can not be 100% blocked. To block BitComet (1.30), BitSpirit (3.2.1), BitTorrent (4.4.1) and UltraTorrent (2.0).	

FastTrack				
Enable	APP Name	Version	Note	
	FASTTRACK		To block BareShare (6.2.0.45), iMesh (9.1), KazaA (1.0.0.3) and Shareaza (4.1.0).	

Gnutella			
Enable	APP Name	Version	Note
	GNUTELLA		To block BareShare (5.1.0.26), Foxy (1.9.9), LimeWireWin (4.18.3) and Shareaza (2.3.0.0).

OpenFT			
Enable	APP Name	Version	Note
D.	OpenFT	11	When blocking the connection, it will show "Connected" at first while the connection is not established successfully. After few seconds it will change back to "Connection" status. KCeasy (0.19) also supports Area

Skyfire

Socks 4/5

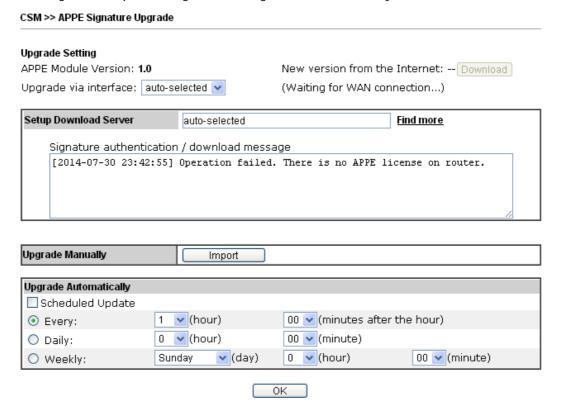
CSM >> APP Enforcement Profile Profile Index : 1 Profile Name: IM P2P Protocol OTHERS Select All Clear All TUNNEL Enable APP Name Version Note DNSCrypt 0.0.6 Only blocks DNSCrypt login. DynaPass 1.5 10 FreeU HTTP Proxy HTTP Tunnel 4.4.4000 Hamachi 1.0.2.5 Block Hotspot Shield from establishing VPN connections. Please note that the APP Enforcement needs to be enabled prior than the VPN connections, or the blocking may not be successful. Hotspot Shield 4.15.3 MS Teredo 7.0.3 **PGPNet** Ping Tunnel 0.61 RealTunnel 1.0.1

Please note that Radmin will also be blocked by this item. Please set the server port of Radmin within 5001~32767

1.5

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.



Available settings are explained as follows:

Item	Description
Upgrade Setting	APPE Module Version - Display current version status of APPE signature.
	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.
	Upgrade via interface - Choose one of the WAN interfaces as a channel for APPE signature upgrade.
Setup Download Server	Specify the download server by typing the URL of the server located. Or you can click <u>Find more</u> link to search the one you want.
	Signature authentication/download message - Display the status of APPE Signature Upgrade.
Upgrade Manually	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 Upgrade and wait for the system completing the process.



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.

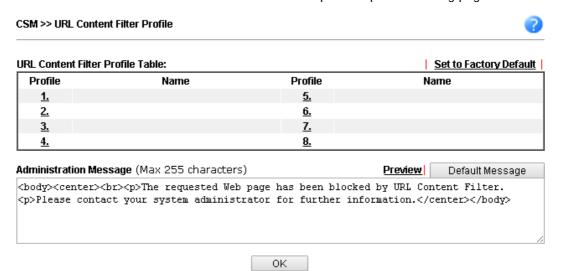
Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine URL Content Filter as a well-trained convenience-store clerk who won't sell adult magazines to 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.



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 type the message manually for your necessity. Default Message - You can type the message manually for your necessity or click this button to get the default message which will be displayed on the field of Administration Message.

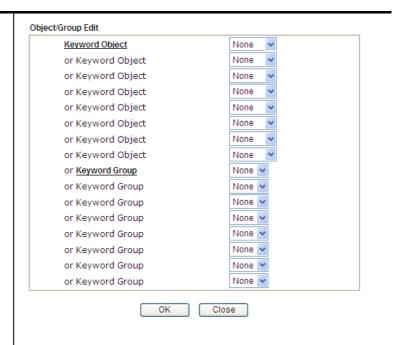
You can set eight profiles as URL content filter. Simply click the index number under Profile to open the following web page.

CSM >> URL Content Filter Profile



Item	Description		
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.		
Priority	It determines the action that this router will apply. 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. Both:Block -The router will block all the packages that match with the conditions specified in URL Access Control and Web Feature below. When you choose this setting, both configuration set in this page for URL Access Control and Web		
	Feature will be inactive. Either: URL Access Control First - When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for URL first, then Web feature second.		
	Either: Web Feature First -When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for web feature first, then URL second.		

	Both: Pass Both: Pass Both: Block Either: URL Access Control First Either: Web Feature First			
Log	None - There is no log file will be recorded for this profile. Pass - Only the log about Pass will be recorded in Syslog. Block - Only the log about Block will be recorded in Syslog. All - All the actions (Pass and Block) will be recorded in Syslog. None Pass Block All			
URL Access Control	Enable URL Access Control - Check the box to activate URL Access Control. Note that the priority for URL Access Control is higher than Restrict Web Feature. If the web content match the setting set in URL Access Control, the router will execute the action specified in this field and ignore the action specified under Restrict Web Feature. Prevent web access from IP address - Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control. You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before. Action - This setting is available only when Either: URL Access Control First or Either: Web Feature First is selected. Pass - Allow accessing into the corresponding webpage with the keywords listed on the box below. Block - Restrict accessing into the corresponding webpage with the keywords listed on the box below. If the web pages do not match with the keyword set here, it will be processed with reverse action. 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.			



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.



After finishing all the settings, please click \mathbf{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.

	ò	
- 40	ī	
- 🔻	u	•

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-239 025151.html



<u>Activate</u>

Web-Filter License

[Status:Not Activated]

Setup Query Server	auto-selected	Find more
Setup Test Server	auto-selected	<u>Find more</u>

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

contact your system administrator for further information.</center></body>

Legend:

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

ΟK

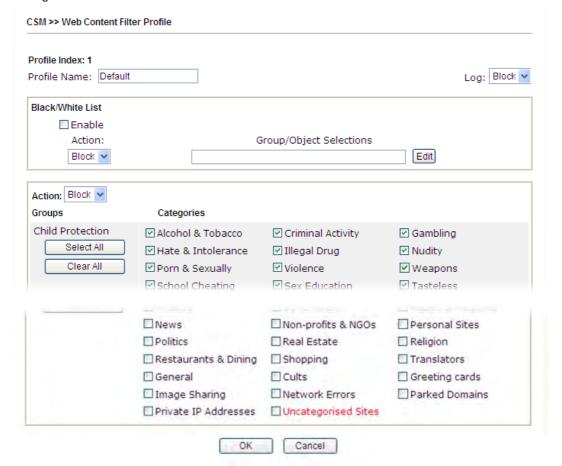
Item	Description	
Activate	Click it to access into MyVigor for activating WCF service.	
Setup Query Server	It is recommended for you to use the default setting, auto-selected. You need to specify a server for categorize searching when you type URL in browser based on the web content filter profile.	
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.	
Test a site to verify whether it is categorized	Click this link to do the verification.	
Set to Factory Default	Click this link to retrieve the factory settings.	
Administration Message	You can type the message manually for your necessity or click Default Message button to get the default text displayed on the field of Administration Message. Preview - A dialog will appear to display the message typed in the Administration Message.	
Cache	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.	
	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.

L2 - the router will check the URL that the user wants to access via WCF. If the data has been accessed previously, the IP addresses of source and destination IDs will be memorized for a short time (about 1 second) in the router. When the user tries to access the same destination ID, the router will check it by comparing the record stored. If it matches, the page will be retrieved quickly. Such item can provide URL matching with the fastest rate.

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

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



Item	Description	
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.	
Black/White List	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.	
	Pass - allow accessing into the corresponding webpage with the characters listed on Group/Object Selections. If the web	

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

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.



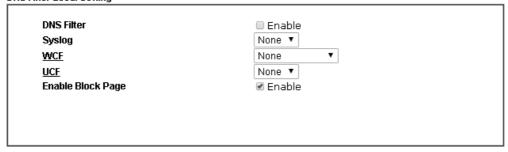
Info

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 Tal	ble		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>	

DNS Filter Local Setting



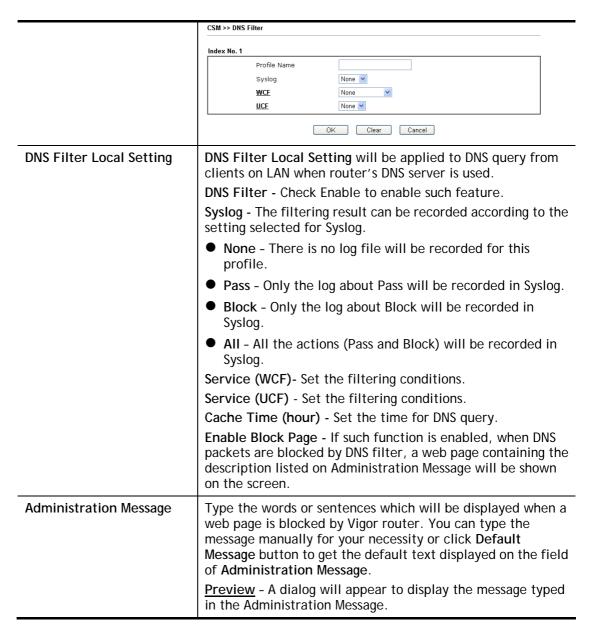
Administration Message	(Max 255 characters)	<u>Preview</u>	Default Mess	age
is categorized with	r> t> t> t> p>The requested W kCL% br>has been blockerator for further inform	ed by %RNAME% DNS	Filter.Plea	
				,

Legend:

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



Item	Description
DNS Filter Profile Table	It displays a list of different DNS filter profiles (with specified WCF and UCF). Click the profile link to open the following page. Then, type the name of the profile and specify WCF/UCF based on your requirement.



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

Application Notes

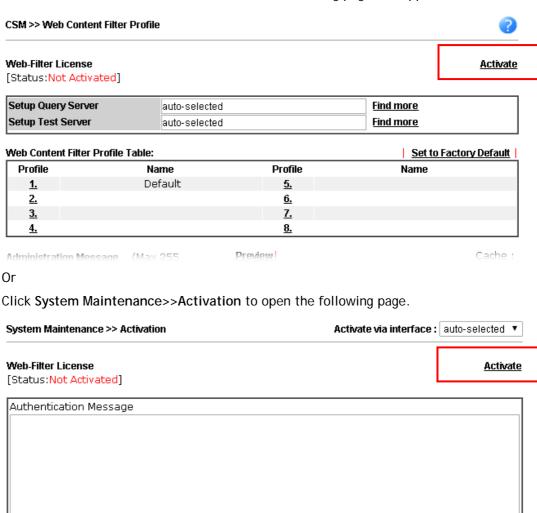
A-1 How to Create an Account for MyVigor

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.

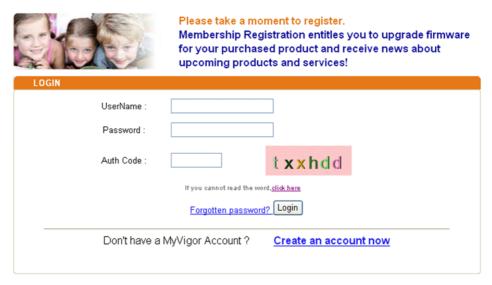
To access into MyVigor for getting more information, please create an account for MyVigor.

Create an Account via Vigor Router

1. Click CSM>> Web Content Filter Profile. The following page will appear.



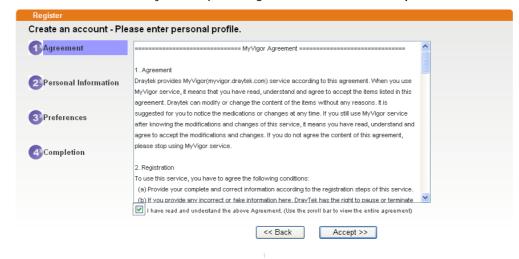
2. Click the Activate link. A login page for MyVigor web site will pop up automatically.



If you are having difficulty logging in, contact our customer service.

Customer Service: (886) 3 597 2727 or

- 3. Click the link of Create an account now.
- 4. Check to confirm that you accept the Agreement and click Accept.



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



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



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



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

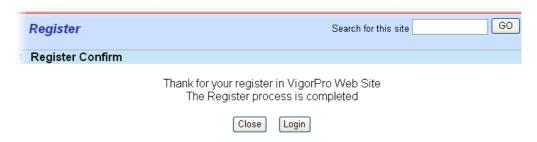
***** This is an automated message from myvigor draytek.com. *****

Thank you (Mary) for creating an account.

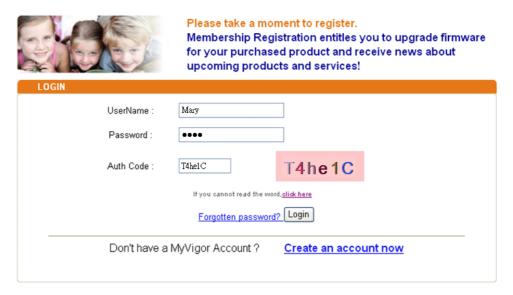
Please click on the activation link below to activate your account

Link: Activate my Account

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



10. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**.



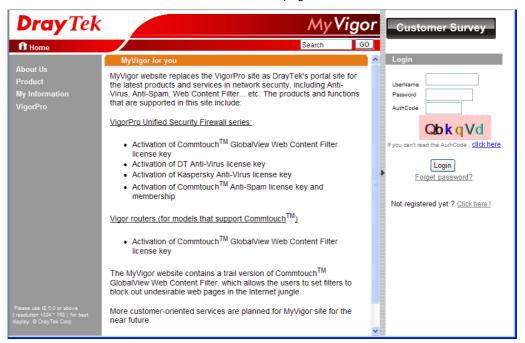
If you are having difficulty logging in, contact our customer service.

Customer Service: (886) 3 597 2727 or

11. Now, click Login. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

Create an Account via MyVigor Web Site

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



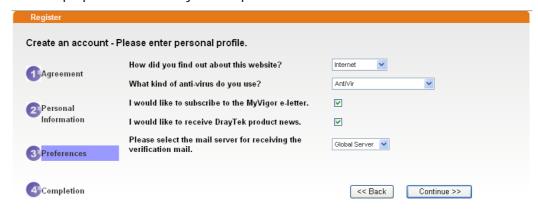
2. Check to confirm that you accept the Agreement and click Accept.



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



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



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



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

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

Thank you (Mary) for creating an account.

Please click on the activation link below to activate your account

Link: Activate my Account

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



The Confirm message of New Owner(Mary) maybe timeout Please try again or contact to draytek.com

Close Login

8. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**. Then type the code in the box of Auth Code according to the value displayed on the right side of it.



If you are having difficulty logging in, contact our customer service.

Customer Service: (886) 3 597 2727 or

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.

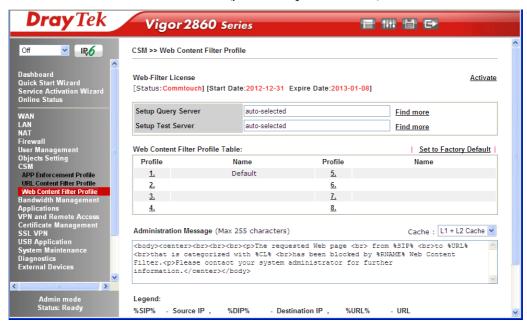
URL Content Filter,

Benefits: Free, flexible for customize webpage.

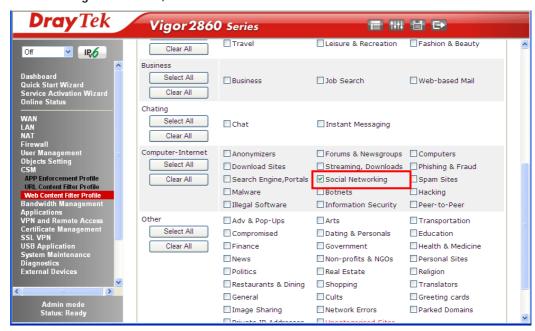
Note: Manual setting (e.g., one keyword for one website.)

I. Via Web Content Filter

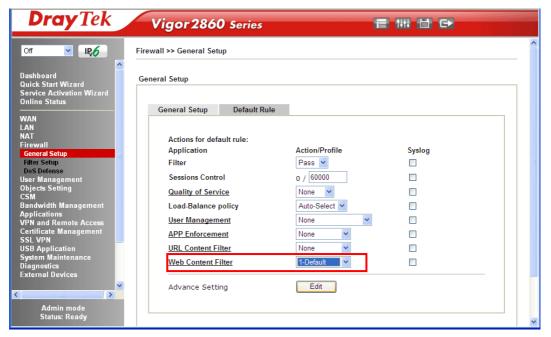
1. Make sure the Web Content Filter (powered by Commtouch) license is valid.



2. Open CSM >> Web Content Filter Profile to create a WCF profile. Check Social Networking with Action, Block.



3. Enable this profile in Firewall>>General Setup>>Default Rule.



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]

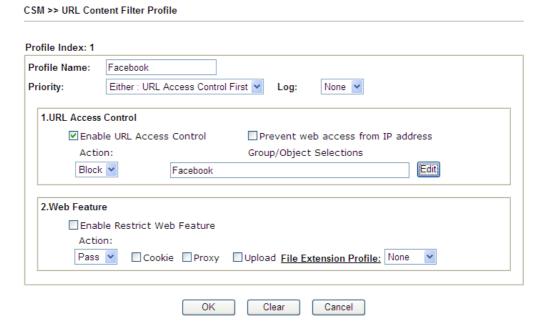
II. Via URL Content Filter

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.

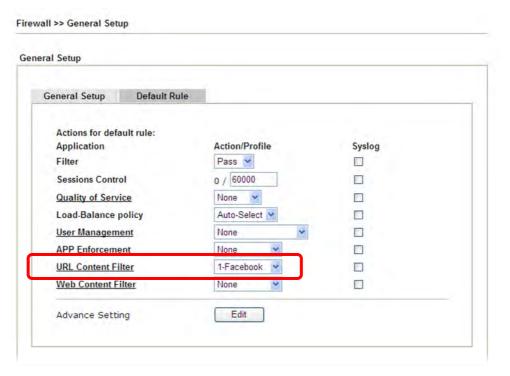


- Open CSM>>URL Content Filter Profile. Click an index number to open the setting page.
- 4. Configure the settings as the following figure.



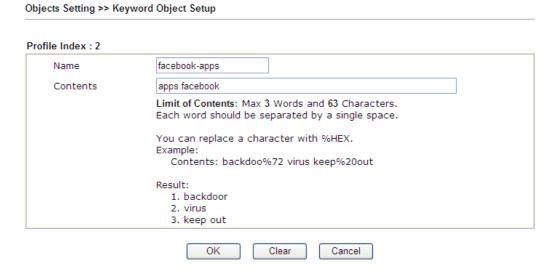
5. When you finished the above steps, click OK. Then, open Firewall>>General Setup.

6. 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.

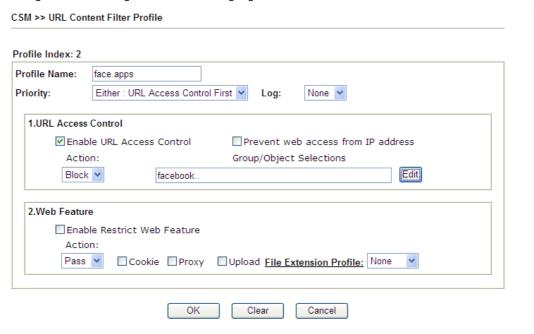


B. Disallow users to play games on Facebook

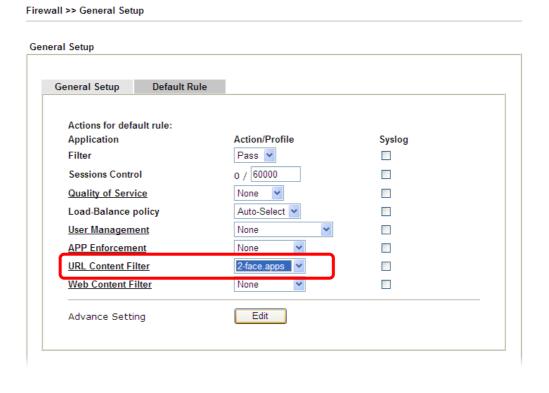
- 1. Open **Object Settings>>Keyword Object**. Click an index number to open the setting page.
- 2. In the field of **Contents**, please type *apps.facebook*. Configure the settings as the following figure.



- 3. Open CSM>>URL Content Filter Profile. Click an index number to open the setting page.
- 4. Configure the settings as the following figure.



- 5. When you finished the above steps, please open Firewall>>General Setup.
- 6. 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.



Part VII 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 bandwith of data transmission through configuration of Sessions Limit, Bandwidth Limit, and Quality of Servie (QoS).





It is a security feature which disallows any IP traffic (except DHCP-related packets) from a particular host until that host has correctly supplied a valid username and password.

User Management

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, Management, Reboot System, Firmware Upgrade and Activation.

Below shows the menu items for System Maintenance.

System Maintenance System Status TR-069 **Administrator Password User Password Login Page Greeting Configuration Backup** SysLog / Mail Alert **Time and Date SNMP** Management Reboot System Firmware Upgrade Modern Code Upgrade Activation Internal Service User List

Web User Interface

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 : Vigor2860Ln Firmware Version : 3.8.2

Build Date/Time : Oct 26 2015 11:07:22

LAN DHCP Server DNS MAC Address IP Address Subnet Mask LAN1 00-1D-AA-DD-75-00 172.17.11.1 255.255.255.0 ON 168.95.1.1 LAN2 00-1D-AA-DD-75-00 192.168.2.1 255.255.255.0 ON 168.95.1.1 LAN3 00-1D-AA-DD-75-00 192.168.3.1 255.255.255.0 ON 168.95.1.1 00-1D-AA-DD-75-00 192.168.4.1 255.255.255.0 ON 00-1D-AA-DD-75-00 192.168.5.1 255.255.255.0 ON 00-1D-AA-DD-75-00 192.168.6.1 255.255.255.0 ON 168.95.1.1 LAN4 168.95.1.1 LAN5 LAN6 168.95.1.1 DMZ PORT 00-1D-AA-DD-75-00 192.168.7.1 255.255.255.0 ON 168.95.1.1 IP Routed Subnet 00-1D-AA-DD-75-00 192.168.0.1 255.255.255.0 ON 168.95.1.1

Wireless LAN				
MAC Address Frequency Firmware Version SSID Domain				
00-1D-AA-DD-75-00	Europe	2.7.1.5	v2860_lte_1	

	WAN				
	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Disconnected	00-1D-AA-DD-75-01	PPPoE		
WAN2	Connected	00-1D-AA-DD-75-02	PPPoE	114.43.184.97	168.95.98.254
LTE	Connected	00-A0-C6-00-00-55	DHCP Client	10.118.138.137	10.118.138.138
WAN4	Disconnected	00-1D-AA-DD-75-04			

	IP	v6	
	Address	Scope	Internet Access Mode
LAN	FE80::21D:AAFF:FEDD:7500/64	Link	

User Mode is OFF now.

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
	- Display the connection type.
	IP Address
	- Display the IP address of the WAN interface.
	Default Gateway
	- Display the assigned IP address of the default gateway.
IPv6	Address - Display the IPv6 address for LAN.
	Scope - Display the scope of IPv6 address. For example, IPv6 Link Local could only be used for direct IPv6 link. It can't be used for IPv6 internet.
	Internet Access Mode - Display the connection mode chosen for accessing into Internet.

VII-1-2 TR-069

System Maintenance >> TR-069 Setting

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.

ACS and CPE Settings ACS Server On Internet ACS Server http://vigoracs.draytek.com/ACSServer/services/ACSServlet URL Username alpha Password Test With Inform | Event Code PERIODIC Last Inform Response Time :Thu Aug 7 10:27:16 2014 🤎 **CPE Client** Enable Disable http://111.251.216.33:8069/cwm/CRN.html URL Port 8069 Username vigor Password Periodic Inform Settings Disable Enable 900 second(s) Interval Time STUN Settings Disable O Enable Server Address Server Port 3478 Minimum Keep Alive Period 60 second(s) -1 second(s) Maximum Keep Alive Period Apply Settings to APs Disable O Enable AP Password OK

Item	Description
ACS Server On	Choose the interface for the router connecting to ACS server.
ACS Server	URL/Username/Password - Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information.
	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.
	Last Inform Response Time - Display the time that VigorACS

	server made a response while receiving Inform message from CPE last time.
CPE Client	Such information is useful for Auto Configuration Server. Enable/Disable - Allow/Deny the CPE Client to connect with Auto Configuration Server.
	Port - Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE. Username and Password - Type the username and password that VigorACS can use to access into such CPE.
Periodic Inform Settings	The default setting is Enable . Please set interval time or schedule time for the router to send notification to CPE. Or click Disable to close the mechanism of notification.
STUN Settings	The default is Disable . If you click Enable , please type the relational settings listed below:
	Server IP - Type the IP address of the STUN server.
	Server Port - Type the port number of the STUN server.
	Minimum Keep Alive Period - If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds".
	Maximum Keep Alive Period - If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.
Apply Settings to APs	This feature is able to apply TR-069 settings (including STUN and ACS server settings) to all of APs managed by Vigor2860 at the same time.
	Disable - Related settings will not be applied to VigorAP.
	Enable - Above settings will be applied to VigorAP after clicking OK to save the configuration. If such feature is enabled, you have to type the password for accessing VigorAP.
	 AP Password - Type the password of the VigorAP that you want to apply Vigor2860's TR-069 settings.

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.

System Maintenance >>	Administrator	Password	Setup
-----------------------	---------------	----------	-------

System Maintenance >> Administrate	or Password Setup		
Administrator Password			
Old Password			
New Password		(Max. 23 characters allowed)	
Confirm Password		(Max. 23 characters allowed)	
Note:Password can contain only a	a-z A-Z 0-9 , ; : . " <	> * + = \ ? @ # ^ ! ()	
Administrator Local User			
Local User			
Local User List			
Index User Name			^
			~
Specific User			
User Name:			
Password:	Confirm Password:		
	Add Edit	Delete	
☑ Enable 'Admin' Login From W	'an		
Administrator LDAP Setting			
Enable LDAP/AD login for Adr	min users		
🗹 Enable 'Admin' Login From W	'an		
LDAP Server Profiles			
LDAP Profile Setup			

Note: Please select 'Admin' from group select box on login UI.

OK

Item	Description
Administrator Password	Old Password - Type in the old password. The factory default setting for password is "admin". New Password -Type in new password in this field. The length of the password is limited to 23 characters. Confirm Password -Type in the new password again.
Administrator Local User	The administrator can login web user interface of Vigor router to modify all of the settings to fit the requirements. This feature allows other user in LAN who can access into the web user interface with the same privilege of the administrator.
	Local User - Check the box to enable the local user configuration.
	Local User List - It displays the username of the local user.
	User Name - Give a user name for the local user.

Password - Type the password for the local user. Confirm Password - Type the password again for confirmation. 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. Enable Admin Login From Wan - The default setting is enabled. It can ensure any user accessing into web user interface of Vigor router through Internet by username/password of "admin/admin". Administrator LDAP Enable LDAP/AD login for Admin users - If it is enabled, any user can access into the web user interface of Vigor router Setting through the LDAP server authentication. Enable Admin Login From Wan - The default setting is enabled. It can ensure any user accessing into web user interface of Vigor router through Internet by username/password of "admin/admin". LDAP Server Profiles - Available profiles will be displayed here under the link of LDAP Profile Setup. LDAP Profile Setup - It allows you to create a new LDAP profile.

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 v	web configuration <u>Set to Factory Default</u>	
Password	(Max. 23 characters allowed)	
Confirm Password	(Max. 23 characters allowed)	
	nly a-z A-Z 0-9 , ; : . " < > * + = \ ? @ # ^ ! () *.Example:'*' or '**' or '***' is illegal, but '123*' or '*45' is OK.	
	ОК	

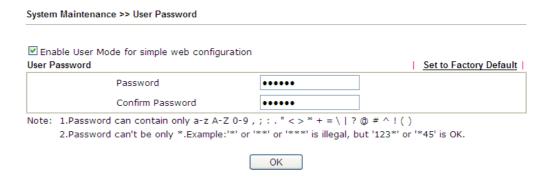
Available settings are explained as follows:

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.
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.



3. The following screen will appear. Simply click **OK**.

System Maintenance >> User Password			
Active Configuration			
	Password	*****	

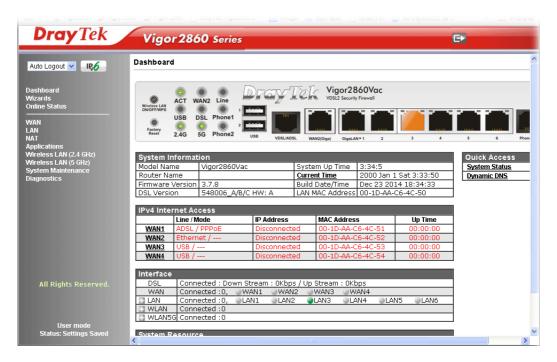
4. Log out Vigor router web user interface by clicking the Logout button.



5. The following window will be open to ask for username and password. Type the new user password in the filed of **Password** and click **Login**.



6. The main screen with User Mode will be shown as follows.



Settings to be configured in User Mode will be less than settings in Admin Mode. Only basic configuration settings will be available in User Mode.



Info

Setting in User Mode can be configured as same as in Admin Mode.

VII-1-5 Login Page Greeting

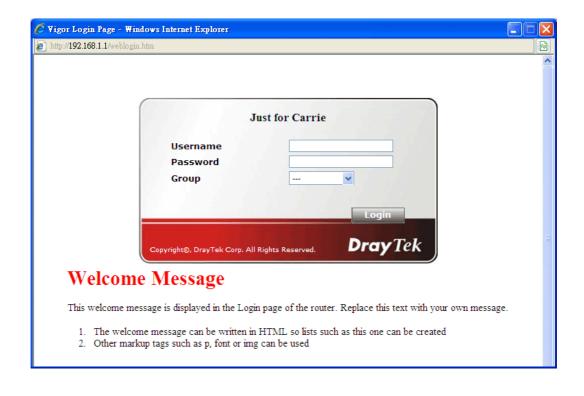
When you want to access into the web user interface of Vigor router, the system will ask you to offer username and password first. At that moment, the background of the web page is blank and no heading will be displayed on the Login window. This page allows you to specify login URL and the heading on the Login window if you have such requirement.



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.



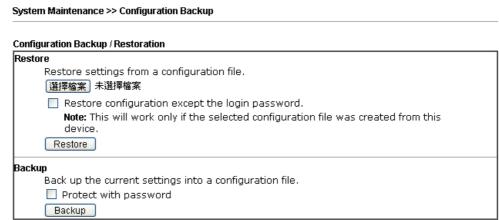
VII-1-6 Configuration Backup

Such function can be used to apply the router settings configured by Vigor2820/ Vigor2830/ Vigor2850 to Vigor2860.

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.



Note: When loading a configuration file from a model in the Supported Model List please note that features and functionality can vary between models so please manually verify the settings after the restoration.

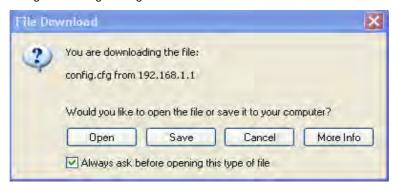
Supported Model List

Model	Firmware Version	Note
Vigor2820	3.3.7.4	Due to different LAN ports between Vigor2820 and Vigor2860, the function "LAN>>VLAN" will be disabled after restarting Vigor2860.The configuration of WAN2 in Vigor2820 will not be converted and applied to WAN2 in Vigor2860 if the physical mode in Vigor2820 is not Ethernet.
Vigor2830	3.6.6.2	Due to different LAN ports between Vigor2830 and Vigor2860, the function "LAN>>VLAN" will be disabled after restarting Vigor2860.
Vigor2850	3.6.6	Due to different LAN ports between Vigor2850 and Vigor2860, the function "LAN>>VLAN" will be disabled after restarting Vigor2860.The configuration of WAN4 in Vigor2850 will not be converted and applied to WAN4 in

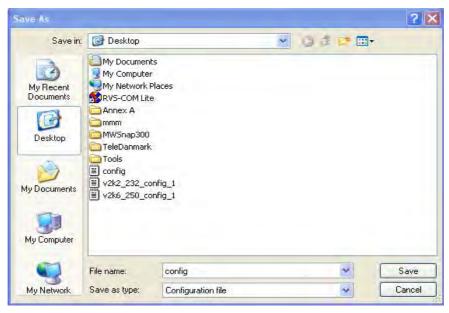
Item	Description	
Restore	Choose File - Click it to specify a file to be restored. Restore configuration except the login password - If the password settings shall not be restored and applied to Vigor2860, simply check this box to get rid of password settings.	
	Click Restore to restore the configuration. If the file is encrypted, the system will ask you to type the password to decrypt the configuration file.	
Backup	Click it to perform the configuration backup of this router.	
	Protect with password- For the sake of security, the configuration file for the router can be encrypted.	

	Backup Back up the current settings into a configuration file. Protect with password Password Confirm Password Backup Mote: When loading a configuration file from a model in the Supported Model Liet please Password - Type several characters as the password for encrypting the configuration file. Confirm Password - Type the password again for confirmation.	
Support Model List	Web configuration file from <i>other</i> Vigor router can be applied to Vigor2860 series. At present, the configuration file of Vigor2820/Vigor2830/Vigor2850 is accepted for Vigor 2860. This field displays model name(s) and firmware which web	
	configuration file saved can be used by such 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.

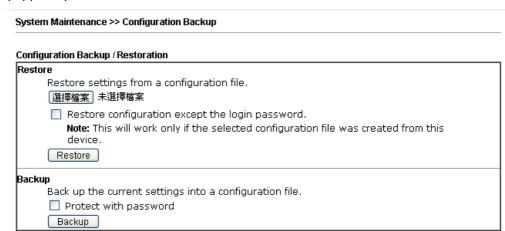


Info

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.



Note: When loading a configuration file from a model in the Supported Model List please note that features and functionality can vary between models so please manually verify the settings after the restoration.

Supported Model List

Model	Firmware Version	Note
Vigor2820	3.3.7.4	Due to different LAN ports between Vigor2820 and Vigor2860, the function "LAN>>VLAN" will be disabled after restarting Vigor2860.The configuration of WAN2 in Vigor2820 will not be converted and applied to WAN2 in Vigor2860 if the physical mode in Vigor2820 is not Ethernet.
Vigor2830	3.6.6.2	Due to different LAN ports between Vigor2830 and Vigor2860, the function "LAN>>VLAN" will be disabled after restarting Vigor2860.
Vigor2850	3.6.6	Due to different LAN ports between Vigor2850 and Vigor2860, the function "LAN>>VLAN" will be disabled after restarting Vigor2860.The configuration of WAN4 in Vigor2850 will not be converted and applied to WAN4 in

- 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 Access Setup	Mail Alert Setup	
SysLog Access Setup I Enable Syslog Save to: I Syslog Server USB Disk Router Name Server IP Address Destination Port Mail Syslog Enable syslog message: I Firewall Log	☐ Enable SMTP Server SMTP Port Mail To Return-Path ☐ Use SSL ☐ Authentication Username Password	Send a test e-mail 25
 ✓ VPN Log ✓ User Access Log ✓ Call Log ✓ WAN Log ✓ Router/DSL information AlertLog Setup Enable AlertLog Port 514 	Enable E-Mail Alert: DoS Attack APPE VPN LOG APPE Signature	

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.



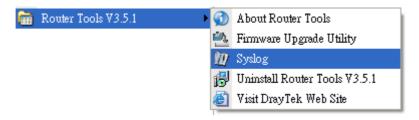
Item	Description
SysLog Access Setup	Enable - Check Enable to activate function of syslog.
	Syslog Save to - Check Syslog Server to save the log to Syslog server.
	Check USB Disk to save the log to the attached USB storage disk.
Router Name	Display the name for such router configured in System Maintenance>>Management.
	If there is no name here, simply lick the link to access into System Maintenance>>Management to set the router name.
	Server IP Address -The IP address of the Syslog server.
	Destination Port - Assign a port for the Syslog protocol.
	Mail Syslog - Check the box to recode the mail event on Syslog.
	Enable syslog message - Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to Syslog.
AlertLog Setup	Check Enable to activate function of alert log.
	AlertLog Port - Type the port number for alert log. The

	default setting is 514.
Mail Alert Setup	Check Enable to activate function of mail alert.
	Send a test e-mail - Make a simple test for the e-mail address specified in this page. Please assign the mail address first and click this button to execute a test for verify the mail address is available or not.
	SMTP Server/SMTP Port - The IP address/Port number of the SMTP server.
	Mail To - Assign a mail address for sending mails out.
	Return-Path - Assign a path for receiving the mail from outside.
	Use SSL - Check this box to use port 465 for SMTP server for some e-mail server uses https as the transmission method.
	Authentication - Check this box to activate this function while using e-mail application.
	User Name - Type the user name for authentication.
	Password - Type the password for authentication.
	Enable E-mail Alert - Check the box to send alert message to the e-mail box while the router detecting the item(s) you specify here.

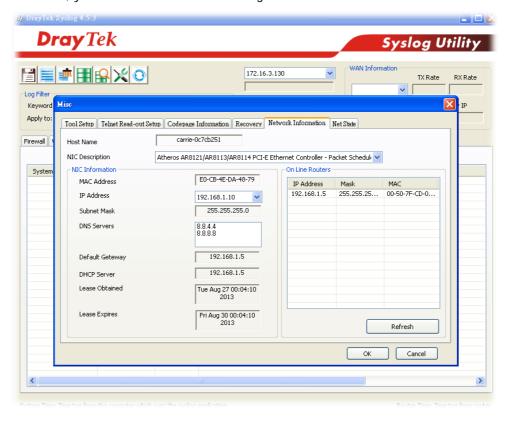
Click **OK** to save these settings.

For viewing the Syslog, please do the following:

- 1. Just set your monitor PC's IP address in the field of Server IP Address
- 2. Install the Router Tools in the **Utility** within provided CD. After installation, click on the **Router Tools>>Syslog** from program menu.



3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.



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 2014 Aug 7 Thu 11:32:12 Inquire Time Time Setup O Use Browser Time O Use Internet Time Time Server pool.ntp.org Priority Auto v Time Zone (GMT+08:00) Taipei Enable Daylight Saving Advanced Automatically Update Interval 1 day ΟK Cancel

Available settings are explained as follows:

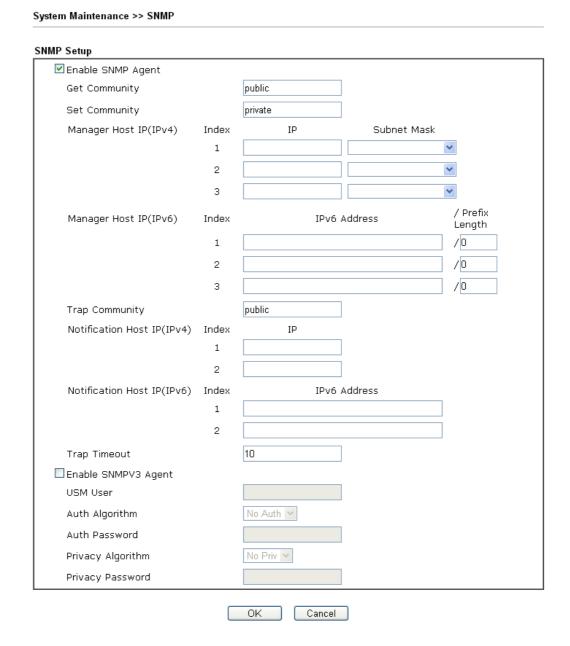
Item	Description
Current System Time	Click Inquire Time to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.
Time Server	Type the 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	Check the box to enable the daylight saving. Such feature is available for certain area. Advanced - Click it to open a pop up dialog. Daylight Saving Advanced Default Start: No Daylight Saving End: No Daylight Saving Date Range Start: Year Month Day 00:00 End: Yearly Start: Yearly On Janual First Sunda 00:00 End: Yearly On Janual First Sunda 00:00 Use the default time setting or set user defined time for your requirement.
Automatically Update Interval	Select a time interval for updating from the NTP server.

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.



Item	Description
Enable SNMP Agent	Check it to enable this function.
Get Community	Set the name for getting community by typing a proper character. The default setting is public . 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. No Auth No Auth MD5 SHA
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. No Priv No Priv DES AES
Privacy Password	Type a password for privacy. The maximum length of the text is limited to 23 characters.

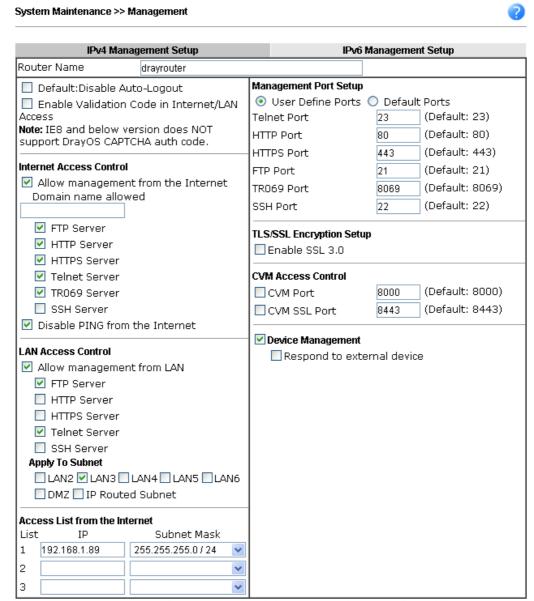
Click **OK** to save these settings.

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, CVM Access Control and Device Management.

The management pages for IPv4 and IPv6 protocols are different.

For IPv4



Note: Subnet LAN1 is always allowed to access all the router services regardless of "LAN Access Control" settings.



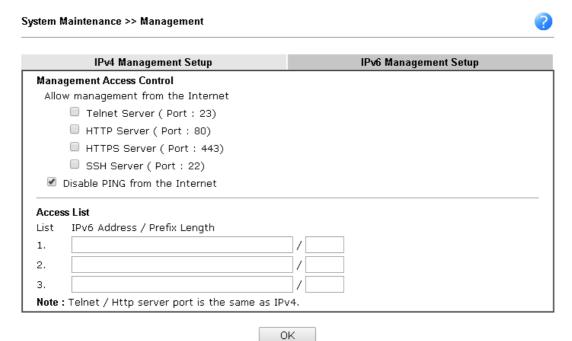
Item	Description
Router Name	Type in the router name provided by ISP.
Default: Disable	If it is enabled, the function of auto-logout for web user

Auto-Logout	interface will be disabled.
	Off PG
	The web user interface will be open until you click the Logout icon manually.
	Logout
Enable Validation Code in Internet/LAN Access	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.
Internet Access Control	Allow management from the Internet - Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.
	Disable PING from the Internet - Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.
LAN Access Control	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.
Access List from the Internet	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.
	List IP - Indicate an IP address allowed to login to the router. Subnet Mask - Represent a subnet mask allowed to login to the router.
Management Port Setup	User Define Ports - Check to specify user-defined port numbers for the Telnet, HTTP, HTTPS, FTP, TR-069 and SSH servers.
	Default Ports - Check to use standard port numbers for the Telnet and HTTP servers.
TLS/SSL Encryption Setup	Enable SSL 3.0 - Check the box to enable the function of SSL 3.0 if required.
	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.
CVM Access Control	CVM Port - Check the box to enable such port setting. CVM SSL Port - Check the box to enable such port setting.

Device Management	Check the box to enable the device management function for Vigor2860.
	Respond to external device - If it is enabled, Vigor2860 will be regarded as slave device. When the external device (master device) sends request packet to Vigor2860, Vigor2860 would send back information to respond the request coming from the external device which is able to manage Vigor2860.

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

For IPv6



Available settings are explained as follows:

Item	Description
Management Access Control	Allow management from the Internet - Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.
	Disable PING from the Internet - Check the checkbox to disable all PING packets from the Internet. For security issue, this function is enabled by default.
Access List	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.
	IPv6 Address /Prefix Length- Indicate the IP address(es) allowed to login to the router.

After finished the above settings, click \mathbf{OK} to save the configuration.

VII-1-11 Reboot System

The Web user interface may be used to restart your router. Click **Reboot System** from **System Maintenance** to open the following page.

System Maintenance >> Reboot System		
Reboot System		
Do you want to reboot your router ?		
Using current configuration		
 Using factory default configuration 		
Reboot Now		
Auto Reboot Time Schedule		
Index(1-15) in <u>Schedule</u> Setup:,,,		
Note: Action and Idle Timeout settings will be ignored.		
OK Cancel		

Index (1-15) in Schedule Setup - You can type in four sets of time schedule for performing system reboot. All the schedules can be set previously in Applications >> Schedule web page and you can use the number that you have set in that web page.

If you want to reboot the router using the current configuration, check **Using current configuration** and click **Reboot Now**. To reset the router settings to default values, check **Using factory default configuration** and click **Reboot Now**. The router will take 5 seconds to reboot the system.



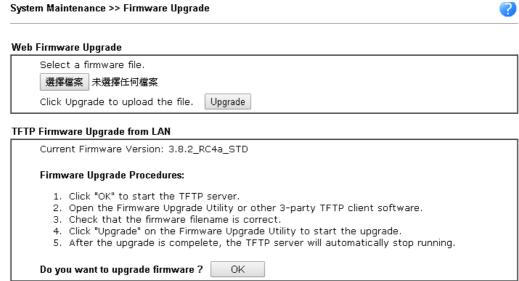
Info

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-1-12 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.

Click System Maintenance>> Firmware Upgrade to launch the Firmware Upgrade Utility.



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.

System Maintenance >> Firmware Upgrade

TFTP server is running. Please execute a Firmware Upgrade Utility software to upgrade router's firmware. This server will be closed by itself when the firmware upgrading finished.

For the detailed information about firmware update, please go to Chapter 5.

VII-1-13 Modem Code Upgrade

This function is used to upgrade modem code if you find built-in modem code is not suitable for Vigor router. Contact with your dealer for further assistance if required.

System Maintenance >> Modem Code Upgrade		
Web DSL Modem Code Upgrade		
Select a modem code file.		
Select		
Click Upgrade to upload the file. Upgrade		

VII-1-14 Activation

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

After you have finished the setting profiles for WCF (refer to Web Content Filter Profile), it is the time to activate the mechanism for your computer.

Click **System Maintenance>>Activation** to open the following page for accessing http://myvigor.draytek.com.

e: auto-selected ▼
<u>Activate</u>

Note: If you want to use email alert or syslog, please configure the <u>SysLog/Mail Alert Setup</u> page.

If you change the service provider, the configuration of the function will be reset.



Item	escription		
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:



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-1-15 Internal Service User List

User profiles (clients) defined and enabled in **User Management>>User Profile** will be displayed in this page.

Such page allows you to turn on or turn off security authentication service (offered by inernal RADIUS and/or Local 802.1X) for each user profile without accessing into the User Management configuration page.

Swetom	Maintenance	>>	Intornal	Convice	Hear	Liet

User Name	Radius	Local 802.1X	User Name	Radius	Local 802.1X
test 1	✓		<u>test sales</u>		
		OK (Cancel		

Note:

- 1. Only the user profiles which is enabled in User Management >> User Profile will be listed here.
- If you enable RADIUS or Local 802.1X for a user profile here, it will use the default authentication methods; however, you may change its authentication methods via User <u>Management >> User Profile</u>.

Available settings are explained as follows:

Item	Description
User Name	Display the name of the existed user profile. To modify the detailed settings, simply click the user name link to access into the web page for modification.
Radius	Check the box to turn on the security authentication service offered by internal RADIUS server for the user profile. Uncheck the box to turn off ecurity authentication service offered by internal RADIUS server for the user profile. If you check the box next to such item, all of the user profiles listed in this page will be enabled with RADIUS service enabled vice versa.
Local 802.1X	Check the box to turn on the security authentication service offered by Local 802.1X server for the user profile. Uncheck the box to turn off ecurity authentication service offered by Local 802.1X server for the user profile. If you check the box next to such item, all of the user profiles listed in this page will be enabled with Local 802.1X service enabled; vice versa.



Info

For the detailed setting (such as IP address, port number) configuration of internal RADIUS, refer to Applications>>RADIUS/TACACS+.

For the detailed setting (such as IP address, port number) configuration of Local 802.1X, refer to LAN>>Wired 802.1X and Wireless LAN>>Security.

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?

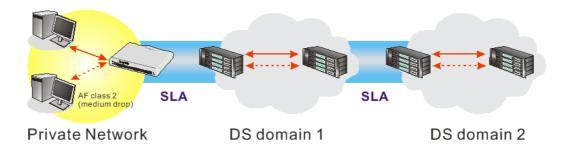
There are two components within Primary configuration of QoS deployment:

- 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 Sessions Limit O Enable O Disable Default Max Sessions: 100 Limitation List Index Start IP End IP Max Sessions Specific Limitation End IP: Start IP: Maximum Sessions: Add Edit Delete Administration Message (Max 256 characters) Preview | Default Message You have reached the maximum number of permitted Internet sessions.Please close one or more applications to allow further Internet access.Contact your system administrator for further information. Time Schedule Index(1-15) in Schedule Setup: Note: Action and Idle Timeout settings will be ignored. OK

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

	used for each computer in LAN.
Limitation List	Displays a list of specific limitations that you set on this web page.
Specific Limitation	Start IP- Defines the start IP address for limit session.
	End IP - Defines the end IP address for limit session.
	Maximum Sessions - Defines the available session number for each host in the specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index.
	Add - Adds the specific session limitation onto the list above.
	Edit - Allows you to edit the settings for the selected limitation.
	Delete - Remove the selected settings existing on the limitation list.
Administration Message	Type the words which will be displayed when reaches the maximum number of Internet sessions permitted.
	Default Message - Click this button to apply the default message offered by the router.
Time Schedule	Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page.

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

VII-2-2 Bandwidth Limit

Bandwidth Management >> Bandwidth Limit

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

Bandwidth Limit O Enable IP Routed Subnet O Disable Default TX Limit: 2000 Kbps ▼ Default RX Limit: 8000 Allow auto adjustment to make the best utilization of available bandwidth. **Limitation List** Index Start IP End IP TX limit RX limit Shared Specific Limitation End IP: Start IP: Kbps V RX Limit: Kbps 🕶 Edit Delete Smart Bandwidth Limit For any LAN IP Not in Limitation List, when session number exceeds 1000 TX Limit: 200 Kbps V RX Limit: 800 Kbps 🗸 Note: For TX/RX, a setting of "0" means unlimited bandwidth. Time Schedule Index(1-15) in Schedule Setup: Note: Action and Idle Timeout settings will be ignored. ΟK

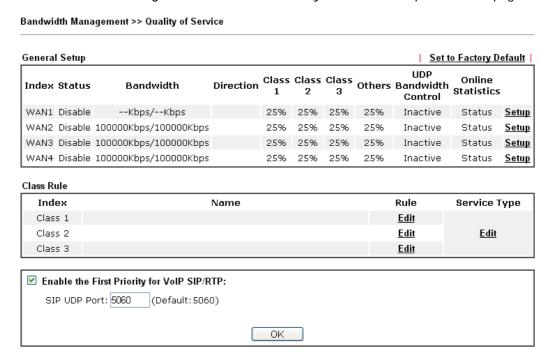
To activate the function of limit bandwidth, simply click **Enable** and set the default upstream and downstream limit.

Item	Description	
Bandwidth Limit	Enable - Click this button to activate the function of limit bandwidth.	
	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 TX limit - Define the default speed of the upstream for each computer in LAN.	
	Default RX limit - Define the default speed of the downstream for each computer in LAN.	
	Allow auto adjustment···- Check this box to make the best utilization of available bandwidth.	
Limitation List	Display a list of specific limitations that you set on this web page.	

Start IP - Define the start IP address for limit bandwidth.
End IP - Define the end IP address for limit bandwidth.
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.
TX limit - Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
RX limit - Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
Add - Add the specific speed limitation onto the list above.
Edit - Allow you to edit the settings for the selected limitation.
Delete - Remove the selected settings existing on the limitation list.
Check this box to have the bandwidth limit determined by the system automatically.
TX limit - Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
RX limit - Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
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.

VII-2-3 Quality of Service

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



Item	Description	
General Setup	Index - Display the WAN/LTE interface number that you can edit.	
	Status - Display if the WAN interface is available for such function or not.	
	Bandwidth - Display the inbound and outbound bandwidth setting for the WAN interface.	
	Direction - Display which direction that such function will influence.	
	Class 1/Class2/Class 3/Others - Display the bandwidth percentage for each class.	
	UDP Bandwidth Control - Display the UDP bandwidth control is enabled or not.	
	Online Statistics - Display an online statistics for quality of service for your reference.	
	Setup - Allow to configure general QoS setting for WAN interface.	
Class Rule	Index - Display the class number that you can edit.	
	Name - Display the name of the class.	
	Rule - Allow to configure detailed settings for the selected Class.	
	Service Type - Allow to configure detailed settings for the service type.	
Enable the First Priority	When this feature is enabled, the VoIP SIP/UDP packets will be	

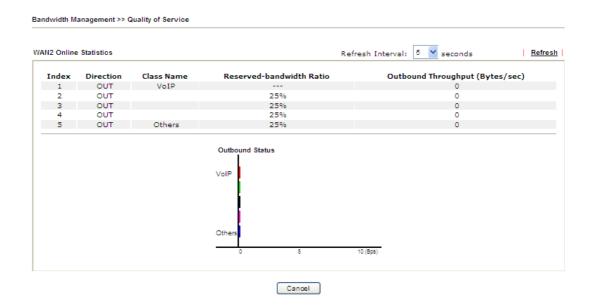
Item	Description
for VoIP SIP/RTP	sent with highest priority.
	SIP UDP Port - Set a port number used for SIP.

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

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

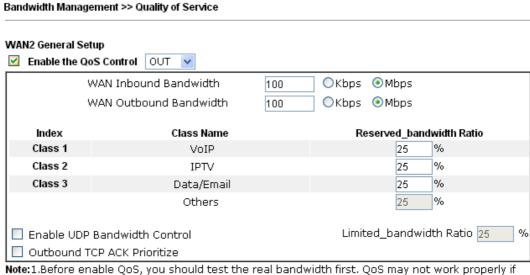
Online Statistics

Display an online statistics for quality of service for your reference. This feature is available only when the Quality of Service for WAN interface is enabled.



General Setup for WAN Interface

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



Note: 1. Before enable QoS, you should test the real bandwidth first. QoS may not work properly if the bandwidth is not accurate.

2.You can do speed test by http://speedtest.net or contact with your ISP for speed test program.



Item	Description
Enable the QoS Control	The factory default for this setting is checked.
	Please also define which traffic the QoS Control settings will apply to.
	IN- apply to incoming traffic only.
	OUT-apply to outgoing traffic only.
	BOTH- apply to both incoming and outgoing traffic.
	Check this box and click OK , then click Setup link again. You will see the Online Statistics link appearing on this page.
WAN Inbound Bandwidth	It allows you to set the connecting rate of data input 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.
WAN Outbound Bandwidth	It allows you to set the connecting rate of data output for other WAN. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 256kbps for this box. The default value is 10000kbps.
Reserved Bandwidth Ratio	It is reserved for the group index in the form of ratio of reserved bandwidth to upstream speed and reserved bandwidth to downstream speed.
Enable UDP Bandwidth Control	Check this and set the limited bandwidth ratio on the right field. This is a protection of TCP application traffic since UDP application traffic such as streaming video will exhaust lots of bandwidth.
Outbound TCP ACK	The difference in bandwidth between download and upload

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



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.

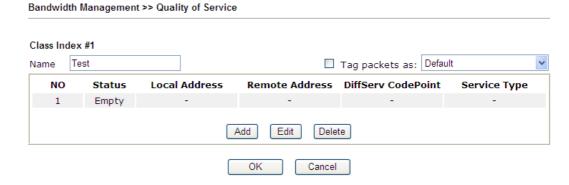
Edit the Class Rule for QoS

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 Edit link of that one.

Bandwidth Management >> Quality of Service General Setup Set to Factory Default UDP Class Class Class Online **Index Status** Bandwidth Direction Others Bandwidth Statistics Control --Kbps/--Kbps WAN1 Disable 25% 25% 25% Inactive 25% Status Setup WAN2 Disable 100000Kbps/100000Kbps 25% 25% 25% 25% Inactive. Status <u>Setup</u> WAN3 Disable 100000Kbps/100000Kbps Inactive 25% 25% 25% 25% Status <u>Setup</u> WAN4 Disable 100000Kbps/100000Kbps 25% 25% 25% 25% Inactive Status <u>Setup</u> Class Rule Index Rule Name Service Type Class 1 <u>Edit</u> Class 2 <u>Edit</u> <u>Edit</u> Class 3 <u>Edit</u> ☑ Enable the First Priority for VolP SIP/RTP: SIP UDP Port: 5060 (Default: 5060)

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

0K



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

Bandwidth Management >> Quality of Service

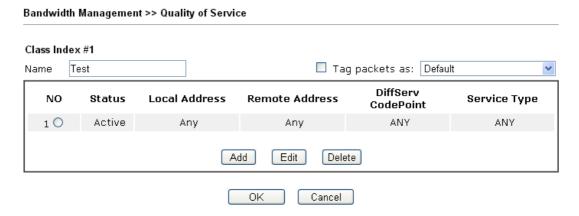


Available settings are explained as follows:

Itam	Description
Item	Description
ACT	Check this box to invoke these settings.
Ethernet Type	Please specify which protocol (IPv4 or IPv6) will be used for this rule.
Local Address	Click the Edit button to set the local IP address (on LAN) for the rule.
Remote Address	Click the Edit button to set the remote IP address (on LAN/WAN) for the rule.
	http://192.168.1.1/doc/QosfpEdt.htm - Microsoft Internet Explorer
	Address Type Start IP Address End IP Address Subnet Mask OK Close Address Type - Determine the address type for the source address. For Single Address, you have to fill in Start IP address and End IP address. For Subnet Address, you have to fill in Start IP address and End IP address, you have to fill in Start IP address and End IP address, you have to fill in Start IP address and End IP address, you have to fill in Start IP address and
DiffCom, Codo Doint	Subnet Mask.
DiffServ CodePoint	All the packets of data will be divided with different levels and will be processed according to the level type by the system. Please assign one of the levels of the data for processing with QoS control.
Service Type	It determines the service type of the data for processing with QoS control. It can also be edited. You can choose the predefined service type from the Service Type drop down list. Those types are predefined in factory. Simply choose the one that you want for using by current QoS.

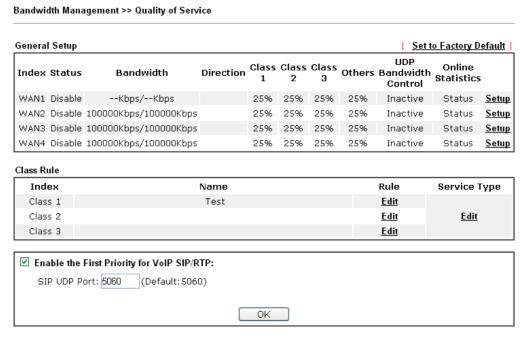
4. After finishing all the settings here, please click **OK** to save the configuration.

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



Edit the Service Type for Class Rule

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



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



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



Available settings are explained as follows:

Item	Description
Service Name	Type in a new service for your request. The maximum length of the name you can set is 11 characters.
Service Type	Choose the type (TCP, UDP or TCP/UDP or other) for the new service.
Port Configuration	Type - Click Single or Range as the Type. If you select Range, you have to type in the starting port number and the end porting number on the boxes below. Port Number - Type in the starting port number and the end porting number here if you choose Range as the type.

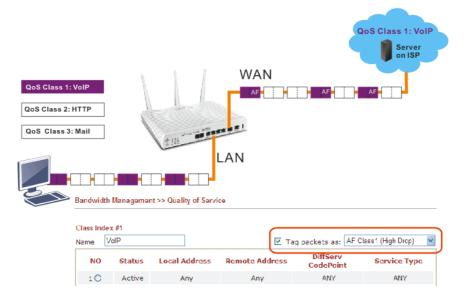
5. After finishing all the settings here, please click **OK** to save the configuration.

By the way, you can set up to 10 service types. If you want to edit/delete an existed service type, please select the radio button of that one and click **Edit/Edit** for modification.

Retag the Packets for Identification

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

For example, in the following illustration, the VoIP packets in LAN go into Vigor router without any header. However, when they go forward to the Server on ISP through Vigor router, all of the packets are tagged with AF (configured in Bandwidth >>QoS>>Class) automatically.



Application Notes

A-1 How to Optimize the Bandwidth through QoS Technology

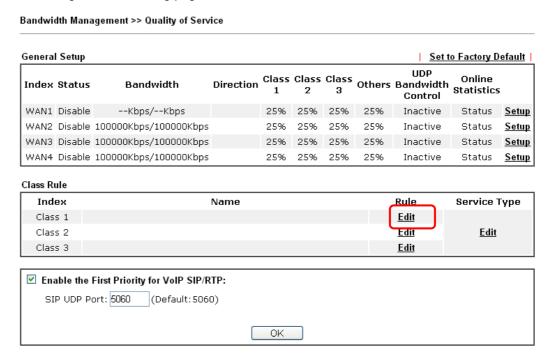
Have you ever gotten any problems in uploading/downloading files (Voice, video or email/data only) with the narrow/districted bandwidth you may share from the common Internet connection line? The advanced bandwidth management technology-QoS (Quality of Service) helps you to well allocate the bandwidth upon your demand of Voice, Video, or Data transferring. Let's see how to get the optimum bandwidth per your request by using DrayTek Vigor router as below.

Scenario: The Internet connection you got from ISP line is 2MB/512Kb. There are VoIP telephony network, IPTV set top box and data server at your home. Assume you want to allocate 30% of the bandwidth you got to VoIP demand, 50% for IPTV, 15% for mail/data, 5% for others. Let's see how easily it is to do the setting as below:

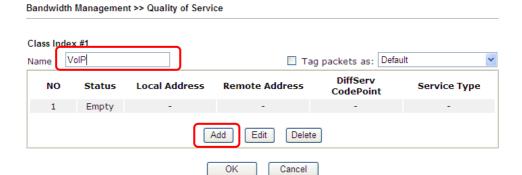
1. Open Bandwidth Management>> Quality of Service.



2. You will get the following page. Click the Edit link for Class 1.



3. In the following page, type a name (e.g., VoIP) for such class and click Add.

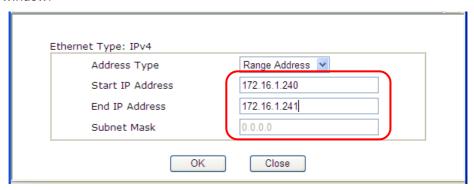


Check the box of ACT. Click Edit to specify the local address.

Bandwidth Management >> Quality of Service

Rule Edit ✓ ACT ⊙ IPv4 ○ IPv6 Ethernet Type Local Address Edit Any Edit Remote Address ANY DiffServ CodePoint Service Type ---Predefined---Note: Please choose/setup the Service Type first. OK Cancel

5. In the pop-up window, choose Range Address as the Address Type and type the start IP address and end IP address in relational fields. Click OK to save the settings and exit the window.

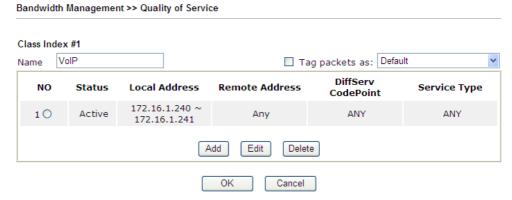


6. Click **OK** again to save the settings.

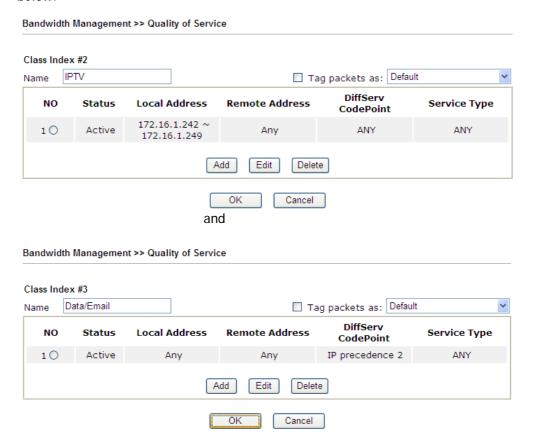
Bandwidth Management >> Quality of Service

Rule Edit ✓ ACT Ethernet Type Local Address 172.16.1.240~172.16.1.241 Edit Remote Address Edit DiffServ CodePoint ANY Service Type ---Predefined---Note: Please choose/setup the $\underline{\textbf{Service Type}}$ first. OK Cancel

7. The class rule for VoIP has been set. Click **OK** to return to previous page.

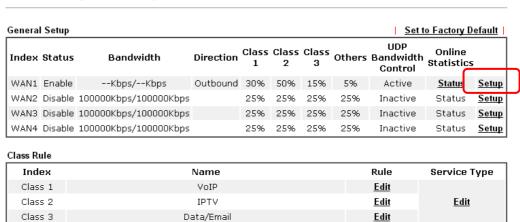


8. Do the same steps to add class rules for IPTV and Data/Email with IP addresses as shown below.

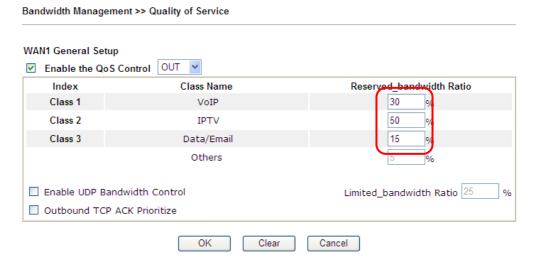


9. Assuming you get 2MB/512Kb Internet line. You can click the **Setup** link of WAN1 to set up the bandwidth for different groups among VoIP, IPTV and Data/Email.

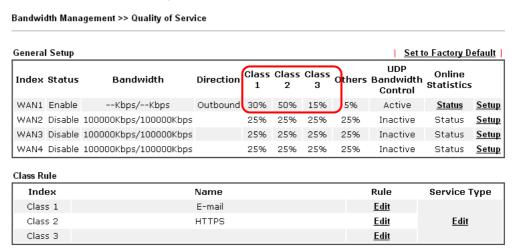
Bandwidth Management >> Quality of Service



 In the Setup page, check the box of Enable the QoS Control. Type 30, 50 and 15 in the boxes for VoIP, IPTV and Data/Email respectively. Check the box of Enable UDP Bandwidth Control.



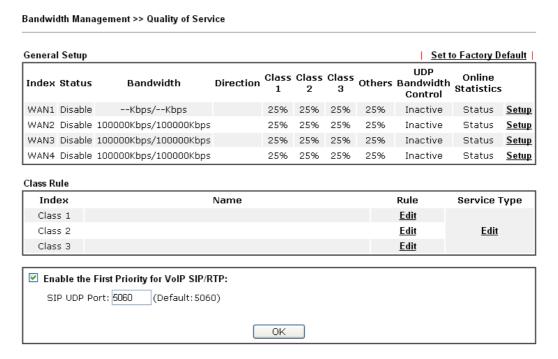
11. Click OK to save the settings. The class rules for WAN1 are defined as shown below.



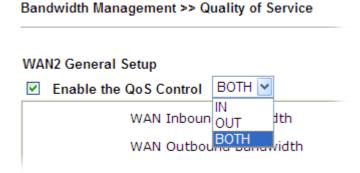
A-2 QoS Setting Example

Assume a teleworker sometimes works at home and takes care of children. When working time, he would use Vigor router at home to connect to the server in the headquarter office downtown via either HTTPS or V PN to check email and access internal database. Meanwhile, children may chat on Skype in the restroom.

1. Go to Bandwidth Management>>Quality of Service.



2. Click **Setup** link of WAN(1/2/3). Make sure the QoS Control on the left corner is checked. And select **BOTH** in **Direction**.



3. Set Inbound/Outbound bandwidth.

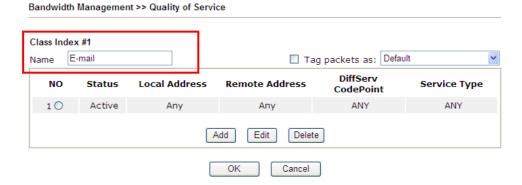




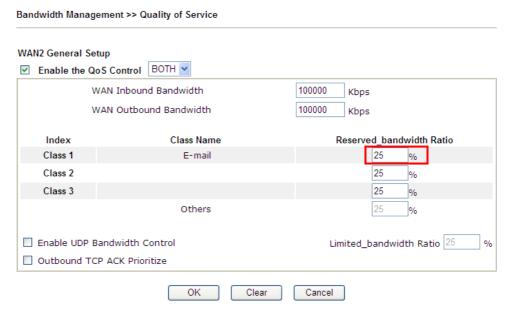
Info

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.

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



5. Click the **Setup** link for WAN2. The user can set reserved bandwidth (e.g., 25%) for **E-mail** using protocol POP3 and SMTP. Click **OK** to save the settings.

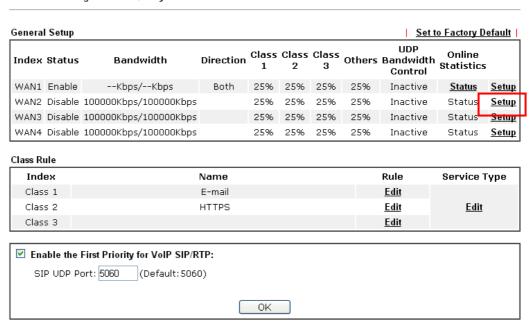


6. Return to previous page. Enter the Name of Index Class #2 by clicking Edit link. In this index, the user will set reserved bandwidth for HTTPS. And click OK.

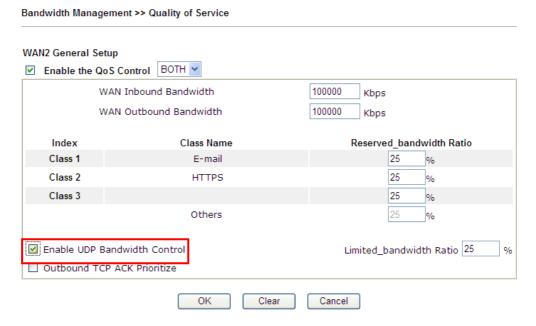


7. Click Setup link for WAN2.

Bandwidth Management >> Quality of Service

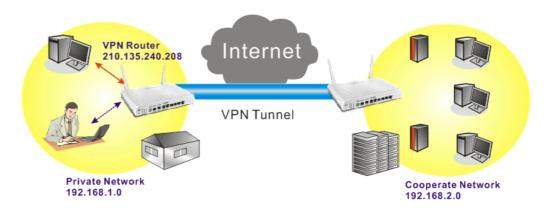


8. Check **Enable UDP Bandwidth Control** on the bottom to prevent enormous UDP traffic influence other application. Click **OK**.



9. If the worker has connected to the headquarter using host to host VPN tunnel. (Please refer to Chapter 3 VPN for detail instruction), he may set up an index for it. Enter the

Class Name of Index 3. In this index, he will set reserved bandwidth for 1 VPN tunnel.



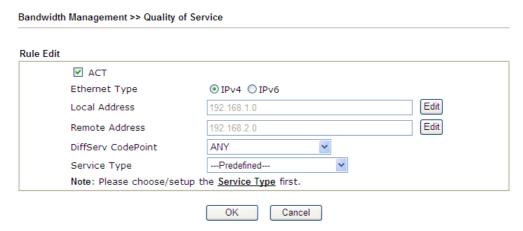
10. Click Edit for Class 3 to open a new window. In this index, the user will set reserved bandwidth for VPN.



11. Click Add to open the following window. Check the ACT box, first.

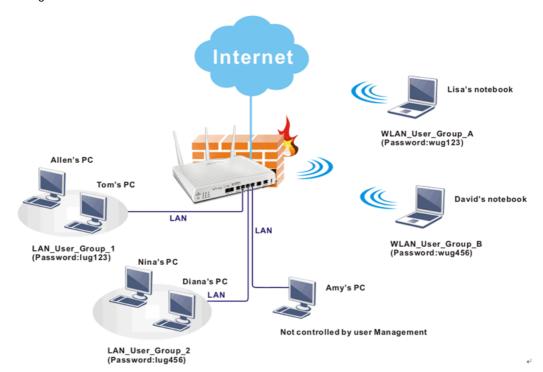


12. Then click **Edit** of **Local Address** to set a worker's subnet address. Click **Edit** of **Remote Address** to set headquarter's IP address. Leave other fields and click **OK**.



VII-3 User Management

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





Info

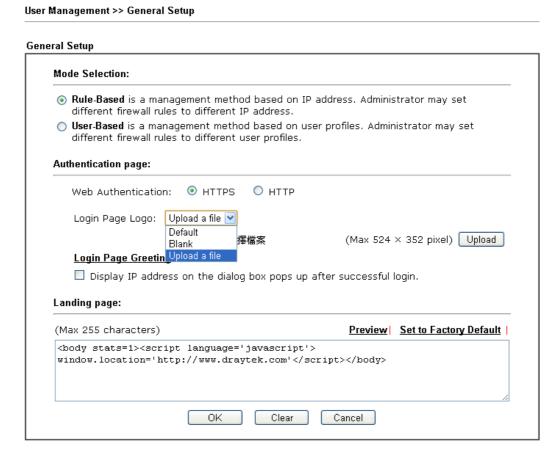
Filter rules configured under Firewall usually are applied to the host (the one that the router installed) only. With user management, the rules can be applied to every user connected to the router with customized profiles.

Web User Interface

User Management General Setup User Profile User Group User Online Status

VII-3-1 General Setup

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



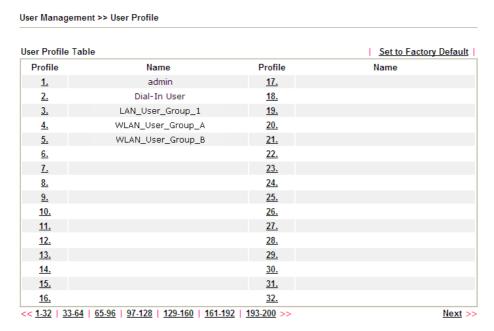
Item	Description
Mode	There are two modes offered here for you to choose. Each mode will bring different filtering effect to the users involved.
	User-Based - If you choose such mode, the router will apply the filter rules configured in User Management>>User Profile to the users.
	Rule-Based -If you choose such mode, the router will apply the filter rules configured in Firewall>>General Setup and

	Filter Rule to the users.
Authentication page	Web Authentication - Choose the protocol for web authentication.
	Login Page Logo - A logo which can be used as an identification of enterprise can be uploaded and displayed on the login page. You can use the default one, blank page or upload other image files (the size no mare than 524 × 352 pixel) to have an image of enterprise or have the effect of advertisement.
	<u>Login Page Greeting</u> - Such link allows you to access into the setting page for login greeting. For detailed information, refer to System Maintenance>>Login Page Greeting.
	Display IP Address on tracking window - Check the box to display the IP address of the client on the tracking window.
Landing Page	Type the information to be displayed on the first web page when the LAN user accessing into Internet via such router.

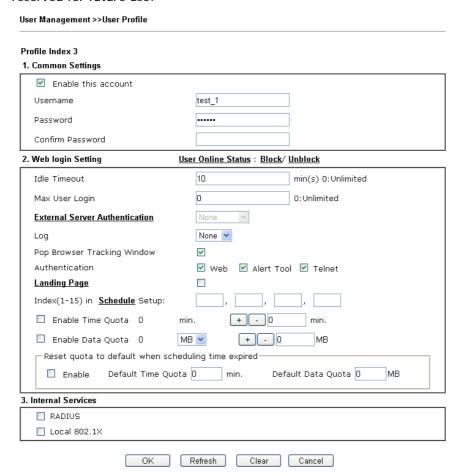
After finishing all the settings here, please click \mathbf{OK} to save the configuration.

VII-3-2 User Profile

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



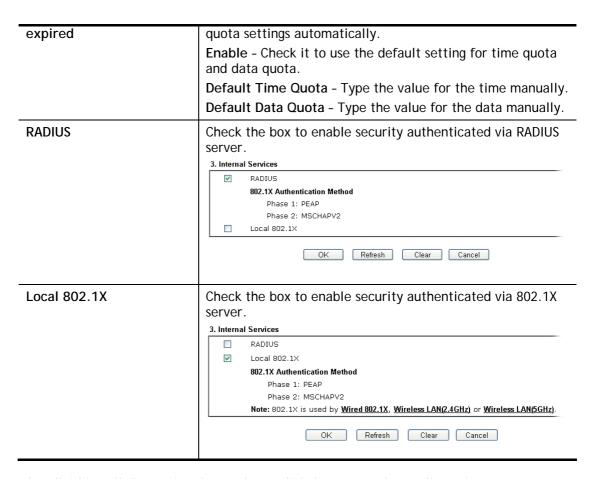
To set the user profile, please click any index number link to open the following page. Notice that profile 1 (admin) and profile 2 (Dial-In User) are factory default settings. Profile 2 is reserved for future use.



Item	Description
Enable this account	Check this box to enable such user profile.
User Name	Type a name for such user profile (e.g., LAN_User_Group_1, WLAN_User_Group_A, WLAN_User_Group_B, etc). When a user tries to access Internet through this router, an authentication step must be performed first. The user has to type the User Name specified here to pass the authentication. When the user passes the authentication, he/she can access Internet via this router. However the accessing operation will be restricted with the conditions configured in this user profile. The maximum length of the name you can set is 24 characters.
Password	Type a password for such profile (e.g., <i>lug123</i> , <i>wug123</i> , <i>wug456</i> , etc). When a user tries to access Internet through this router, an authentication step must be performed first. The user has to type the password specified here to pass the authentication. When the user passes the authentication, he/she can access Internet via this router with the limitation configured in this user profile. The maximum length of the password you can set is 24 characters.
Confirm Password	Type the password again for confirmation.
Idle Timeout	If the user is idle over the limitation of the timer, the network connection will be stopped for such user. By default, the Idle Timeout is set to 10 minutes.
Max User Login	Such profile can be used by many users. You can set the limitation for the number of users accessing Internet with the conditions of such profile. The default setting is 0 which means no limitation in the number of users.
Policy	It is available only when User-Based mode selected in User Management>>General Setup. Default [Create New Policy] Default - If you choose such item, the filter rules pre-configured in Firewall can be adopted for such user profile. Create New Policy - If you choose such item, the following page will be popped up for you to define another filter rule as a new policy.

	Firewall >> Edit Filter Set >> Edit Filter Rule	
	Filter Set 1 Rule 2 Check to enable the Filter Rule Comments: Index(1-15) in Schedule Setup: Clear sessions when schedule ON: Direction: Source IP: Destination IP: Service Type: For the detailed configuration Firewall>>Filter Rule. The firewall>>Generation available for use in User Man	irewall filter rules that are not also also also be
External Service Authentication	external service such as LDAF TACACS+ server. If LDAP, Rachere, it is not necessary to coabove. None None LDAP Radius TACACS+	dius or TACACS+ is selected onfigure the password setting
Log		unblock for the user(s) can be og. Please choose any one of the onal records for the user(s).
Pop Browser Tracking Window		time remaining for connection er, the system will update the connection always on. Thus,
Authentication	first. There are three ways of to choose for authentication. Web - If it is selected, the us router from any browser. The popped up and ask the user t password for authentication. Message (configured in User Setup) will be displayed. After destination URL (if requested automatically by the router. Alert Tool - If it is selected, to type the user name and passon.	t be authenticated by the router fered by the router for the user the can type the URL of the en, a login window will be o type the user name and If succeed, a Welcome Management >> General er authentication, the I by the user) will be guided the user can open Alert Tool and

	be displayed. Next, the user can access Internet through any browser on Windows. Note that Alert Tool can be downloaded from DrayTek web site. Telnet - If it is selected, the user can use Telnet command to perform the authentication job.
Landing Page	When a user tries to access into the web user interface of Vigor router series with the user name and password specified in this profile, he/she will be lead into the web page configured in Landing Page field in User Management>>General Setup. Check this box to enable such function.
Index (1-15) in Schedule Setup	You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page.
Enable Time Quota	Time quota means the total connection time allowed by the router for the user with such profile. Check the box to enable the function of time quota. The first box displays the remaining time of the network connection. The second box allows to type the number of time (unit is minute) which is available for the user (using such profile) to access Internet. + - Click this box to set and increase the time quota for such profile. Click this box to decrease the time quota for such profile. Note: A dialog will be popped up to notify how many time remained when a user accesses into Internet through Vigor router successfully. Internet Access
Enable Data Quota	Data Quota means the total amount for data transmission allowed for the user. The unit is MB/GB. - Click this box to set and increase the data quota for such profile. - Click this box to decrease the data quota for such profile.
Reset quota to default when scheduling time	Set default time quota and data quota for such profile. When the scheduling time is up, the router will use the default



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

VII-3-3 User Group

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

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

32.

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

User Management >> User Group

<u>16.</u>



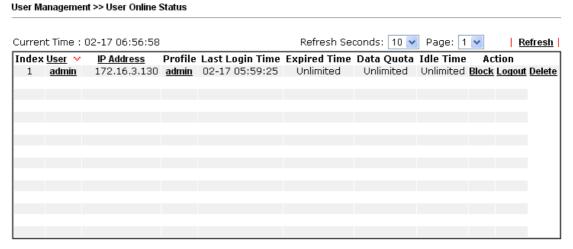
Item	Description
Name	Type a name for this user group.
Available User Objects	You can gather user profiles (objects) from User Profile page within one user group. All the available user objects that you have created will be shown in this box. Notice that user object, Admin and Dial-In User are factory settings. User defined profiles will be numbered with 3, 4, 5 and so on.

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

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

VII-3-4 User Online Status

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



Total Number: 1

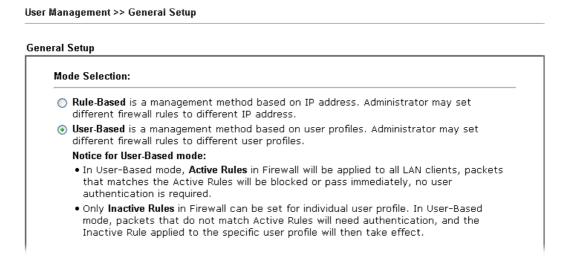
Item	Description
Refresh Seconds	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically.
	Refresh Seconds: 10 V 10 15 30
Refresh	Click this link to refresh this page manually.
Index	Display the number of the data flow.
User	Display the users which connect to Vigor router currently. You can click the link under the username to open the user profile setting page for that user.
IP Address	Display the IP address of the device.
Profile	Display the authority of the account.
Last Login Time	Display the login time that such user connects to the router last time.
Expired Time	Display the expired time of the network connection for the user.
Data Quota	Display the quota for data transmission.
Idle Time	Display the idle timeout setting for such profile.
	Display the fale timeout setting for such profile.

Action	Block - can avoid specified user accessing into Internet.
	Unblock - allow the user to access into Internet.
	Logout - the user will be logged out forcefully.

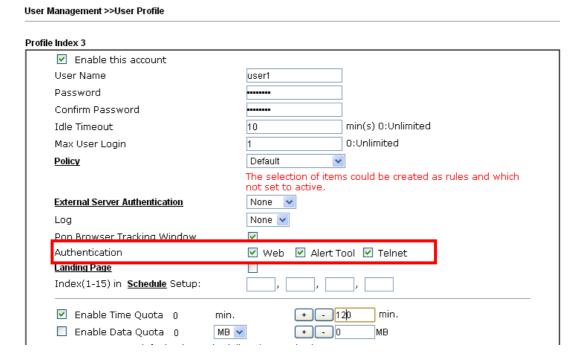
Application Notes

A-1 How to authenticate clients via User Management

Before using the function of User Management, please make sure **User-Based** has been selected as the **Mode** in the **User Management>>General Setup** page.



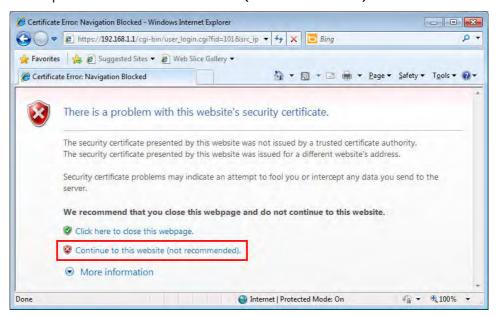
With User Management authentication function, before a valid username and password have been correctly supplied, a particular client will not be allowed to access Internet through the router. There are three ways for authentication: Web, Telnet and Alert Tool.



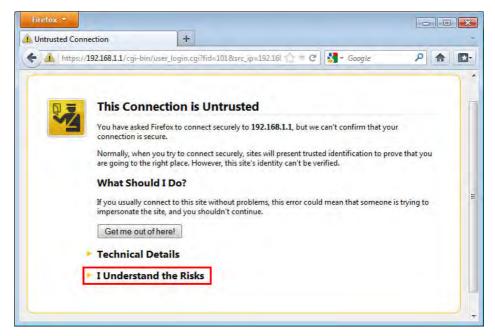
Authentication via Web

■ If a LAN client who hasn't passed the authentication opens an external web site in his browser, he will be redirected to the router's Web authentication interface first. Then, the client is trying to access http://www.draytek.com and but brought to the Vigor router. Since this is an SSL connection, some web browsers will display warning messages.

• With Microsoft Internet Explorer, you may get the following warning message. Please press Continue to this website (not recommended).



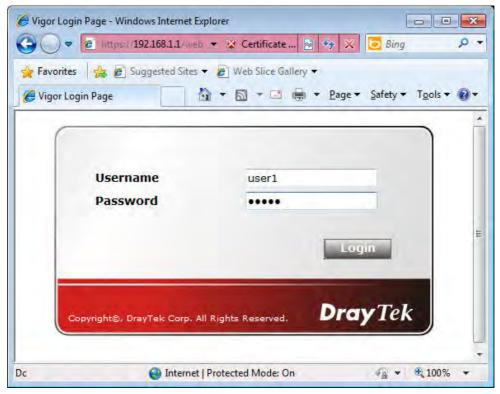
 With Mozilla Firefox, you may get the following warning message. Select I Understand the Risks.



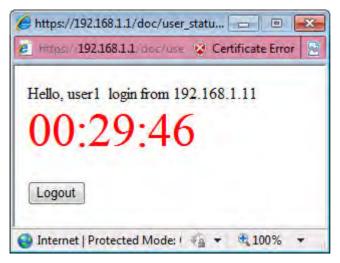
• With Chrome browser, you may get the following warning. Click **Proceed** anyway.



After that, the web authentication window will appear. Input the user name and the password for your account (defined in User Management) and click Login.



If the authentication is successful, the client will be redirected to the original web site that he tried to access. In this example, it is http://www.draytek.com . Furthermore, you will get a popped up window as the following. Then you can access the Internet.



Note, if you block the web browser to pop up any window, you will not see such window.

If the authentication is failed, you will get the error message, The username or password you entered is incorrect. Please login again.



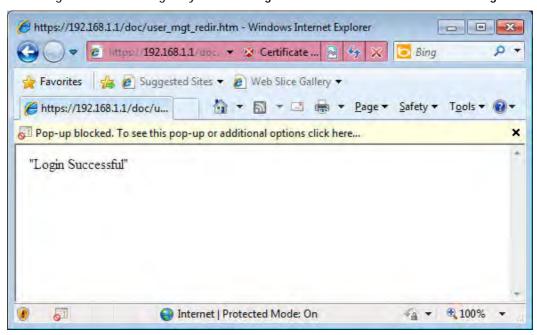
■ In above description, you access an external web site to trigger the authentication. You may also directly access the router's Web UI for authentication. Both HTTP and HTTPS are supported, for example http://192.168.1.1 or https://192.168.1.1 . Replace 192.168.1.1 with your router's real IP address, and add the port number if the default management port has been modified.

If the authentication is successful, you will get the Welcome Message that is set in the User Management >> General Setup page.

General Setup



With the default setup <body stats=1><script language='javascript'> window.location='http://www.draytek.com'</script></body>, you will be redirected to http://www.draytek.com . You may change it if you want. For example, you will get the following welcome message if you enter Login Successful in the Welcome Message table.



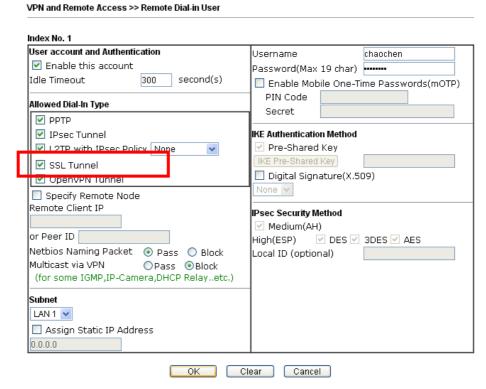
Also you will get a Tracking Window if you don't block the pop-up window.

■ Don't setup a user profile in **User Management** and a VPN Remote Dial-in user profile with the same Username. Otherwise, you may get unexpected result. It is because the

VPN Remote Dial-in User profiles can be extended to the User profiles in User Management for authentication.

There are two different behaviors when a User Management account and a VPN profile share the same Username:

• If SSL Tunnel or SSL Web Proxy is enabled in the VPN profile, the user profile in User Management will always be invalid for Web authentication. For example, if you create a user profile in User Management with chaochen/test as username/password, while a VPN Remote Dial-in user profile with the same username "chaochen" but a different password "1234", you will always get error message The username or password you entered is incorrect when you use chaochen/test via Web to do authentication.



• If SSL Tunnel or SSL Web Proxy is disabled in the VPN profile, a User Management account and a remote dial-in VPN profile can use the same Username, even with different passwords. However, we recommend you to use different usernames for different user profiles in User Management and VPN profiles.

Authentication via Telnet

The LAN clients can also authenticate their accounts via telnet.

1. Telnet to the router's LAN IP address and input the account name for the authentication:



2. Type the password for authentication and press Enter. The message User login successful will be displayed with the expired time (if configured).

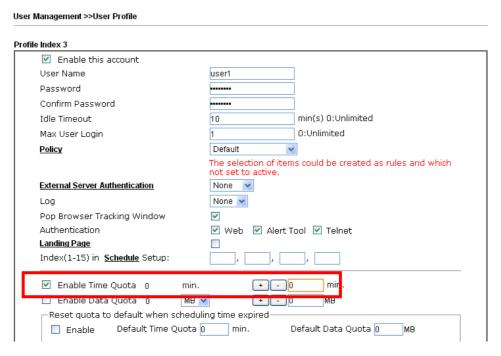




Info

Here expired time is "Unlimited" means the Time Quota function is not enabled for this account. After login, this account will not be expired until it is logout.

3. In the Web interface of router, the configuration page of Time Quota is shown as below.



4. If the Time Quota is set with "0" minute, you will get the following message which means this account has no time quota.



If the Time Quota is enabled and time is not 0 minute,

Enable this account		
User Name	user1	
Password	•••••	
Confirm Password	•••••	
Idle Timeout	10	min(s) 0:Unlimited
Max User Login	1	0:Unlimited
Policy	Default	
External Server Authentication	The selection of iter not set to active. None	ns could be created as rules and which
Log	None 🗸	
Pop Browser Tracking Window	<u> </u>	
Authentication	Web ✓ Alert ¹	Γool ☑ Telnet
<u>Landing Page</u>		
Index(1-15) in <u>Schedule</u> Setup:	, , ,	,
✓ Enable Time Quota 0 mi	n. +	12 0 min.

You will get the following message. The expired time is shown after you login.

```
Account:user1
Password: *****
User login successful, expired time is "12-23 10:21:33".
```

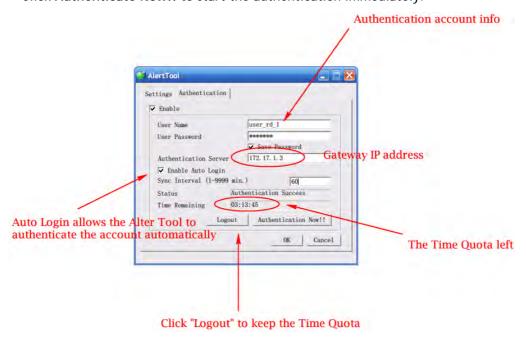
After you run out the available time, you can't use this account any more until the administrator manually adds additional time for you.

Authentication via VigorPro Alert Notice Tool

Authentication via Web or Telnet is convenient for users; however, it has some limitations. The most advantage with VigorPro Alert Notice Tool to operate the authentication is the ability to do auto login. If the timeout value set on the router for the user account has been reached, the router will stop the client computer from accessing the Internet until it does an authentication again. Authentication via VigorPro Alert Notice Tool allows user to setup the re-authentication interval so that the utility will send authentication requests periodically. This will keep the client hosts from having to manually authenticate again and again.

The configuration of the VigorPro Alert Notice Tool is as follows:

1. Click Authenticate Now!! to start the authentication immediately.



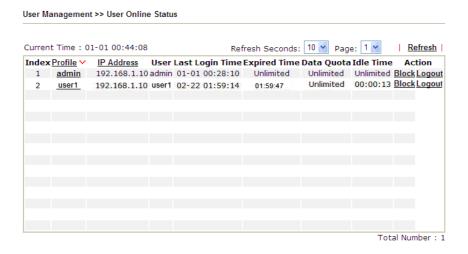
2. You may get the **VigorPro Alert Notice Tool** from the following link: http://www.draytek.com/user/SupportDLUtility.php



Info 1

Any modification to the Firewall policy will break down the connections of all current users. They all have to authenticate again for Internet access.

Info 2 The administrator may check the current users from User Online Status page.

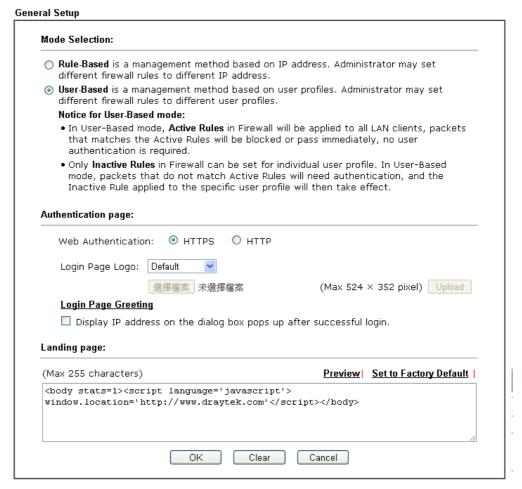


A-2 How to use Landing Page Feature

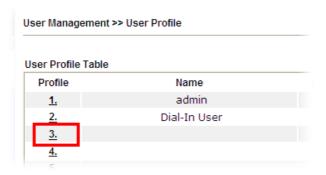
Landing Page is a special feature configured under User Management. It can specify the message, content to be seen or specify which website to be accessed into when users try to access into the Internet by passing the authentication. Here, we take Vigor2860 series router as an example.

Example 1: Users can see the message for landing page after logging into Internet successfully

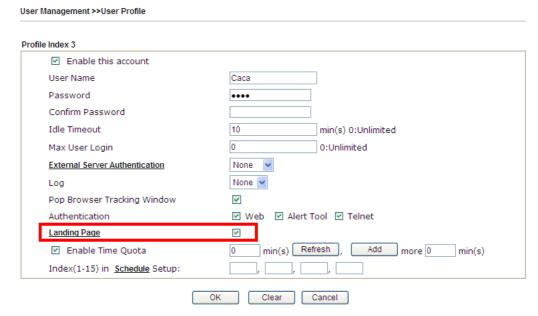
- 1. Open the web user interface of Vigor2860.
- Open User Management -> General Setup to get the following page. In the field of Landing Page, please type the words of "Login Success". Please note that the maximum number of characters to be typed here is 255.



3. Now you can enable the Landing Page function. Open User Management -> User Profile and click one of the index number (e.g., index number 3) links.



4. In the following page, check the box of Landing page and click OK to save the settings.



5. Open any browser (e.g., FireFox, Internet Explorer). The logging page will appear and asks for username and password. Please type the correct username and password.

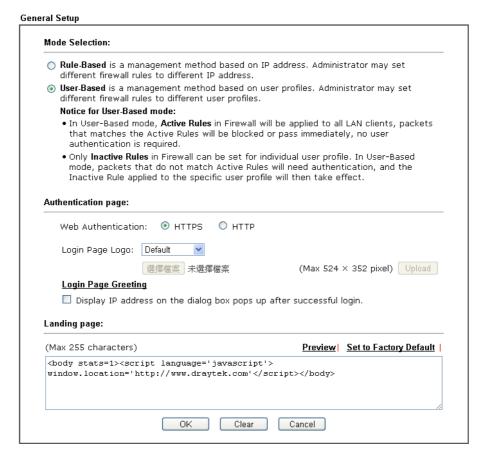


6. Click Login. If the logging is successful, you will see the message of Login Success from the browser you use.

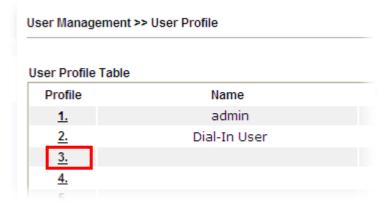


Example 2: The system will connect to http://www.draytek.com automatically after logging into Internet successfully

- 1. In the field of Landing Page, please type the words as below:
 - " <body stats=1><script language='javascript'>
 window.location='http://www.draytek.com'</script></body>"



2. Next, enable the Landing Page function. Open User Management -> User Profile and click one of the index number (e.g., index number 3) links.



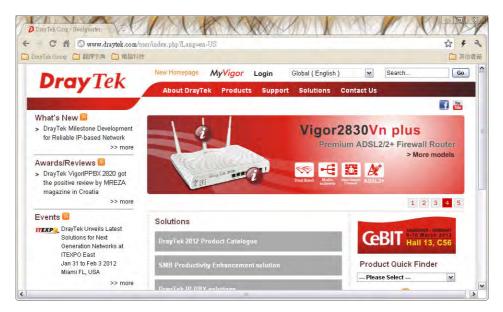
3. In the following page, check the box of Landing page and click OK to save the settings.

Profile Index 3	
✓ Enable this account	
User Name	Caca
Password	••••
Confirm Password	
Idle Timeout	10 min(s) 0:Unlimited
Max User Login	0 0:Unlimited
External Server Authentication	None 💌
Log	None 🔻
Pop Browser Tracking Window	
Authentication	✓ Web ✓ Alert Tool ✓ Telnet
Landing Page	
✓ Enable Time Quota	0 min(s) Refresh , Add more 0 min(s)
Index(1-15) in <u>Schedule</u> Setup:	,,
	OK Clear Cancel

4. Open any browser (e.g., FireFox, Internet Explorer). The logging page will appear and asks for username and password. Please type the correct username and password.



5. Click **Login**. If the logging is successful, you will be directed into the website of www.draytek.com.



VII-4 Central AP Management (CAM)

Vigor2860 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

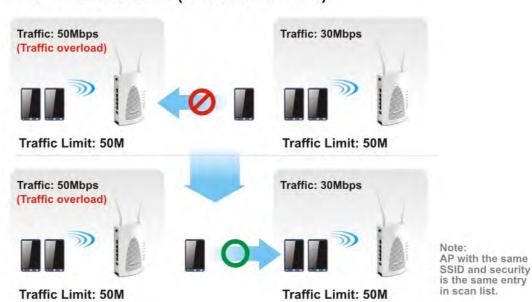
AP Maintenance

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.

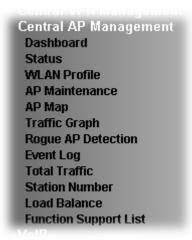
Load Balance for AP

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



VII-4-1 Dashboard

This page shows VigorAP's information about Status, Event Log, Total Traffic or Station Number by displaying VigorAP icon, text and histogram. Just move and click your mouse cursor on Status, Event Log, Total Traffic or Station Number. Corresponding web pages will be open immediately.



To access into the web user interface of VigorAP, simply move your mouse cursor on the VigorAP icon and click it. The system will guide you to access into the web user interface of VigorAP.

VII-4-2 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. Please open Central AP Management>>Function Support List to check what AP Models are supported.





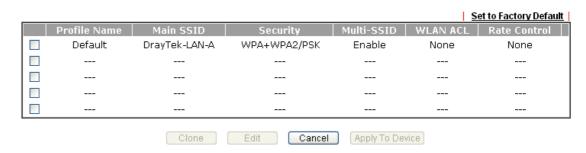
When AP Devices connect via an intermediary switch, please ensure that UDP:4944 port and the HTTP port of AP Devices are not blocked so that the AP status can be retrieved.

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 true IP address of the access point.
SSID	Display the SSID configured for the access point(s) connected to Vigor2860.
Encryption	Display the encryption mode used by the access point.
Ch.	Display the channel used by the access point.
WL Client	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.
Version	Display the firmware version used by the access point.
Password	Vigor2860 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-4-3 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 AP Management >> WLAN Profile

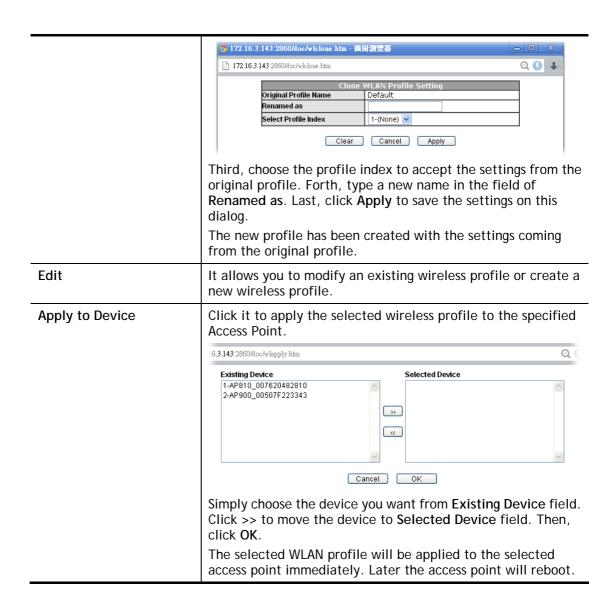


Check the box on the left side of the selected profile to modify the content of the profile. The Clone, Edit and Apply To Device buttons will be available then.

Central AP Management >> WLAN Profile

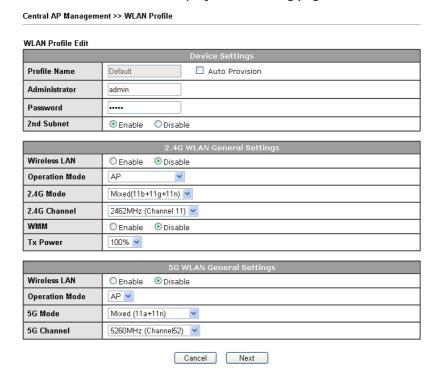


Item	Description
Profile	Display the name of the profile.
	The default profile cannot be renamed.
Main SSID	Display the SSID configured by such wireless profile.
Security	Display the security mode selected by such wireless profile.
Multi-SSID	Enable means multiple SSIDs (more than one) are active.
	Disable means only SSID1 is active.
WLAN ACL	Display the name of the access control list.
Rate Control	Display the upload and/or download transmission rate.
Clone	It can copy settings from an existing WLAN profile to another WLAN profile.
	First, you have to check the box of the existing profile as the original profile. Second, click Clone. The following dialog will appear.



How to edit the wireless LAN profile?

- 1. Check the box on the left side of the selected profile.
- 2. Click the Edit button to display the following page.

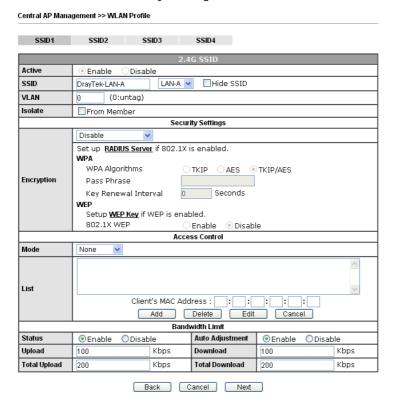




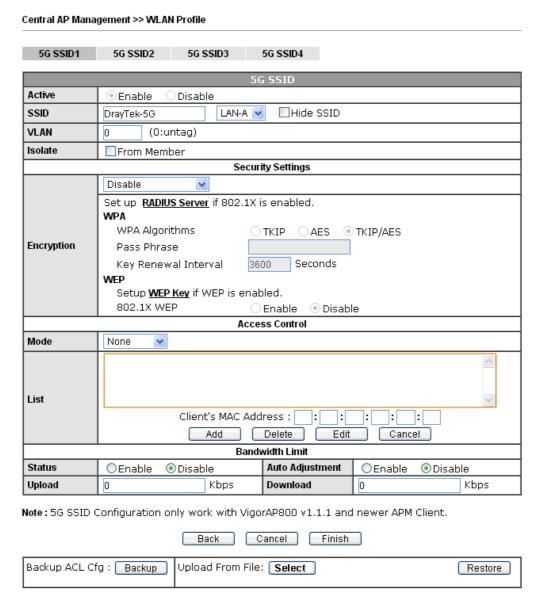
Info

The function of Auto Provision is available for the default WLAN profile.

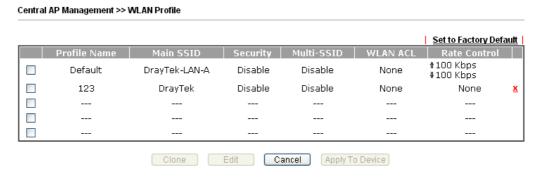
3. After finished the general settings configuration, click **Next** to open the following page for 2.4G wireless security settings.



4. After finished the above web page configuration, click **Next** to open the following page for 5G wireless security settings.



5. 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-4-4 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 Vigor2860.

Central AP Management >> AP Maintenance

Select Action Action Type: Config Backup File/Path: Select Select Device Existing Device Selected Device **Cancel OK**

Item	Description
Action	There are four actions provided by Vigor router to manage the access points. Config Backup Config Restore Firmware Upgrade Remote Reboot Factory Reset 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.
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

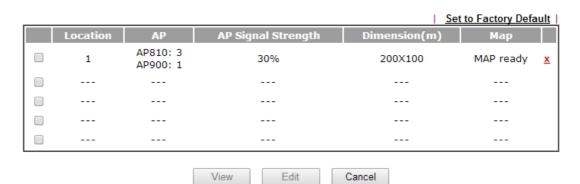
	Select Device and Selected Device areas.
Selected Device	Display the access points that will be applied by such function after clicking OK.

After finishing all the settings here, please click **OK** to perform the action.

VII-4-5 AP Map

This function 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.

Central AP Management >> AP Map



Item	Description
Set to Factory Default	Click the link to clear current page configuration.
	Check the box to view or edit the AP Map.
Location	Display a brief description (e.g., ground, roof) of the AP Map.
AP	Display the model name and number of VigorAP located on the AP map.
AP Signal Strength	Display the pre-defined signal strength of the AP map.
Dimension(m)	Display the width and length of the AP map.
Мар	Display if the uploaded file for AP map is ready or not.
View	Click it to review the layout for the selected AP map.
Edit	Click it to modify the geographic settings for the selected AP Map profile.
Cancel	Click it to cancel the configuration in such page.

Editing the AP Map Profile

7. Select an index \square and click **Edit** to open the following web page.

Central AP Management >> AP Map

AP Map Profile Edit

Geographic Settings

Location(Profile Name)

Dimensions

Length 80 m width 40 m

Upload Map

選擇檔案 2dhi6v7.png

Note: The size of the map should be 200KB or smaller.

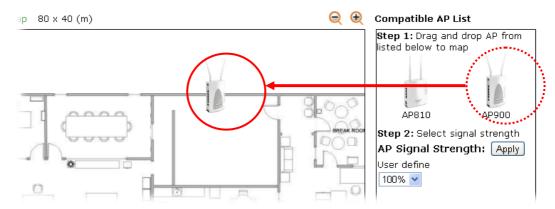
Available settings are explained as follows:

Item	Description
Location (Profile Name)	Type a name (e.g., groudfloor) for the AP map profile.
Dimensions	Type the real length and width of the uploaded map.
Upload Map	Click the Select button to choose an image file (only JPG and PNG are supported) for floor plan.
Cancel	Click it to cancel the configuration.
Next	Click it to go to the next configuration page.

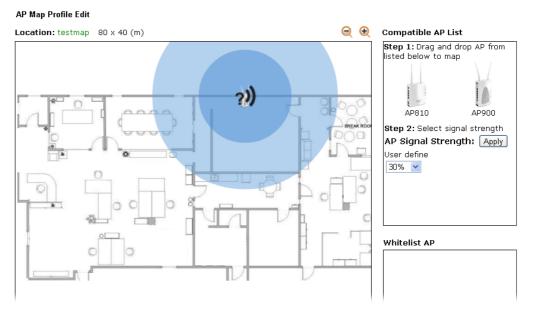
2. Click Next. The configuration page with floor plan will be shown as follows.



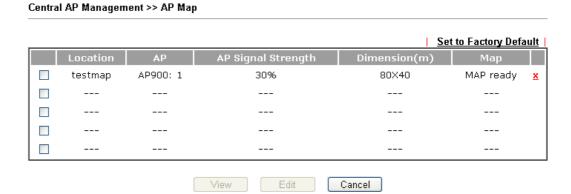
3. Drag and drop an AP icon from Compatible AP List to the map on the left side.



4. Choose the signal strength (e.g., 30% in this case) from User Define drop down list. Click Apply.



5. Adjust the AP on the map to find out which place can have the best wireless coverage. At last, click Save.



VII-4-6 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.





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).

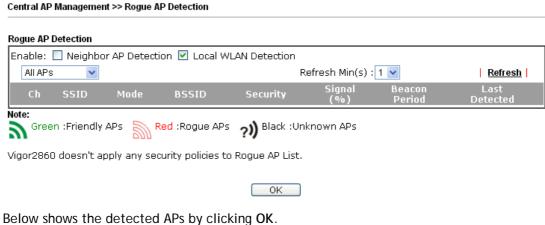


Info

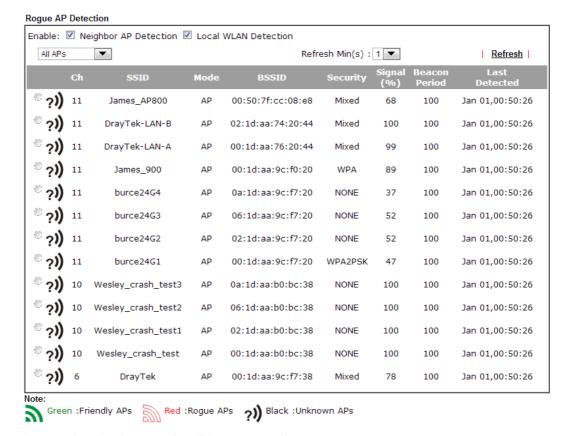
Enabling/Disabling such function will also enable/disable the External Devices function.

VII-4-7 Rogue AP Detection

It displays the access point scanned by Vigor router. In which, the APs will be classified with friendly APs, rogue APs and unknown APs in different colors.



Central AP Management >> Rogue AP Detection



Vigor2860 doesn't apply any security policies to Rogue AP List.

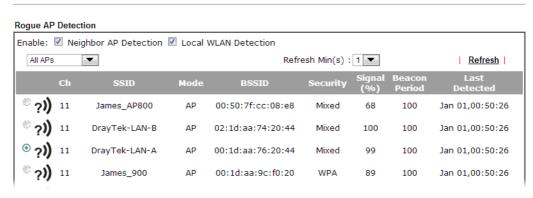
OK

Item	Description
Enable	Neighbor AP Detection - The access point(s) registered to Vigor2860 will be used to detect other access points and send the scanned results to Vigor2860. Later, the scanned result

	will be displayed on this page.
	Local WLAN Detection - The router will detect all the access points through wireless LAN connection.
All APs All APs Unknown APs Rogue APs Friendly APs	Specify the access points which are classified under each type.
Refresh Min(s)	Use the drop down list to specify the time to refresh the web page.
Refresh	Click such link to refresh the web page immediately.
Ch	Display the channel used by the detected access point.
SSID	Display the SSID specified for the detected access point.
Mode	Display the mode (AP or Ad Hoc) used by the detected access point.
BSSID	Display the MAC address of the detected access point.
Security	Display the encryption mode used by the access point.
Signal (%)	Display the signal strength (represented by percentage) sent by the access point.
Beacon Period	Display the period (time) of the beacon. The beacon signal will be sent out periodically.
Last Detected	Display the date and time that such access point was detected by Vigor router.

All the APs detected by Vigor router will be treated as unknown APs. You have to specify which AP is friendly and which one is Rogue respectively. Follow the steps below to perform the classification of access points.

 Click the radio button on one of the access points. In this case, DrayTek-LAN-A is selected.



2. Later, some options will appear on the bottom of the page.

Central AP Management >> Rogue AP Detection

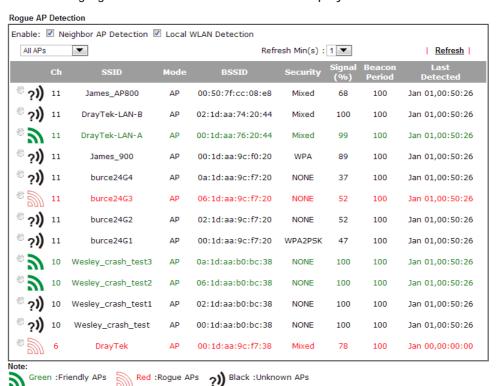


Available settings are explained as follows:

Item	Description
AP's MAC Address	The MAC address of the selected AP will be displayed here automatically.
AP's SSID	The SSID of the selected AP will be displayed here automatically.
Add to	Friendly APs - If the selected AP shall be treated as Friendly AP, simply click Add to change its classification from unknown to Friendly.
	Rogue APs - If the selected AP shall be treated as rogue AP, simply click Add to change its classification from unknown to Rogue.
Delete From	Rogue APs - If you want to change the classification of the rogue AP, simply choose the one and click Delete. Later, the page will refresh and the one will be classified as Unknown.
	Friendly APs - If you want to change the classification of the friendly AP, simply choose the one and click Delete. Later, the page will refresh and the one will be classified as Unknown.

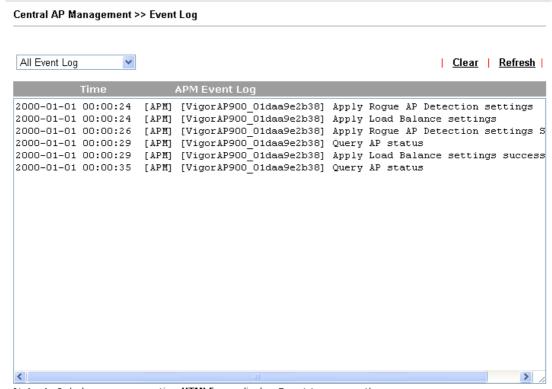
3. Click **OK** to save the settings.

The following figure shows the APs classified and displayed in different colors.



VII-4-8 Event Log

Time and event log for all of the APs managed by Vigor router will be shown on this page. It is userful for troubleshooting if required.

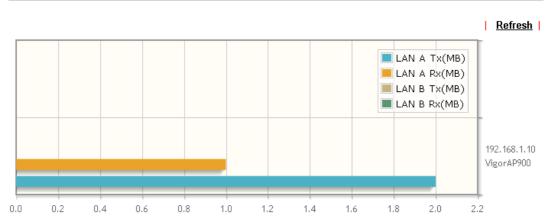


Note 1: Only browser supporting <u>HTML5</u> can display Event Log correctly. Note 2: The APs Log can be refreshed after at least 30 seconds.

VII-4-9 Total Traffic

Such page will display the total traffic of data receiving and data transmitting for VigorAPs managed by Vigor router.

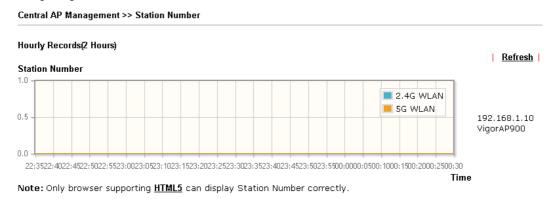




Note: Only browser supporting HTML5 can display Total Traffic correctly.

VII-4-10 Station Number

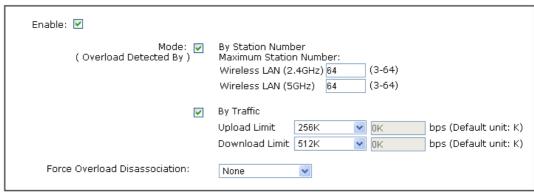
The total number of the wireless clients will be shown on this page, no matter what mode of wireless connection (2.4G WLAN) or 5G WLAN) used by wireless clients to access into Internet through VigorAP.



VII-4-11 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 AP Management >> Load Balance



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.



Item	Description
Enable	Check the box to enable such function.
Mode	It is used to determine the operation mode when the system detects overload between access points.
	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.

	By Traffic - The operation of load balance will executed according to the traffic configuration in this page. Upload Limit -Use the drop down list to specify the traffic limit for uploading.
	Download Limit - Use the drop down list to specify the traffic limit for downloading.
Force Overload Disassociation	By Idle 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.
	By signal Strength - 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.
	None None By Idle Time By signal Strength

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

VII-4-12 Function Support List

Click the Client tab to list the AP management functions that the Access Points support under different firmware versions.

Click the **Server** tab to list the AP management functions that Vigor router supports under different firmware versions.

Central AP Management >> Function Support List
Central AP Management >> Function Support List

Client S	erver									
		Model Name								
Function Name		AP800			AP810			AP900		
	1.0.5	1.1.0	1.1.1	1.1.0	1.1.1	1.1.5	1.1.0	1.1.1	1.1.6	1.1.4
Register										
DHCP	V	٧	٧	٧	٧	٧	٧	٧	٧	V
Static IP			٧	٧	٧	٧		٧	٧	V
Profile										
2.4GHz	V	٧	٧	٧	٧	٧	٧	٧	٧	٧
5GHz			٧				٧	٧	٧	V
AP Mode	V	٧	٧	٧	٧	٧	٧	٧	٧	V
Repeater Mode			٧	٧	٧	٧	٧	٧	٧	V
Client Disable Auto Provision			٧	V	٧	٧		٧	٧	V
WLAN Enable/Disable				٧	٧	٧		٧	٧	V
Station List										
Station List			٧	٧	٧	٧	٧	٧	٧	V
Load Balance		•					•			
Load Balance					٧	٧		٧	٧	V
Traffic Graph										
Traffic Granh			V	V	V	V	V	V	V	V

Application Notes

A-1 How to use AP Management function (in Vigor2860) to check AP status and deploy WLAN profile

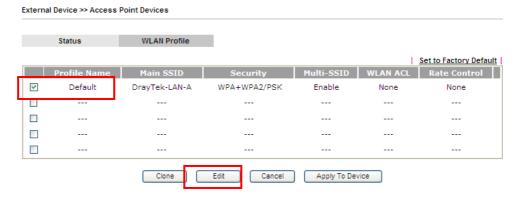
The administrator can manage the access points linked to Vigor2860.

1. Open External Devices>>Access Point Devices. Vigor2860 will detect the AP connecting to the router automatically and display as below:

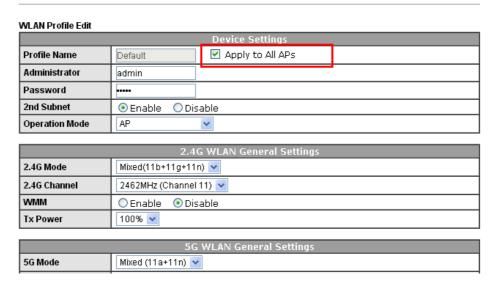


In this case, a device named with AP800_00507F6EE4980 has been detected by Vigor router.

2. Click the WLAN Profile tab to get the following page. Check the box of the default profile to make the Edit button be available. Then, click the Edit button.



3. When the following configuration page appears, make the changes you want and check Apply to All APs. Then, click Next to access into the next page.

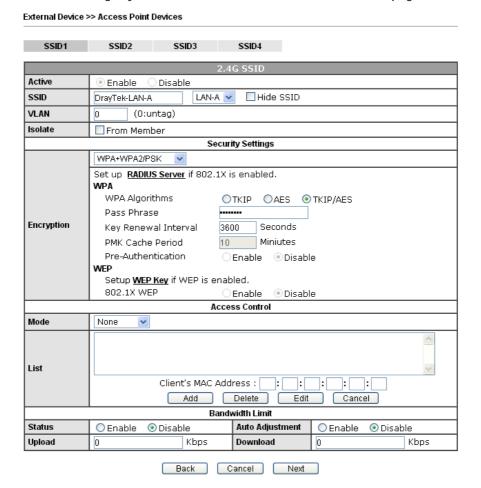




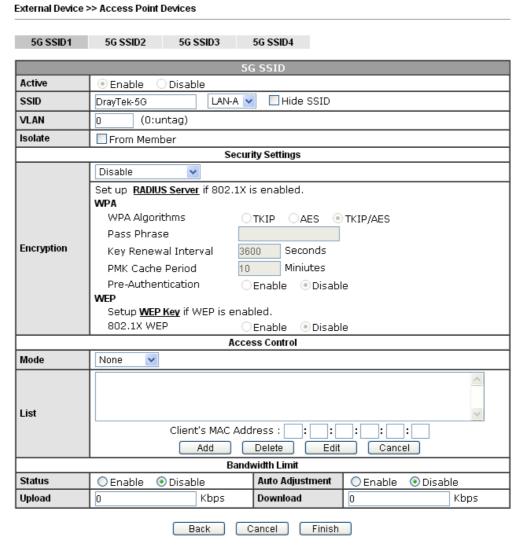
Info

Apply to All APs can automatically apply the settings on Default profile to all of the access points registered to Vigor2860 later. Hence, it is not necessary for you to manually apply wireless profiles for APs respectively. Such feature will be convenient for people who want to *quickly deploy* multiple Vigor APs in a large exhibition to reach the goal of "plug and play" and "zero-configuration".

4. The following page allows you to modify related settings for 2.4G SSID of managed AP. Make the changes you want for 2.4G SSID. Click **Next** for next page.



5. The following page is offered for you to modify related settings for 5G SSID of managed AP. Continue to make any changes you want. After finished all of the changes, simply click **Finish**.



6. Now, the AP (represented with *AP800_00507F6EE4980*) detected by Vigor router will be applied with the settings modified by Vigor router.

VII-5 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.

VII-5-1 All Devices

External Device >> All Devices External Device Auto Discovery External Devices Connected Below shows available devices that connected externally: On Line VigorAP900, VigorAP900, Connection Uptime:02:05:36 IP Address:192.168.1.11 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.

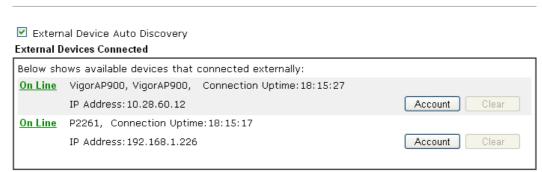


Available settings are explained as follows:

Item	Description
External Device Auto Discovery	Check this box to detect the external device automatically and display on this page.

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 >> All Devices



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.



When you finished the configuration, click **OK** to save it.



Info

Only DrayTek products can be detected by this function.

Part VIII Others





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

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

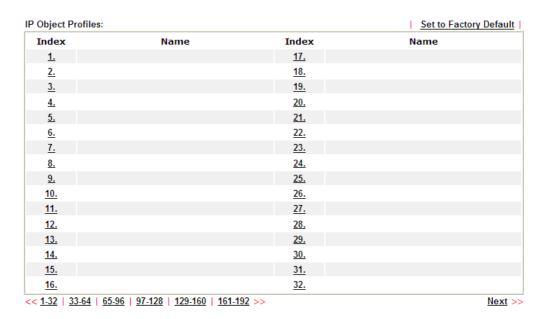
Web User Interface

Objects Setting
IP Object
IP Group
IPv6 Object
IPv6 Group
Service Type Object
Service Type Group
Keyword Object
Keyword Group
File Extension Object
SMS/Mail Service Object
Notification Object

VIII-1-1 IP Object

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

Objects Setting >> IP Object



Available settings are explained as follows:

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

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

- 1. Click the number (e.g., #1) under Index column for configuration in details.
- 2. The configuration page will be shown as follows:

Name:	RD Department
Interface:	Any
Address Type:	Range Address 🕶
Mac Address:	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:	

Item	Description				
Name	Type a name for this profile. Maximum 15 characters are allowed.				
Interface	Choose a proper interface. Any Any LAN/DMZ/RT/VPN WAN For example, the Direction setting in Edit Filter Rule will ask you specify IP or IP range for WAN or LAN/DMZ/RT/VPN or any IP address. If you choose LAN/DMZ/RT/VPN as the Interface here, and choose LAN/DMZ/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 Single Address Single Address Range Address Subnet Address Mac Address Mac Address				
MAC Address	Type the MAC address of the network card which will be controlled.				
Start IP Address	Type the start IP address for Single Address type.				
End IP Address	Type the end IP address if the Range Address type is				

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

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

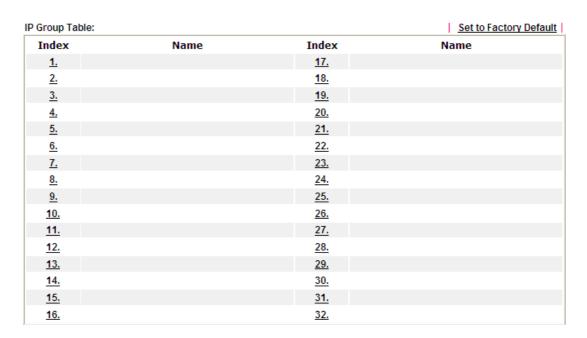
IP Object Profiles:

-		
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



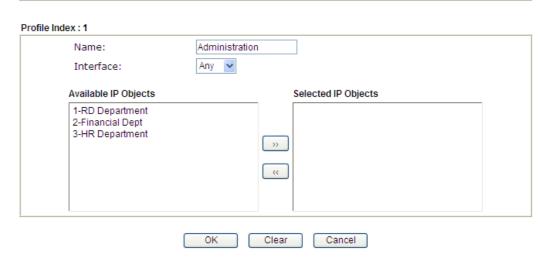
Available settings are explained as follows:

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



Available settings are explained as follows:

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

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

VIII-1-3 IPv6 Object

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

Objects Setting >> IPv6 Object

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

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

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

Available settings are explained as follows:

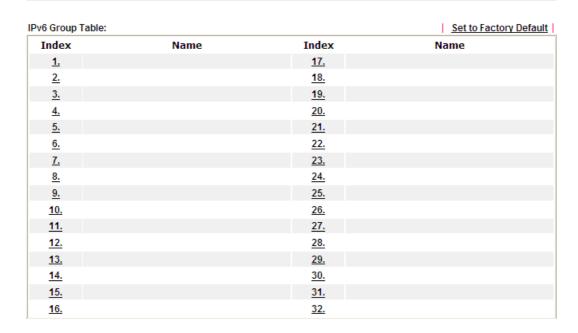
Item	Description	
Name	Type a name for this profile. Maximum 15 characters are allowed.	
Address Type	Determine the address type for the IPv6 address. Select Single Address if this object contains one IPv6 address only. Select Range Address if this object contains several IPv6s within a range. Select Subnet Address if this object contains one subnet for IPv6 address. Select Any Address if this object contains any IPv6 address. Select Mac Address if this object contains Mac address. Range Address Single Address Single Address Range Address Subnet Address Mac Address Mac Address	
Mac Address	Type the MAC address of the network card which will be controlled.	
Start IP Address	Type the start IP address for Single Address type.	
End IP Address	Type the end IP address if the Range Address type is selected.	
Prefix Length	Type 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



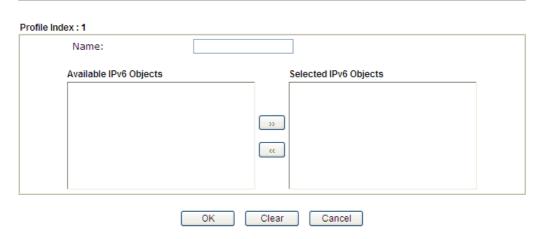
Available settings are explained as follows:

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



Available settings are explained as follows:

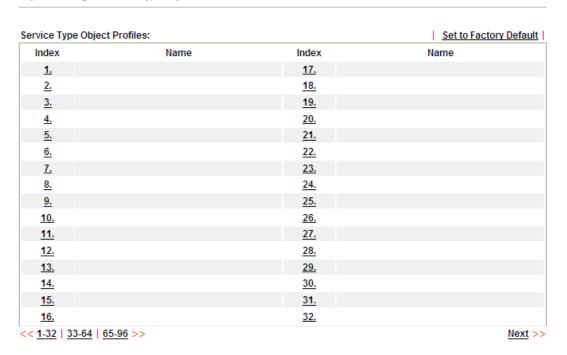
Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Available IPv6 Objects	All the available IPv6 objects with the specified interface chosen above will be shown in this box.
Selected IPv6 Objects	Click >> button to add the selected IPv6 objects in this box.

3. After finishing all the settings, 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



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 >> Service Type Object Setup

Profile Index : 1

Name
Protocol
TCP
Source Port
Destination Port

OK
Clear
Cancel

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. TCP Any ICMP IGMP TCP UDP TCP/UDP Other	
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 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	Inde
<u>1.</u>	www	<u>1</u> 7
<u>2.</u>	SIP	<u>1</u> 8
<u>3.</u>		1 9
4.		20

VIII-1-6 Service Type Group

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

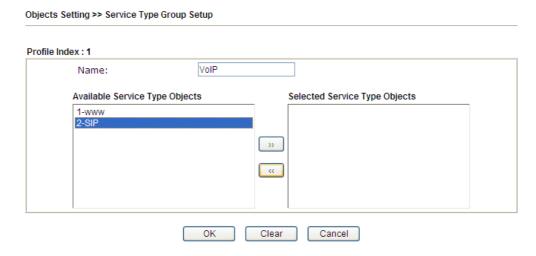
Objects Setting >> Service Type Group

ervice Type Group 1	able:		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>	

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:



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

eyword Object Prof	files:		Set to Factory Default
Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	
< <u>1-32</u> <u>33-64</u> <u>65</u>	5-96 <u>97-128</u> <u>129-160</u> <u>161-</u> 1	192 <u>193-200</u> >>	Next >

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:



Available settings are explained as follows:

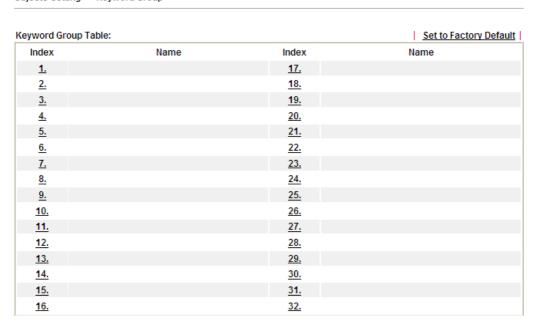
Item	Description
Name	Type a name for this profile, e.g., game. Maximum 15 characters are allowed.
Contents	Type the content for such profile. For example, type gambling as Contents. When you browse the webpage, the page with gambling information will be watched out and be passed/blocked based on the 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



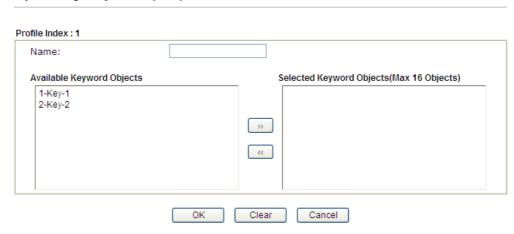
Available settings are explained as follows:

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



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.

3. 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 >>	ile Ex	tension	Object	
--------------------	--------	---------	--------	--

ile 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>	

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:



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
<u>1.</u>			kotsms.com.tw (TW)
<u>2.</u>			kotsms.com.tw (TW)
<u>3.</u>			kotsms.com.tw (TW)
<u>4.</u>			kotsms.com.tw (TW)
<u>5.</u>			kotsms.com.tw (TW)
<u>6.</u>			kotsms.com.tw (TW)
<u>7.</u>			kotsms.com.tw (TW)
<u>8.</u>			kotsms.com.tw (TW)
<u>9.</u>	Cust	com 1	
<u>10.</u>	Cust	tom 2	

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.
Index	Display the profile number that you can configure.
Profile	Display the name for such SMS profile.
SMS Provider	Display the service provider which offers SMS service.

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

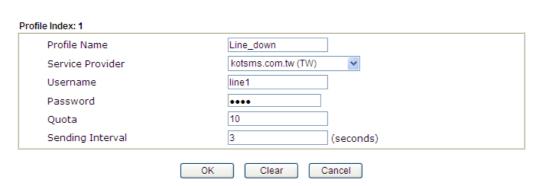
1. Click the SMS Provider tab, and click the number (e.g., #1) under Index column for configuration in details.

Object Settings >> SMS / Mail Service Object

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

2. The configuration page will be shown as follows:

Object Settings >> SMS / Mail Service Object



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	Type the number of the credit that you purchase from the service provider chosen above. Note that one credit equals to one SMS text message on the standard route.
Sending Interval	To avoid quota being exhausted soon, type time interval for sending the SMS.

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

Object Settings >> SMS / Mail Service Object



Customized SMS Service

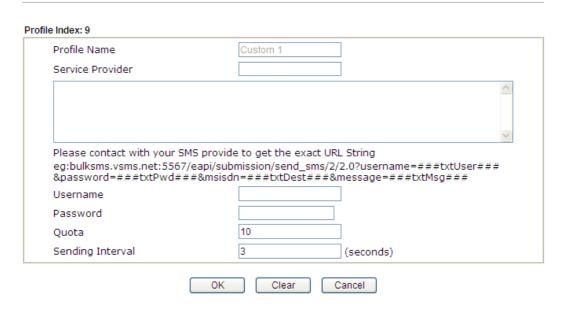
Vigor router offers several SMS service provider to offer the SMS service. However, if your service provider cannot be found from the service provider list, simply use Index 9 and Index 10 to make customized SMS service. The profile name for Index 9 and Index 10 are fixed.

Object Settings >> SMS / Mail Service Object

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

You can click the number (e.g., #9) under Index column for configuration in details.

Object Settings >> SMS / Mail Service Object



Item	Description	
Profile Name	Display the name of this profile. It cannot be modified.	
Service Provider	Type the website of the service provider. Type the URL string in the box under the filed of Service Provider. You have to contact your SMS provider to obtain the exact URL string.	
Username	Type a user name that the sender can use to register to selected SMS provider. 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	Type the total number of the messages that the router will send out.
Sending Interval	Type the shortest time interval for the system to send SMS.

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

Mail Service Object

This page allows you to set ten profiles which will be applied in Application>>SMS/Mail Alert Service.

Object Settings >> SMS / Mail Service Object

SMS Provider	Mail Server	Set to Fa	ctory 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.

Object Settings >> SMS / Mail Service Object

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

2. The configuration page will be shown as follows:

Object Settings >> SMS / Mail Service Object

Profile Index: 1	
Profile Name	Mail_Notify
SMTP Server	192.168.1.98
SMTP Port	25
Sender Address	carrie_ni@draytek.com
Use SSL	
Authentication	
Username	John
Password	••••
Sending Interval	0 (seconds)

Note: 1. Only one mail can be sent during the "Sending Interval" time.

OK	Clear	Cancel

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	Type the IP address of the mail server.
SMTP Port	Type the port number for SMTP server.
Sender Address	Type the e-mail address of the sender.
Use SSL	Check this box to use port 465 for SMTP server for some e-mail server uses https as the transmission method.
Authentication	The mail server must be authenticated with the correct username and password to have the right of sending message out. Check the box to enable the function.
	Username - Type a name for authentication. 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.

^{2.} If the "Sending Interval" was set to 0, there will be no limitation.

Sending Interval	Define the interval for the system to send the SMS out.

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

Object Settings >> SMS / Mail Service Object

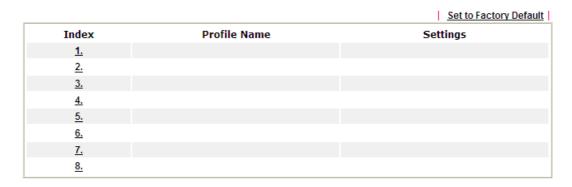


VIII-1-11 Notification Object

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.

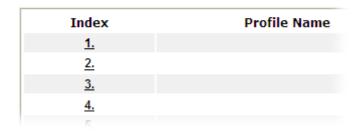
Object Settings >> Notification Object



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

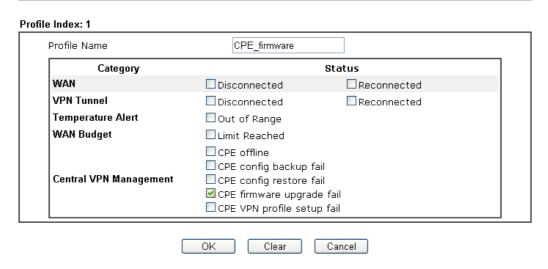
1. Open Object Setting>>Notification Object, and click the number (e.g., #1) under Index column for configuration in details.

Object Settings >> Notification Object



2. The configuration page will be shown as follows:

Object Settings >> Notification Object

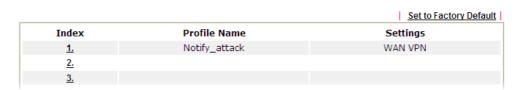


Available settings are explained as follows:

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 to be monitored.
	For example, the check box of CPE firmware upgrade fail under the category of Central VPN Management is checked. Once such profile is enabled, Vigor router system will send out notification to the recipient via SMS.

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

Object Settings >> Notification Object



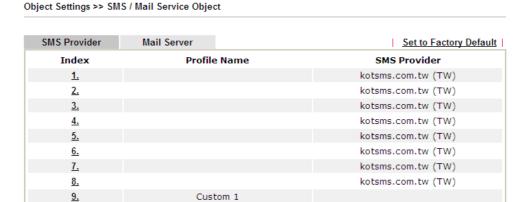
Application Notes

A-1 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection

Follow the steps listed below:

<u>10.</u>

- 1. Log into the web user interface of Vigor router.
- Configure relational objects first. Open Object Settings>>SMS/Mail Server Object to get the following page.



Custom 2

Index 1 to Index 8 allows you to choose the built-in SMS service provider. If the SMS service provider is not on the list, you can configure Index 9 and Index 10 to add the new service provider to Vigor router.

3. Choose any index number (e.g., Index 1 in this case) to configure the SMS Provider setting. In the following page, type the username and password and set the quota that the router can send the message out.



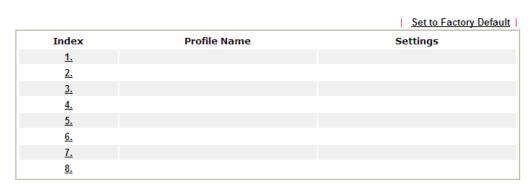
4. After finished the settings, click **OK** to return to previous page. Now you have finished the configuration of the SMS Provider profile setting.

Object Settings >> SMS / Mail Service Object



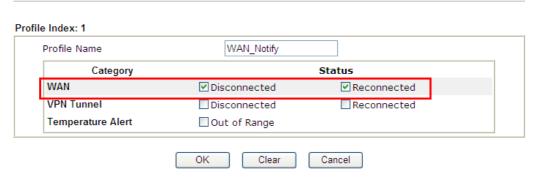
5. Open **Object Settings>>Notification Object** to configure the event conditions of the notification.

Object Settings >> Notification Object



6. Choose any index number (e.g., Index 1 in this case) to configure conditions for sending the SMS. In the following page, type the name of the profile and check the Disconnected and Reconnected boxes for WAN to work in concert with the topic of this paper.

Object Settings >> Notification Object



7. After finished the settings, click **OK** to return to previous page. You have finished the configuration of the notification object profile setting.

Object Settings >> Notification Object



8. Now, open Application >> SMS / Mail Alert Service. Use the drop down list to choose SMS Provider and the Notify Profile (specify the time of sending SMS). Then, type the phone number in the field of Recipient (the one who will receive the SMS).

Application >> SMS / Mail Alert Service



9. 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, type the URL string of the SMS provider and type 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.



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 type the IP address of the Vigor router and username/password created in USB Application>>USB User Management on the client software. Then, the client can use the FTP site (USB storage disk) or share the 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

USB Application
USB General Settings
USB User Management
File Explorer
USB Device Status
Temperature Sensor
Modem Support List
SMB Client Support List

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	5 (Maximum 6)
Default Charset	English ▼
SMB File Sharing Service (Network Neighb	oorhood)
◯ Enable ◯ Disable	
Access Mode	
LAN Only LAN And WAN	
NetBios Name Service	
Workgroup Name	WORKGROUP
Host Name	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 multiconnection mechanism, such as FileZilla, you should limit client connections to 1 to improve performance.
- 3. A workgroup name must be different from the host name. The workgroup name can have up to 15 characters and the host name can have up to 15 characters. Names cannot contain any of the following: . ; : * < > * + = / \ | ?.

OK

Item	Description
General Settings	Simultaneous FTP Connections - This field is used to specify the quantity of the FTP sessions. The router allows up to 6 FTP sessions connecting to USB storage disk at one time. Default Charset - At present, Vigor router supports four types of character sets. Default Charset is for English based file name.
	types of character sets. Default Charset is for English base file name.

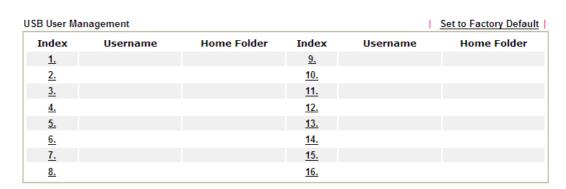
	English Chinese(Simple) Chinese(Traditional) German	
SMB File Sharing Service	Click Enable to invoke SMB service (file sharing) via the router.	
Access Mode	LAN Only - Users coming from internet cannot connect to the SMB server of the router. LAN And WAN - Both LAN and WAN users can access SMB server of the router.	
NetBios Name Service	For the NetBios service of USB storage disk, you have to specify a workgroup name and a host name. A workgroup name must not be the same as the host name. The workgroup name can have as many as 15 characters and the host name can have as many as 23 characters. Both them cannot contain any of the following; : " < > * + = \ ?. Workgroup Name - Type a name for the workgroup. Host Name - Type the host name for the router.	

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

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 type the same username and password configured in this page. Before adding or modifying settings in this page, please insert a USB storage disk first. Otherwise, an error message will appear to warn you.

USB Application >> USB User Management

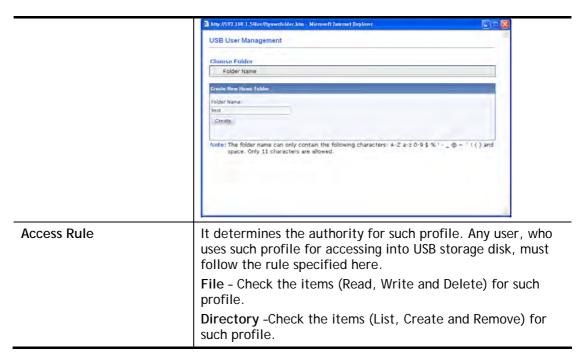


Click index number to access into configuration page.

Profile Index: 1 FTP/SMB User Username Password Confirm Password Home Folder File Directory Enable Disable (Maximum 11 Characters) (Maximum 11 Characters) Enable Disable
Note: The folder name can only contain the following characters: A-Z a-z 0-9 \$ % ' - _ @ ~ `!() and space.



Item	Description
FTP/SMB User	Enable - Click this button to activate this profile (account) for FTP service or SMB User service. Later, the user can use the username specified in this page to login into FTP server. Disable - Click this button to disable such profile.
Username	Type the username for FTP/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 type 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	Type the password for FTP/SMB users for accessing FTP server. Later, you can open FTP client software and type the password specified here for accessing into USB storage disk. The length of the password is limited to 11 characters.
Confirm Password	Type the password again to make confirmation.
Home Folder	It determines the folder for the client to access into. The user can enter a directory name in this field. Then, after clicking OK , the router will create the specific/new folder in the USB storage disk. In addition, if the user types "/" here, he/she can access into all of the disk folders and files in USB 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.



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.



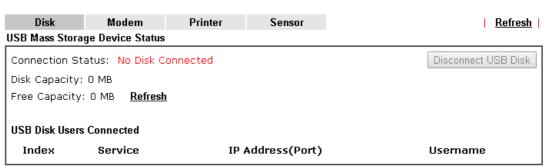
Item	Description
Refresh	Click this icon to refresh files list.
† Back	Click this icon to return to the upper directory.
Create	Click this icon to add a new folder.
Current Path	Display current folder.

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



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

Available settings are explained as follows:

Item	Description
Connection Status	If there is no USB 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		Refresh
USB Mass Stora	age Device Status	i		
Connection S	tatus: Disk Cor	nected		Disconnect USB Disk
Write Protect Status: No				
Disk Capacity	Disk Capacity: 2009 MB			
Free Capacity: 925 MB Refresh				
l				
USB Disk User:	s Connected			
Index	Service	IP	Address(Port)	Username

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

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	0.00	
Temperature Unit Alarm Settings Enable Syslog Alarm	⊙ Celsius	
Upper temperature limit	30.00	
Lower temperature limit	18.00	
	OK	

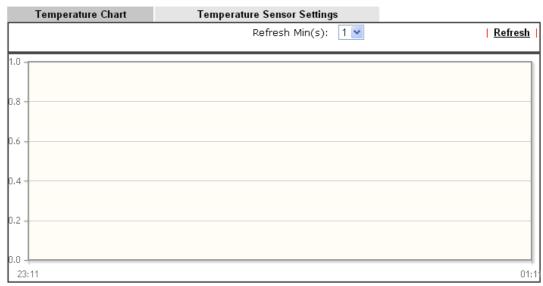
Available settings are explained as follows:

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 - Type 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.

PPP mode	DHCP mode		
Brand	Model	LTE	Status
Aiko	Aiko 83D		Υ
Alcatel	Alcatel L100V	Ø	Υ
Alcatel	Alcatel W100	Ø	Υ
BandRich	Bandluxe C170		Υ
BandRich	Bandluxe C270		Υ
BandRich	Bandluxe C321		Υ
BandRich	Bandluxe C330		Υ
BandRich	Bandluxe C331		Υ
BandRich	Bandluxe C502		Υ
Huawei	Huawei E169u		Υ
Huawei	Huawei E220		Υ
Huawei	Huawei E303D		Υ
Huawei	Huawei E3131		Υ
Huawei	Huawei E392	Ø	Υ
Unawai	Unawai E200	(m)	V

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 TM	Built in	Υ
Microsoft® Windows® 7	Built in	Υ
Microsoft® Windows® 8	Built in	М
OS X® 10.7.5	Built in	Υ
OS X® 10.10	Built in	Υ
Android TM	AndSMB	Υ
Android TM	ES File Explorer	Υ
Android TM	File Expert	Y
Android TM	File Manager	Y
Android TM	Solid Explorer	Υ
Android TM	SharesFinder	Y
ios	eXPlayer	Υ
ios	nPlayer	Υ

Y: Tested and is supported.

I: Supported but has some issue.

M: Has not been tested but might be supported.

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 Applicaiton>>File Explorer. If it is necessary for you to delete, copy files on the device or write, paste files to the devcie, it must be done through SMB server or FTP server.

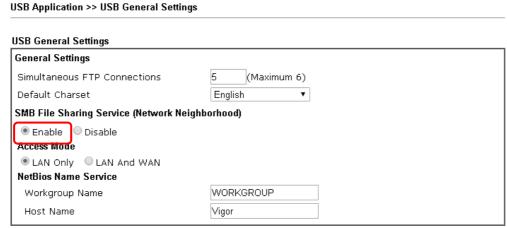
SMB service is based on the original USB FTP service. You will need to setup USB FTP first. We would like to give brief instructions on USB FTP setup here.

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



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.



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: . ; : " < > * + = $/ \setminus$ | ?.

OK

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

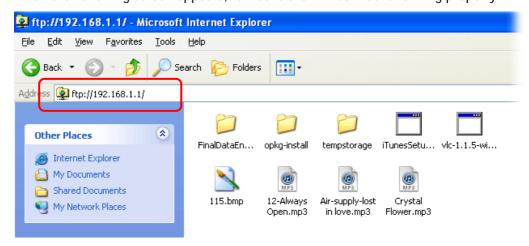
USB Application >> USB User Management



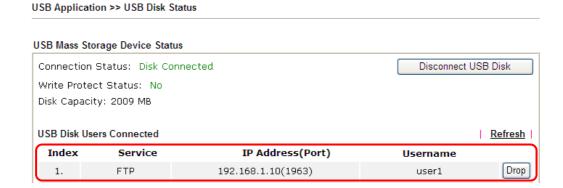
- 4. Click **OK** to save the configuration.
- 5. Make sure the FTP service is running properly. Please open a browser and type *ftp://192.168.1.1.* Use the account "user1" to login.



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.



Now, users in LAN of Vigor2860 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



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-1Diagnostics

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.

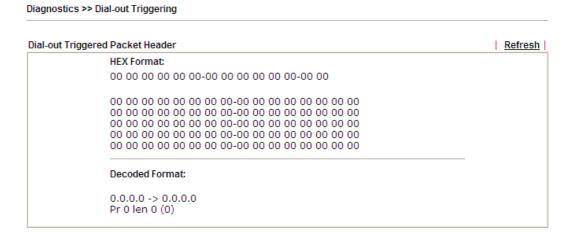
Web User Interface

Fisrt, 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.

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 Authentication Information DoS Flood Table**

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.

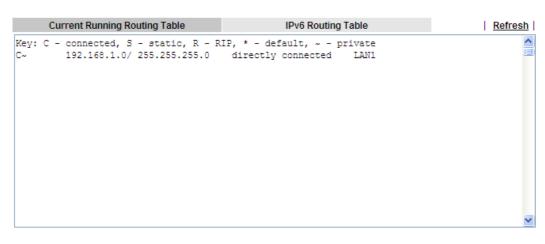


Item	Description
Decoded Format	It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.
Refresh	Click it to reload the page.

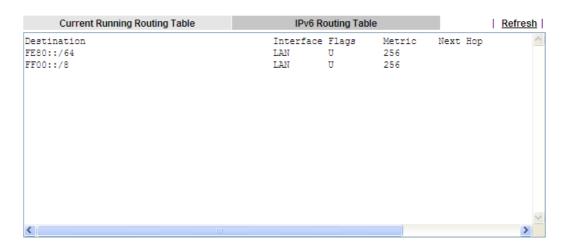
IX-1-2 Routing Table

Click Diagnostics and click Routing Table to open the web page.

Diagnostics >> View Routing Table



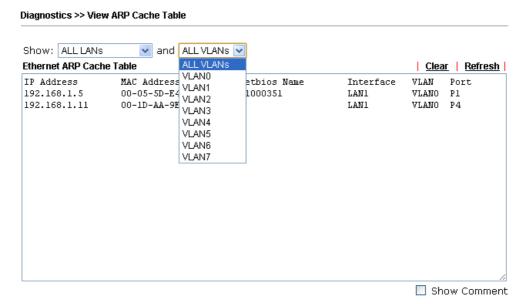
Diagnostics >> View Routing Table



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.



Item	Description
Show	Specify LAN and VLAN to display related information. In default, this page will display all of the information about LAN and VLAN.
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 33-33-00-00-00-02 FF02::2 LAN FF02::1:3 33-33-00-01-00-03 LAN e8-9d-87-87-69-2f FE80::3D5E:E74:8751:A44B 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 33-33-00-00-00-01 LAN FF02::1 FF02::1 00-00-00-00-00 USB2 FF02::1:2 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:

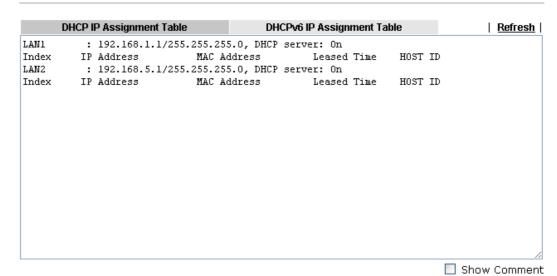
Item	Description
Refresh	Click it to reload the page.

IX-1-5 DHCP Table

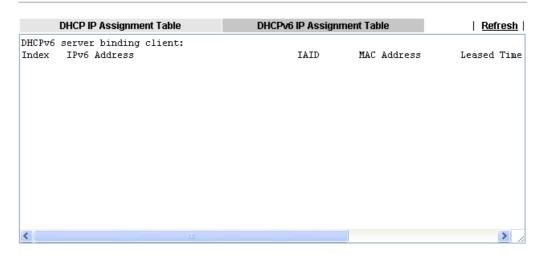
The facility provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

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

Diagnostics >> View DHCP Assigned IP Addresses



Diagnostics >> View DHCP Assigned IP Addresses



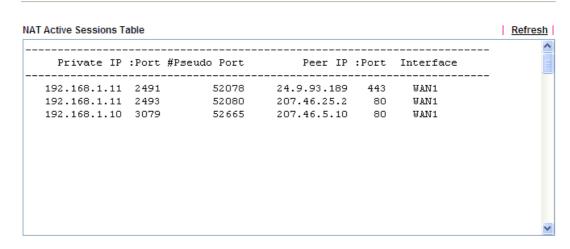
Available settings are explained as follows:

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



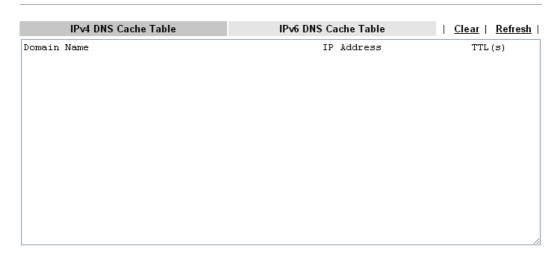
Item	Description
Private IP:Port	It indicates the source IP address and port of local PC.
#Pseudo Port	It indicates the temporary port of the router used for NAT.
Peer IP:Port	It indicates the destination IP address and port of remote host.
Interface	It displays the representing number for different 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



 $\ensuremath{\textbf{Note:}}$ The LAN DNS entry's TTL is static.

When an entry's TTL is larger than 0 s, this entry will be deleted from the table.

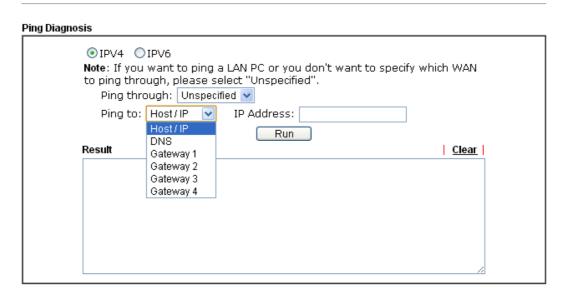
0K

Item	Description
Clear	Click this link to remove the result on the window.
Refresh	Click it to reload the page.
When an entry's TTL is larger than	Check the box the type the value of TTL (time to live) for each entry. Click OK to enable such function.
	It means when the TTL value of each DNS query reaches the threshold of the value specified here, the corresponding record will be deleted from router's Cache automatically.

IX-1-8 Ping Diagnosis

Click Diagnostics and click Ping Diagnosis to open the web page.

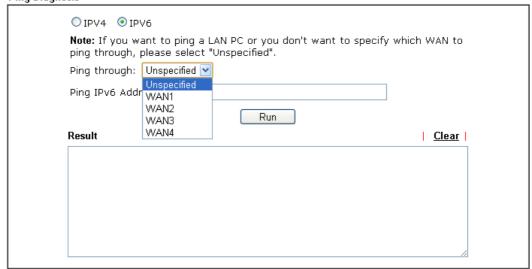
Diagnostics >> Ping Diagnosis



or

Diagnostics >> Ping Diagnosis

Ping Diagnosis

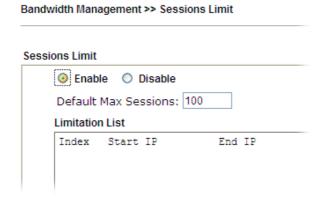


Item	Description
IPV4 /IPV6	Choose the interface for such function.
Ping through	Use the drop down list to choose the WAN/LTE interface that you want to ping through or choose Unspecified to be determined by the router automatically.
Ping to	Use the drop down list to choose the destination that you want to ping.

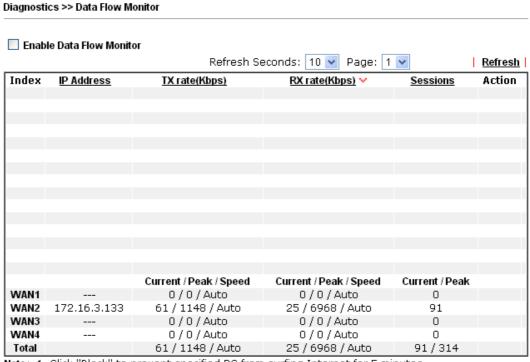
IP Address	Type the IP address of the Host/IP that you want to ping.
Ping IPv6 Address	Type the IPv6 address that you want to ping.
Run	Click this button to start the ping work. The result will be displayed on the screen.
Clear	Click this link to remove the result on the window.

IX-1-9 Data Flow Monitor

This page displays the running procedure for the IP address monitored and refreshes the data in an interval of several seconds. The IP address listed here is configured in Bandwidth Management. You have to enable IP bandwidth limit and IP session limit before invoking Data Flow Monitor. If not, a notification dialog box will appear to remind you enabling it.



Click **Diagnostics** and click **Data Flow Monitor** to open the web page. You can click **IP Address**, **TX rate**, **RX rate** or **Session** link for arranging the data display.



Note: 1. Click "Block" to prevent specified PC from surfing Internet for 5 minutes.

^{2.} The IP blocked by the router will be shown in red, and the session column will display the remaining time that the specified IP will be blocked.

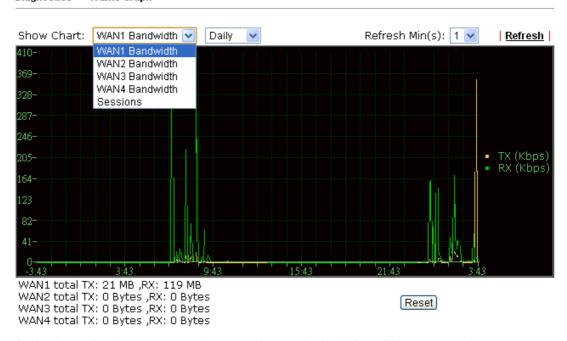
 ⁽Kbps): shared bandwidth
 residual bandwidth used
 Current/Peak are average.

Item	Description
Enable Data Flow Monitor	Check this box to enable this function.
Refresh Seconds	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically. Refresh Seconds: 10 V
	10 15 30
Refresh	Click this link to refresh this page manually.
Index	Display the number of the data flow.
IP Address	Display the IP address of the monitored device.
TX rate (kbps)	Display the transmission speed of the monitored device.
RX rate (kbps)	Display the receiving speed of the monitored device.
Sessions	Display the session number that you specified in Limit Session web page.
Action	Block - can prevent specified PC accessing into Internet within 5 minutes. Page: 1
Current /Peak/Speed	Current means current transmission rate and receiving rate for WAN interface. Peak means the highest peak value detected by the router in data transmission. Speed means line speed specified in WAN>>General Setup. If you do not specify any rate at that page, here will display Auto for instead.

IX-1-10 Traffic Graph

Click Diagnostics and click Traffic Graph to open the web page. Choose WAN1/WAN2/WAN3/WAN4 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

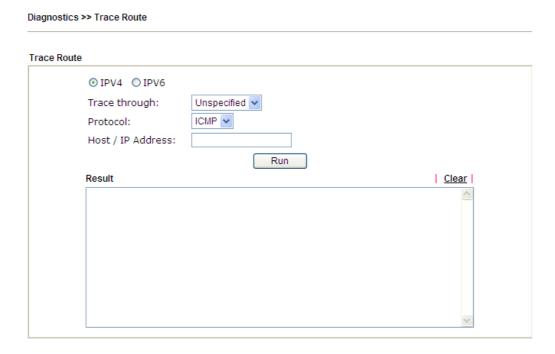


The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1/WAN2/WAN3/LTE/WAN4 Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

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 type the IP address of the host in the box and click **Run**. The result of route trace will be shown on the screen.



or

Diagnostics >> Trace Route



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



Item	Description	
Enable Web Syslog	Check this box to enable the function of Web Syslog.	
Syslog Type	Use the drop down list to specify a type of Syslog to be displayed. User Firewall Call WAN VPN All	
Export	Click this link to save the data as a file.	
Refresh	Click this link to refresh this page manually.	
Clear	Click this link to clear information on this page.	
Display Mode	There are two modes for you to choose. Stop record when fulls Stop record when fulls Always record the new event Stop record when fulls - when the capacity of syslog is full,	

	the system will stop recording.	
	Always record the new event - only the newest events will be recorded by the system.	
Time	Display the time of the event occurred.	
Message	Display the information for each event.	

For USB Syslog

This page displays the syslog recorded on the USB storage disk.

Diagnostics >> Syslog Explorer

Web Syslog	USB Syslog
g	,

Note:The syslog will sh	ow while the saved s	yslog file size is over 1	MB.	
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.

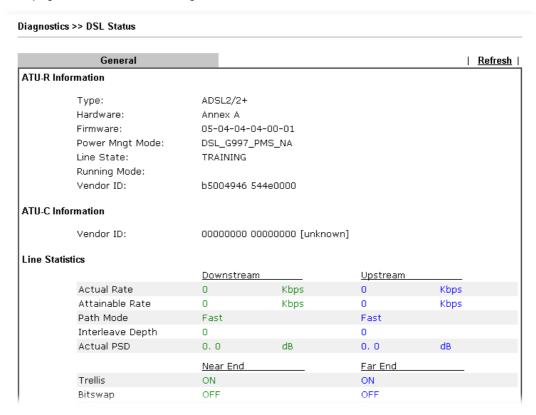
Diagnostics >> IPv6 TSPC Status

WAN1	WAN2	WAN3	WAN4	Refresh
TSPC Enabled				
TSPC Connection Sta	tus			
Local Endpoint v4 A	ddress :	114.44.54.220		
Local Endpoint v6 A	ddress :	2001:05c0:1400:000b:0000:0000:0000:10b9		10b9
Router DNS name : 88		88886666.broker.freenet6.net		
Remote Endpoint v4 Address: 81.171.72.11				
Remote Endpoint v6	Address:	2001:05c0:1400:00	ob:0000:0000:0000:	10b8
Tspc Prefix :		2001:05c0:1502:0d00:0000:0000:0000:0000		
Tspc Prefixlen :		56		
Tunnel Broker :		amsterdam.freenet6	i.net	
Tunnel Status :		Connected		

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.



IX-1-15 Authentication Information

Authentication User List

Such page displays authentication jobs made by Internal RADIUS or Local 802.1X.

When the mouse cursor moves to the name link under User Name, the connection message (including authentication failed information) about internal RADIUS or local 802.1X service will be shown by a popped up dialog box.

Diagnostics >> Authentication Information

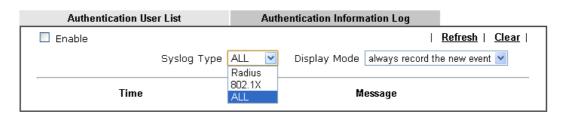
Authentication User List		Authentication Inform	nation Log
			<u>Refresh</u> <u>Clear</u>
User Name	Authentication Failure Tin	es User Name	Authentication Failure Times
test_1	<u>0</u>	test_sales	<u>0</u>

- 1. This is the authentication list for router's <u>Internal RADIUS</u> or Local 802.1X 2. For those clients are authenticated by external RADIUS server, please find the information from the server.

Authentication Information Log

This page will display the complete authentication log information.

Diagnostics >> Authentication Information



Item	Description	
Enable	Check the box to enable such function.	
Refresh	Click it to update current page.	
Clear	Click it to remove all of the records.	
Syslog Type	Specify RADIUS, 802.1X or All to display related authentication information log.	
Display Mode	Choose the mode you want to display the related information on the following table.	
	• Stop record when fulls - when the capacity of CVM log is full, the system will stop recording.	
	 Always record the new event - only the newest events will be recorded by the system. 	
Time	Display the time the user authenticated by Vigor2860 series.	
Message	Display authentication information done by Vigor2860 series.	

IX-1-16 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.

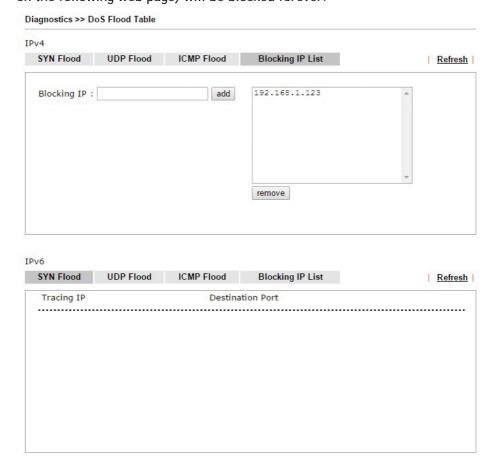


U

Info

The icon - (3) - means there is something wrong (e.g., attacking the system) with that IP address.

However, if an IP address is comfirmed to be blocked due to its abnormal behavior, click the **Blocking IP List** tab to block it forever. For example, IP address "192.168.1.123" (displayed on the following web page) will be blocked forever.



Available settings are explained as follows:

Item	Description
Blocking IP	Type the IP address in this field and click add. It will be added to the IP List and appear in the right frame.
	IP list in the right frame will be blocked by Vigor system permanatly.
	Remove - It is used to remove selected IP address from the Blocking IP List.
Refresh	Click this link to refresh current page.

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 stilled 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.

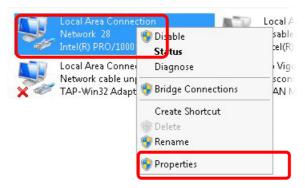
 Open All Programs>>Getting Started>>Control Panel. Click Network and Sharing Center.



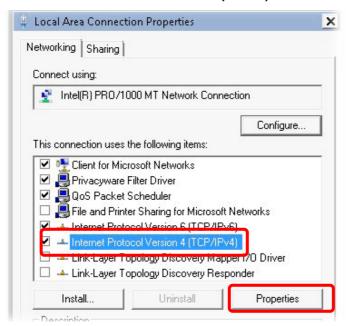
2. In the following window, click Change adapter settings.



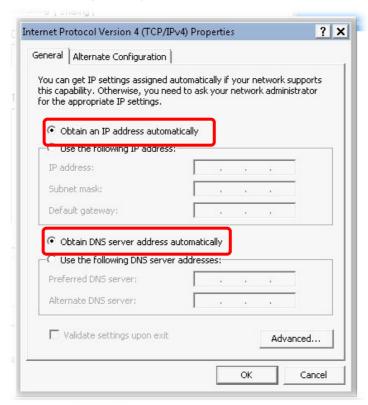
3. Icons of network connection will be shown on the window. Right-click on Local Area Connection and click on Properties.



4. Select Internet Protocol Version 4 (TCP/IP) and then click Properties.

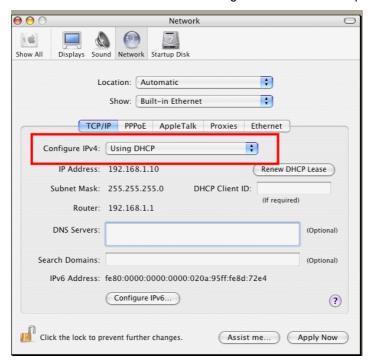


5. Select Obtain an IP address automatically and Obtain DNS server address automatically. Finally, click OK.



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.



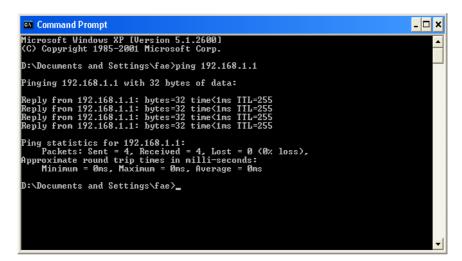
IX-4 Pinging the Router from Your Computer

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 previous section IX-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). The DOS command dialog will appear.



- 3. Type ping 192.168.1.1 and press [Enter]. If the link is OK, the line of "Reply from 192.168.1.1:bytes=32 time<1ms TTL=255" will appear.
- 4. If the line does not appear, please check the IP address setting of your computer.

For Mac OS (Terminal)

- 1. Double click on the current used 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=xxxx ms" will appear.

```
Terminal — bash — 80x24

Last login: Sat Jan 3 02:24:18 on ttyp1

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 tt!=255 time=0.755 ms

64 bytes from 192.168.1.1: icmp_seq=1 tt!=255 time=0.697 ms

64 bytes from 192.168.1.1: icmp_seq=2 tt!=255 time=0.716 ms

64 bytes from 192.168.1.1: icmp_seq=3 tt!=255 time=0.731 ms

64 bytes from 192.168.1.1: icmp_seq=4 tt!=255 time=0.72 ms

AC

---- 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$

■
```

606

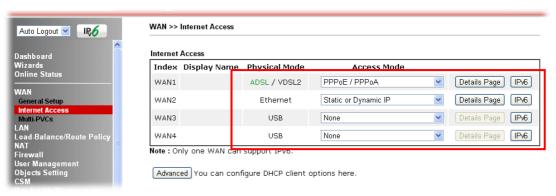
IX-5 Checking If the ISP Settings are OK or Not

If WAN connection cannot be up, check if the LEDs (according to the LED explanations listed on section 1.2) 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/FTTX(GPON)/Cable modem) 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.



IX-6 Problems for 3G/4G Network Connection

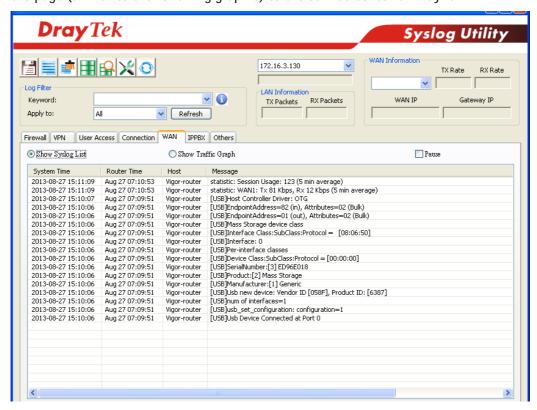
When you have trouble in using 3G/4G network transmission, please check the following:

Check if USB LED lights on or off

You have to wait about 15 seconds after inserting 3G/4G USB Modem into your Vigor2860. 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 Vigor2860.

USB LED lights on but the network connection does not work

Check the PIN Code of SIM card is disabled or not. Please use the utility of 3G/4G USB Modem to disable PIN code and try again. If it still fails, it might be the compliance problem of system. Please open DrayTek Syslog Tool to capture the connection information (WAN Log) and send the page (similar to the following graphic) to the service center of DrayTek.



Transmission Rate is not fast enough

Please connect your Notebook with 3G/4G USB Modem to test the connection speed to verify if the problem is caused by Vigor2860. 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 loose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null.

Software Reset

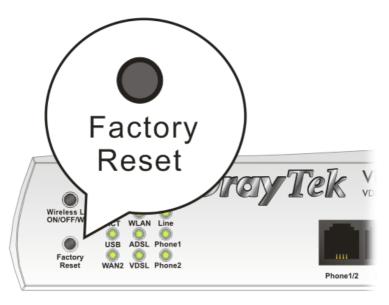
You can reset the router to factory default via Web page. Such function is available in **Admin Mode** only.

Go to System Maintenance and choose Reboot System on the web page. The following screen will appear. Choose Using factory default configuration and click 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
O Using factory default configuration
Reboot Now Auto Reboot Time Schedule
Index(1-15) in <u>Schedule</u> Setup:,,,,
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

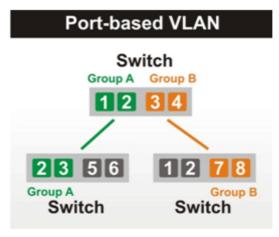
If the router still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@DrayTek.com.

Appendix I: VLAN Applications on Vigor Router

Virtual Local Area Network is so-called VLAN. It offers the logical grouping technique to separate the physical ports of Ethernet switches, thus we can manage our local network easier, more flexible and secure. For instance, you're a networking administrator in your company and you're planning to isolate the visitors' traffics from your private network for security considerations because you cannot ensure that visitors' computer is clean. Or you want to separate your private network into several parts by divisions because there are too many computers in the same network segment and it results in the local traffics heavily. VLAN helps you to solve these situations, and DrayTek's products support bellow two popular types:

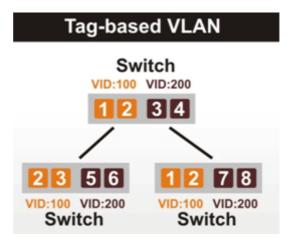
Port-based

It uses a matrix table of the physical ports to define the traffics how to exchange between each port, and the traffics will be isolated from the ports are not being ticked in the same line. It is the easiest way to setup an isolate network, but not a flexible way to maintain a growing network. Because the idea of port-based VLAN is grouping by physical ports, but the difficulty is how to handle the traffics between two or more Ethernet switches. Thus, VLAN is suitable for some circumstances, for example, the rental apartment, SOHO office...and so on. These clients may need two or three isolated networks only and setup a network in a simple way.



Tag-based

The idea of tag-based VLAN is to identify a virtual LAN with a specific ID, therefore, VLAN ID introduced by tag-based VLAN. Through VLAN ID, ports with different VID (VLAN ID) will be identified as in different LANs, so the traffics also will be isolated from each of VLANs. Many administrators who manage an enterprise network or even the internet service providers (ISP) adopt Tag-based VLAN popularly because it is convenient to maintain and manage a distributed network. Setting a large-scale network is easy by giving each of them with different VID and isolating the traffics at the same time. Besides the VLAN ID, there is another feature, Trunk, introduced. While the role of a port on an Ethernet switch is setup as a Trunk port, it means the VLAN ID will be kept while forwarding the packets between switches. By this feature, VLANs are able to distribute over two or more Ethernet switches easily, moreover design a large and secured network is possible through Trunk port. When VLAN is being enabled on Vigor routers, the LAN ports are being turned into Trunk mode automatically. Therefore, a VLAN supported switch, like VigorSwitch G2260/P2261, or VigorSwitch G1240, is needed.



Vigor routers [Note] support Tag-based feature both on LAN and WAN interfaces. The next we'll demonstrate our web design and how to configure the settings by introducing the functionalities of Vigor router.

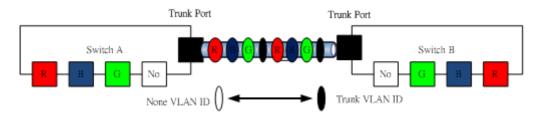
[Note]

Broadband router: Vigor2920/Vigor3200/Vigor2925/Vigo2960/Vigor3900

Modem router: Vigor2850/Vigor2860

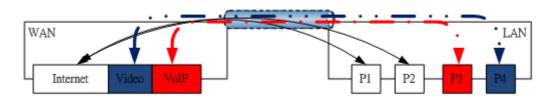
VLAN Packets on Vigor routers

Trunk mode of LAN



Trunk Port can carry the packets with VID but replace the Non-VID packet as the VID of Trunk port while forwarding the packets to another switch.

Bridge mode of WAN

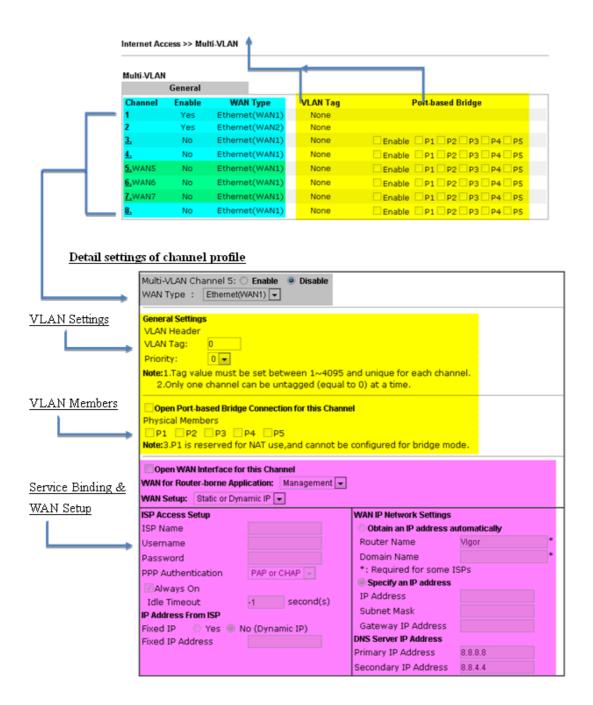


P1 and P2 are doing NAT flow to access to the internet, but P3 and P4 will forward the packets between WAN and LAN ports directly.

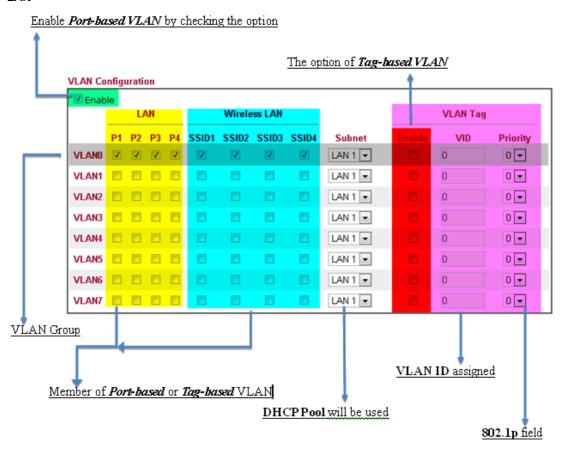
Web User Interface

So far, there are two kinds of open system on Vigor router. One is DrayOS, which is DrayTek owned, and another is Linux-like which customized by DrayTek from OpenWRT. Here DrayOS system is going to be introduced to you because it is the most stable and superfast booting system in DrayTek products. If the UI style of yours is different from the following. It may not DrayOS system with new web style or maybe the Linux-like model.

WAN

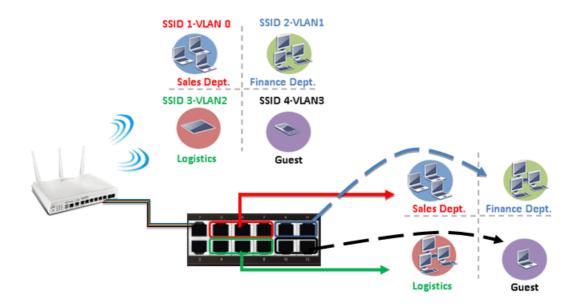


LAN

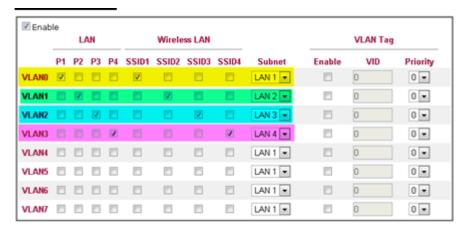


VLAN applications on Vigor router

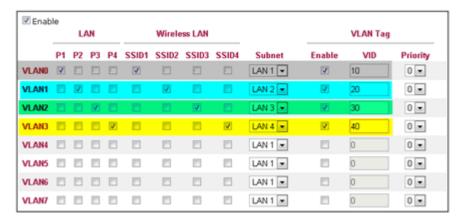
Multi Subnet (VLAN of LAN)



Port-based mode

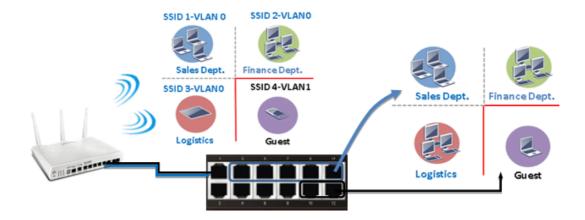


Tag-based mode



By above settings, there are four private networks will be created and computers attached with each of LAN ports or SSIDs which are able to obtain a private IP address from each DHCP server (LAN1/LAN2/LAN3/LAN4). However, the traffics of the LAN port or SSID that are NOT being grouped in the same VLAN are unable to forward to each other. The benefit of Port-based is able to extend the wired ports by installing a cheaper dumb switch as many as you need, but Tag-based offers you a flexible and well-managed network. The networks are isolated, secured and reduce the broadcasting storm effectively in each of networks with VLAN.

Guest Network

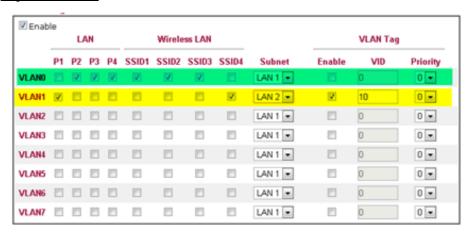


Port-based mode

VLAN Configuration

 Enab	le											
	LAN			Wireless LAN				VLAN Tag				
	P1	P2	Р3	P4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
VLAN0	\overline{V}	\checkmark	V	\checkmark	7	V	V	6	LAN 1 💌		0	0 💌
VLAN1								V	LAN 2 💌		0	0 💌
VLAN2									LAN 1 ▼		0	0 💌
VLAN3									LAN 1 ▼		0	0 💌
VLAN4									LAN 1 ▼		0	0 -
VLAN5									LAN 1 ▼		0	0 💌
VLAN6									LAN1 ▼		0	0 💌
VLAN7						E13			LAN 1 💌	E	0	0 💌

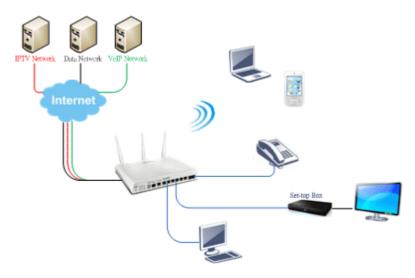
Tag-based mode



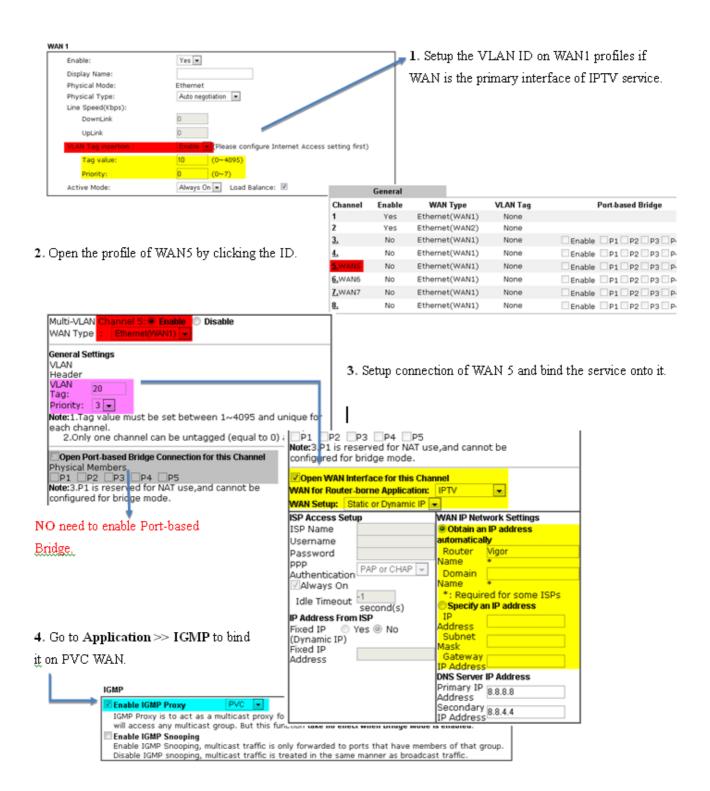
To deploy a guest network, which serves your guests the internet accessibility, but the traffics have to be isolated from your private network due to the security considerations, it can be done by above settings. However, a switch support VLAN function is need if VLAN Tag enabled.

Triple Play (Multi-WAN)

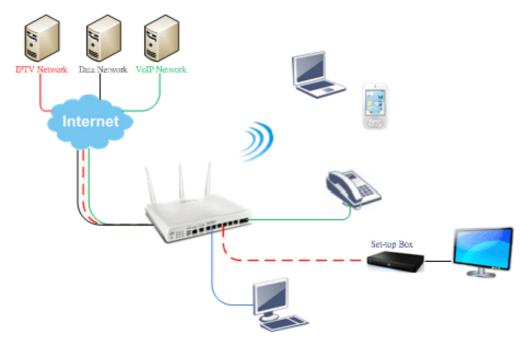
NAT mode with VLAN



Following settings, the set-top box (STB) is able to attach with any LAN port. Video streaming which your ISP provided will be played on your monitor.



Bridge mode with VLAN





Set-top box (STB) or the other kinds of media devices are able to attach with Port4 or Port5 of LAN. Those devices that attached with Port4 or Port5 are able to access the services network directly which your ISP provided.

Part X Telnet Commands

Accessing Telnet of Vigor2860

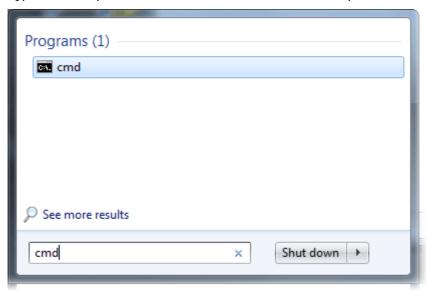
This chapter also gives you a general description for accessing telnet and describes the firmware versions for the routers explained in this manual.



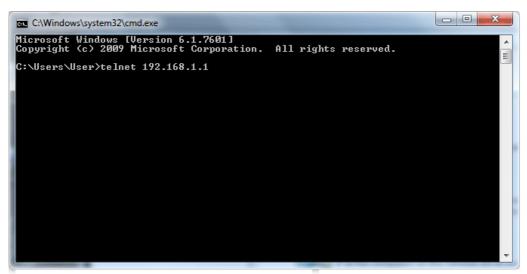
Info

For Windows 7 user, please make sure the Windows Features of Telnet Client has been turned on under Control Panel>>Programs.

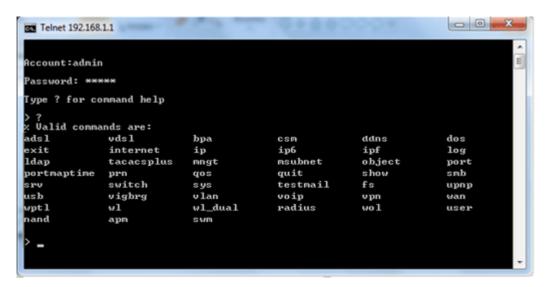
Type cmd and press Enter. The Telnet terminal will be open later.



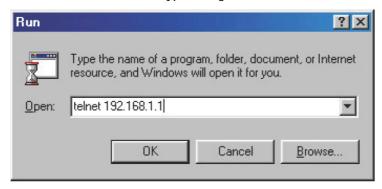
In the following window, type Telnet 192.168.1.1 as below and press Enter. Note that the IP address in the example is the default address of the router. If you have changed the default, enter the current IP address of the router.



Next, type admin/admin for Account/Password. Then, type? You will see a list of valid/common commands depending on the router that your use.



For users using previous Windows system (e.g., 2000/XP), simply click Start >> Run and type Telnet 192.168.1.1 in the Open box as below. Next, type admin/admin for Account/Password. And, type ? to get a list of valid/common commands.



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]

Parameter	Description
auto	It means auto detection of ADSL transmission packet.
percent	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 [more | counts | hlog | qln | snr | bandinfo | olr]

Example

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 acqlP 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. Type 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.

```
> 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.

Syntax

adsl bridge [pvc_no/status/save/enable/disable] [on/off/clear/tag tag_no] [service type]
[px ...]

Syntax Description

Parameter	Description
pvc_no	It means <i>pvc</i> number and must be between 0(Channel 1) to 7(Channel 8).
status	It means to shown the whole bridge status.
save	It means to save the configuration to flash.
enable	It means to enable the Multi-VLAN function.
disable	It means to disable the Multi-VLAN function.
on/off	It means to turn on/off bridge mode for the specific channel.
clear	It means to turn off and clear all the PVC settings.
tag tag_no	No tag: -1 Available number for tag: 0-4095
pri pri_no	The number 0 to 7 can be set to indicate the priority. "7" is the highest.
service type	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.
рх	It means the number of LAN port (x=2~4). Port 1 is locked for NAT.

Telnet Command: adsl idle

This command can make the router accessing into the idle status. If you want to invoke the router again, you have to reboot the router by using "reboot" command.

Syntax

adsl idle [on | tcpmessage | tcpmessage_off]

Syntax Description

Parameter	Description
on	DSL is under test mode.
tcpmessage	DSL debug tool mode is off. DSL debug tool mode is on.
tcpmessage_off	DSL debug tool mode is off.

Example

```
> adsl idle on
% DSL is under [IDLE/QUIET] test mode.
% DSL debug tool mode is off.
> adsl idle tcpmessage
% Set DSL debug tool mode on. Please reboot system to take effect.
> adsl idle tcpmessage_off
% Set DSL debug tool mode off. Please reboot system to take effect.
```

Telnet Command: adsl drivemode

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 reboot the router.

```
> 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.

Syntax

adsl oamlb [n][type]
adsl oamlb chklink [on/off]
adsl oamlb [log_on/log_off]

Syntax Description

Parameter	Description
n	It means the total number of transmitted packets.
type	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)
chklink	Check the DSL connection.
Log_on/log_off	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.

Syntax

adsl vcilimit [n]

Syntax Description

Parameter	Description
n	The number shall be between 1 ~ 254.

```
> 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.

Syntax

adsl automode [add/remove/set/default/show] [adsl_mode]

Syntax Description

Parameter	Description
add	It means to add ADSL mode.
remove	It means to remove ADSL mode.
set	It means to use default settings plus the new added ADSL mode.
default	It means to use default settings.
show	It means to display current setting.
adsl_mode	There are three modes to be choose, ANNEXL, ANNEXM (annexA: ADSL over POTS) and ANNEXJ (annexB: ADSL over ISDN).

Example

```
> adsl automode set ANNEXJ
Automode supported: T1.413, G.DMT, ADSL2, ADSL2+, ANNEXJ,

> 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.

Syntax

adsl showbins [startbin endbin | up]

Syntax Description

Parameter	Description
startbin	The number is between 0 ~ 4092.
endbin	The number is between 4 ~ 4095.
ир	Show upstream information.

```
> 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
```

Telnet Command: adsl optn

This command allows you to configure DSL line feature.

Syntax

adsl optn FUNC [us/ds/bi [value/on/off]]

Syntax Description

Parameter	Description
FUNC	Available settings contain: 'bitswap', 'sra', 'aelem', 'g.vector', 'status', 'trellis', 'retx', 'default'.
us/ds/bi	us: upstream ds: downstream bi: bidirection. 'aelem' and 'g.vector' can be only on/off.
value	The value shall be hex digits. bitswap=0~2, sra=0,2,3,4.
on/off	Type "on" for enabling such function. Type "off" for disabling such function.

Example

```
> adsl optn default
trellis
           [US] =
                      ON, [DS] =
bitswap
            [US] =
                     0, [DS] =
           [0: default(ON), 1: ON, 2: OFF]
                     0, [DS] =
           [US] =
                                    0.
sra
           [0: default(=3), 2: OFF, 3: ON , 4: DYNAMIC SOS]
                     ON, [DS] =
retx
           [US] =
                                   ON.
aelem
            ON
            ON
G.Vector
```

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.

Syntax

adsl vendorid [status/on/off/ set vid0 vid1]

Syntax Description

Parameter	Description
status	Display current status of user-defined vendor ID.
on	Enable the user-defined function.
off	Disable the user-defined function.
set vid0 vid1	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.

Syntax

```
adsl atm pcr [pvc_no][PCR][max][status]
adsl atm scr [pvc_no][SCR]
adsl atm mbs [pvc_no][MBS]
adsl atm status
```

Syntax Description

Parameter	Description
pvc_no	It means <i>pvc</i> number and must be between 0(Channel 1) to 7(Channel 8).
PCR	It means Peak Cell Rate for upstream. The range for the number is "1" to "2539".
max	It means to get the highest speed for the upstream.
SCR	It means Sustainable Cell Rate.
MBS	It means Maximum Burst Size.
status	It means to display PCR/SCR/MBS setting.

	0	1	0
	1	2	200
	2	3	0
	3	4	0
	4	5	0
	5	6	0
	6	7	0
	7	8	0
>	ads	l atm mbs	2 300 max
%	MBS	is 300 for	r pvc 2.

Telnet Command: adsl pvcbinding

This command can configure PVC to PVC binding. Such command is available only for PPPoE and MPoA 1483 Bridge mode.

Syntax

adsl pvcbinding [pvc_x pvc_y | status | -1]

Syntax Description

Parameter	Description
pvc_x	It means the PVC number for the source.
pvc_y	It means the PVC number that the source PVC will be bound to.
status	Display a table for PVC binding group.
-1	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
со	It means DSLAM (Digital Subscriber Line Access Multiplexer) or CO (Central Office).
сре	It means CPE (Customer Premise Equipment).

```
> 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: vdsl status

This command is used to display current status of VDSL setting.

Syntax

vdsl status [more | counts | hlog | qln | snr | bandinfo | olr]

Example

Telnet Command: vdsl idle

This command can make the router accessing into the idle status. If you want to invoke the router again, you have to reboot the router by using "reboot" command.

Syntax

vdsl idle [on | tcpmessage | tcpmessage_off]

Syntax Description

Parameter	Description
on	DSL is under test mode.
	DSL debug tool mode is off.

tcpmessage	DSL debug tool mode is on.
tcpmessage_off	DSL debug tool mode is off.

Example

```
> vdsl idle on
% DSL is under [IDLE/QUIET] test mode.
% DSL debug tool mode is off.
> vdsl idle tcpmessage
% Set DSL debug tool mode on. Please reboot system to take effect.
> vdsl idle tcpmessage_off
% Set DSL debug tool mode off. Please reboot system to take effect.
```

Telnet Command: vdsl drivermode

This command is useful for laboratory to measure largest power of data transmission. Please follow the steps below to set vdsl 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 vdsI2/2+ led is always ON.
- 5. Use 'vdsl reboot' to restart dsl to normal mode.

Telnet Command: vdsl reboot

This command can reboot the DSL router.

Example

```
> vdsl reboot
% Adsl is Rebooting...
```

Telnet Command: vdsl annex

This command can display the annex interface of this router.

Example

```
> vdsl annex
% hardware is annex A.
% ADSL modem code is annex A
```

Telnet Command: vdsl showbins

This command can display the allocation for each Bin (Tone) SNR, Gain, and Bits.

Syntax

vdsl showbins [startbin endbin | up]

Syntax Description

Parameter	Description
startbin	The number is between 0 ~ 4092.
endbin	The number is between 4 ~ 4095.
ир	Show upstream information.

```
> vdsl showbins 2 30
DOWNSTREAM:
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
dB .1dB ts dB .1dB ts dB .1dB ts dB .1dB ts
```

Telnet Command: vdsl optn

This command allows you to configure DSL line feature.

Syntax

vdsl optn FUNC [us/ds/bi [value/on/off]]

Syntax Description

Parameter	Description
FUNC	Available settings contain: 'bitswap', 'sra', 'aelem', 'g.vector', 'status', 'trellis', 'retx', 'default'.
us/ds/bi	us: upstream ds: downstream bi: bidirection. 'aelem' and 'g.vector' can be only on/off.
value	The value shall be hex digits. bitswap=0~2, sra=0,2,3,4.
on/off	Type "on" for enabling such function. Type "off" for disabling such function.

Example

Telnet Command: vdsl savecfg

This command can save the configuration into FLASH with a file format of cfg.

Example

```
> vdsl savecfg
% Xdsl Cfg Save OK!
```

Telnet Command: vdsl vendorid

This command allows you to configure user-defined CPE vendor ID.

Syntax

vdsl vendorid [status/on/off/ set vid0 vid1]

Syntax Description

Parameter	Description	
status	Display current status of user-defined vendor ID.	
on	Enable the user-defined function.	
off	Disable the user-defined function.	
set vid0 vid1	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

```
> vdsl vendorid status
% User define CPE Vendor ID is OFF
% vid0:vid1 = 0x00fe7244:79612f21
> vdsl vendorid on set vid0 vid1
% User define CPE Vendor ID is ON
```

Telnet Command: vdsl inventory

This command is used to display information about CO or CPE.

Syntax

vdsl inventory [co/cpe]

Syntax Description

Parameter	Description
со	It means DSLAM (Digital Subscriber Line Access Multiplexer) or CO (Central Office).
cpe	It means CPE (Customer Premise Equipment).

```
> vdsl inventory co
xDSL inventory info only available in showtime.
> vdsl 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
                          : 0XB500
 System country code
                           : IFTN
 System provider code
 System vendor info
                          : 0x000
Version number

Version number(16 octets) : 0X3
: PASS
                         : 3.8.2_RC4a_STD
                            : 0X332E382E325F524334615F5354440000
Transmission mode capability : 0X40004004C010400
```

Telnet Command: bpa

This command allows to configure a network setting specified for Australia's ISP.

Syntax

bpa m [-<command> <parameter> | ...]

Syntax Description

Parameter	Description	
m	Available settings are 1 and 2.	
-a <enable></enable>	1/0 to enable/disable this entry	
-n <username></username>	contact UserName(max. 24 characters)	
-p <password></password>	contact PassWord (max. 24 characters)	
-s <select></select>	It means to specify an IP address for Server.	
	0 : no selection.	
	1: NSW(61.9.192.13)	
	2 : QLD(61.9.208.13),	
	3: VIC(61.9.128.13)	
	4 : SA(61.9.224.13),	
	5 : WA(61.9.240.13)	
-I <list></list>	List all settings configured.	

```
> bpa 1 -a 1 -n testUser -p testPassword -s 4
> bpa -l
-----index: 1 active-----
UserName[1]: testUser
PassWord[1]: testPassword
ServerIP[1]:4
-----index: 2 inactive-----
UserName[2]:
PassWord[2]:
ServerIP[2]:0
>
```

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
INDEX	It means to specify the index number of CSM profile, from 1 to 32.
- V	It means to view the configuration of the CSM profile.
- n	It means to set a name for the CSM profile.
NAME	It means to specify a name for the CSM profile, less then 15 characters.
setdefault	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.

csm appe set -i INDEX [-v GROUP| -e AP_IDX | -d AP_IDX| -a AP_IDX [ACTION]]

Parameter	Description
INDEX	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
GROUP	Specify the category of the application. Available options are: IM, P2P, Protocol and Others.
AP_IDX	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 inex number, do the following (Take IM as an example): Type "csm appe set -I 1 -v IM", the system will list all of the index numbers of the applications categorized under IM.
ACTION	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.

```
>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. csm appe show [-a/-i/-p/-t/-m]

Syntax Description

Parameter	Description
-a	View the configuration status for AII groups.
-i	View the configuration status of IM group.
-р	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				
Туре	Index	Name	Version Advanc	e
Advanced Option:	(M)essage,	(F)ile Transfer,	(G)ame, (C)onference	, and (0)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.

csm appe config -v INDEX [-i/-p/-t/-m]

Syntax Description

Parameter	Description
INDEX	Specify the index number of CSM profile, from 1 to 32.
-i	View the configuration status of IM group.
- <i>p</i>	View the configuration status of P2P group.
-t	View the configuration status of protocol group.
-m	View the configuration status of Others group.

```
> csm appe config -v 1 -m
```

vance Enable	**	Index		Enable A Conference, and Other	
Advance abbre		-		conference, and coner	
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		
OTHERS	TUNNEL	84	Ping Tunnel	Disable	
•					
•					
Total 66 APPs					
TOTAL DO APPS					
>					

Telnet Command: csm appe interface

It is used to configure APPE signature download interface. csm appe interface [AUTO/WAN#]

Syntax Description

Parameter	Description	
AUTO	Vigor router specifies WAN interface automatically.	
WAN	Specify the WAN interface for signature downloading.	

```
> 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 checkd under Enable E-Mail Alert).

csm appe email [-e/-d/-s]

Syntax Description

Parameter	Description	
-е	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.

Syntax

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

Parameter	Description
show	It means to display all of the profiles.
setdefault	It means to return to default settings for all of the profile.
msg MSG	It means de set the administration message. MSG means the content (less than 255 characters) of the message itself.
obj	It means to specify the object for the profile.
INDEX	It means to specify the index number of CSM profile, from 1 to 8.
-n	It means to set the profile name.
PROFILE_NAME	It means to specify the name of the profile (less than 16 characters)
-р	Set the priority (defined by the number specified in VALUE) for the profile.

VALUE	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.
-/	It means the log type of the profile. They are: P: Pass, B: Block, A: AII, N: None
MSG	It means to specify the Administration Message, less then 255 characters
uac	It means to set URL Access Control part.
wf	It means to set Web Feature part.

Telnet Command: csm ucf obj INDEX uac

It means to configure the settings regarding to URL Access Control (uac).

Syntax

```
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
```

Parameter	Description
INDEX	It means to specify the index number of CSM profile, from 1 to 8.

- V	It means to view the protocol configuration of the CSM profile.
-е	It means to enable the function of URL Access Control.
-d	It means to disable the function of URL Access Control.
-a	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	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.
-0	Set the keyword object.
KEY_WORD_Object_Index	Specify the index number of the object profile.
<i>-g</i>	Set the keyword group.
KEY_WORD_Group_Index	Specify the index number of the group profile.

```
> 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).

Syntax

```
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
INDEX	It means to specify the index number of CSM profile, from 1 to 8.
- V	It means to view the protocol configuration of the CSM profile.
-е	It means to enable the restriction of web feature.
-d	It means to disable the restriction of web feature.
-a	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>	It means to enable the the Web Feature configuration.
	Features available for configuration are:
	c: Cookie
	p: Proxy
	u: Upload
-U	It means to cancel the web feature configuration.
-f	It means to set the file extension object index number.
File_Extension_Object_inde x	Type the index number (1 to 8) for the file extension object.

```
[ ]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).

Syntax

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

Parameter	Description
show	It means to display the web content filter profiles.
Look	It means to display the license information of WCF.
Cache	It means to set the cache level for the profile.
Server WCF_SERVER	It means to set web content filter server.
Msg MSG	It means de set the administration message.
	MSG means the content (less than 255 characters) of the message itself.
setdefault	It means to return to default settings for all of the profile.
obj	It means to specify the object profile.
INDEX	It means to specify the index number of web content filter profile, from 1 to 8.
- V	It means to 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	It means to set the profile name.
PROFILE_NAME	It means to specify the name of the profile (less than 16 characters)
-1	It means the log type of the profile. They are:

	P: Pass,
	B: Block,
	A: AII,
	N: None
-0	Set the keyword object.
KEY_WORD_Object_Index	Specify the index number of the object profile.
<i>-g</i>	Set the keyword group.
KEY_WORD_Group_Index	Specify the index number of the group profile.
-W	It means to set the action for the black and white list.
	E:Enable,
	D:Disable,
	P:Pass,
	B:Block
-S	It means to choose the items under CATEGORY or WEB_GROUP.
-U	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)

```
> 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]Nudity
 [v]Hate & Intolerance [v]Illegal Drug
 [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
                   [ ]Leisure & Recreation [ ]Fashion & Beauty
 [ ]Travel
```

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 -u WCF_PROFILE

csm dnsf profile_edit INDEX -u UCF_PROFILE
```

Syntax Description

Parameter	Description
enable	Enable or disable DNS Filter.
	ON: enable.
	OFF: disable.
syslog	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.
service WCF_PROFILE	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).
time CACHE_TIME	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.
blockpage	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 visisted.
	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.
profile_show	Display the table of the DNS filter profile.
profile_edit	Modify the content of the DNS filter profile.
-n PROFILE_NAME	PROFILE_NAME: Type the name of the DNS filter profile that you want to modify.
-I N/P/B/A	Specify the log type of the profile.
	P: Pass.
	B: Block.
	A: AII.
	N: None.
-w WCF_PROFILE	WCF_PROFILE: Type the index number of the WCF profile.
-u UCF_PROFILE	UCF_PROFILE: Type the index number of the UCF profile.
-c CACHE_TIME	-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.

```
> 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.

Syntax

ddns time <update in minutes>

Syntax Description

Parameter	Description
Update in minutes	Type the value as DDNS time. The range is from 1 to 14400.

Example

```
> ddns time
ddns time <update in minutes>
Valid: 1 ~ 1440
%Now: 1440
> ddns time 1000
ddns time <update in minutes>
Valid: 1 ~ 1440
%Now: 1000
```

Telnet Command: dos

This command allows users to configure the settings for DoS defense system.

Syntax

```
dos [-V | D | A]
dos [-s ATTACK_F [THRESHOLD][ TIMEOUT]]
dos [-a | e [ATTACK_F][ATTACK_0] | d [ATTACK_F][ATTACK_0]]
```

Parameter	Description
-V	It means to view the configuration of DoS defense system.
-D	It means to deactivate the DoS defense system.
-А	It means to activate the DoS defense system.
-S	It means to enable the defense function for a specific attack and set its parameter(s).
ATTACK_F	It means to specify the name of flooding attack(s) or portscan, e.g., synflood, udpflood, icmpflood, or postscan.
THRESHOLD	It means the packet rate (packet/second) that a flooding attack will be detected. Set a value larger than 20.

TIMEOUT	It means the time (seconds) that a flooding attack will be blocked. Set a value larger than 5.
-a	It means to enable the defense function for all attacks listed in ATTACK_0.
-е	It means to enable defense function for a specific attack(s).
ATTACK_0	It means to specify a name of the following attacks: ip_option, tcp_flag, land, teardrop, smurf, pingofdeath, traceroute, icmp_frag, syn_frag, unknow_proto, fraggle.
-d	It means to disable the defense function for a specific attack(s).

```
>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> / ...]

Parameter	Description
-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
<command/> <parameter>]</parameter>	The available commands with parameters are listed below. [] means that you can type in several commands in one line.
-S <isp name=""></isp>	It means to set ISP Name (max. 23 characters).
-P <on off=""></on>	It means to enable PPPoE Service.
-u <username></username>	It means to set username (max. 49 characters) for Internet accessing.
-p <password></password>	It means to 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	It means to 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=""></ip>	It means that <i>PPPoE server</i> 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.</ip>
-w <ip address=""></ip>	It means to assign WAN IP address for such connection. Please type an IP address here for WAN port.
-n <netmask></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></gateway>	It means to assign gateway IP for such WAN connection.
-V	It means to view Internet Access profile.
-C <sim code="" pin=""></sim>	Set (PPP mode) SIM PIN code (max. 15 characters).
-0 <init string=""></init>	Set (PPP mode) Modem Initial String (max. 47 characters).
-T <init string2=""></init>	Set (PPP mode) Modem Initial String2 (max. 47 characters)
-D <dial string=""></dial>	Set (PPP mode) Modem Dial String (max. 31 characters).
-v <service name=""></service>	Set (PPP mode) Service Name (max. 23 characters).
-m <ppp username=""></ppp>	Set (PPP mode) PPP Username (max. 63 characters).
-o <ppp password=""></ppp>	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></mode>	Set (PPP mode or DHCP mode) WAN Connection Detection Mode. <mode> 0: ARP Detect; 1: Ping Detect</mode>
-l <ping ip=""></ping>	Set (PPP mode or DHCP mode) WAN Connection Detection Ping IP. <pre><pre><pre><pre><pre><pre><pre><pre></pre></pre></pre></pre></pre></pre></pre></pre>
-L n	Set (PPP mode) WAN Connection Detection TTL (1-255) value.
-E <sim code="" pin=""></sim>	Set (DHCP mode) SIM PIN code (max. 19 characters).
-G <mode></mode>	Set (DHCP mode) Network Mode. <mode> 0: 4G/3G/2G; 1: 4G Only; 2: 3G Only; 3: 2G Only</mode>
-N <apn name=""></apn>	Set (DHCP mode) APN Name (max. 47 characters)
-U n	(DHCP mode) MTU(1000-1440)

>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
```

Telnet Command: ip pubsubnet

This command allows users to enable or disable the IP routing subnet for your router.

Syntax

ip 2ndsubnet < Enable / Disable >

Syntax Description

Parameter	Description
Enable	Enable the function.
Disable	Disable the function.

Example

```
> ip 2ndsubnet enable
2nd 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
?	Display an IP address which allows users set as the public subnet IP address.
public subnet IP address	Specify an IP address. The system will set the one that you specified as the public subnet IP address.

```
> 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
?	Display an IP address which allows users set as the public subnet mask.
public subnet IP address	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
add	It means to create a new WAN IP address.
remove	It means to delete an existed WAN IP address.
IP	It means the auxiliary WAN IP address.
Join to NAT Pool	0 (disable) or 1 (enable).
wanX	Add or remove an address for WAN interface.
index	Type the index number of the table displayed on your screen.

```
> ip aux add 192.168.1.65 1 % 192.168.1.65 has added in index 2.
```

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
IP address	It means 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
IP netmask	It means the netmask of LAN IP.

Example

```
> ip nmask 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.

Parameter	Description
IP address	It means the LAN IP address.
MAC address	It means the MAC address of your router.
LAN or WAN	It indicates the direction for the arp function.
0/1/2/3/4/5	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.
Time	Available settings will be 10, 20, 30,2550 seconds.

Telnet Command: ip dhcpc

This command is available for WAN DHCP.

Syntax

ip dhcpc option

ip dhcpc option -h/I

ip dhcpc option -d [idx]

ip dhcpc option -e [1 or 0] -w [wan unmber] -c [option number] -v [option value]

ip dhcpc option -e [1 or 0] -w [wan unmber] -c [option number] -x "[option value]"

ip dhcpc option -u [idx unmber]

ip dhcpc release [wan number]

ip dhcpc renew [wan number]

ip dhcpc status

Syntax Description

Parameter	Description
option	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
release	It means to release current WAN IP address.
renew	It means to renew the WAN IP address and obtain another new one.
status	It displays current status of DHCP client.

```
>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/PVC3/PVC4/PVC5 for verifying if the WAN connection is OK or not.

Syntax

ip ping [IP address] [WAN1 /PVC3/PVC4/PVC5]

Syntax Description

Parameter	Description
IP address	It means the WAN IP address.
WAN1/PVC3/PVC4/PVC5	It means the WAN port /PVC 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.

Syntax

ip tracert [Host/IP address] [WAN1/WAN2/WAN3/WAN4/WAN5] [Udp/Icmp]

Parameter	Description
IP address	It means the target IP address.
WAN1/WAN2	It means the WAN port that the above IP address passes through.
Udp/Icmp	It means the UDP or ICMP.

```
>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  168.95.90.66  50ms
5  211.22.38.134  50ms
6  220.128.2.62  50ms
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
IP address	Type the WAN or LAN IP address of the remote device.
Port	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
0/1/2	0 means disable; 1 means first subnet and 2 means second subnet.

```
> ip rip 1
%% Set RIP 1st subnet.
```

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
ifno	It means the connection interface. 1: WAN1,2: WAN2, 3: PVC3,4: PVC4,5: PVC5 Note: PVC3 ~PVC5 are virtual WANs.
-е	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.

```
> 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
WAN[6] Rip Protocol enable
WAN[7] Rip Protocol enable
> 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
add	It means to add an IP address as static route.
del	It means to delete specified IP address.
status	It means current status of static route.
dst	It means the IP address of the destination.
netmask	It means the netmask of the specified IP address.
gateway	It means the gateway of the connected router.
ifno	It means the connection interface. 3=WAN1 5=WAN3,6=WAN4,7=WAN5 However, WAN3, WAN4, WAN5 are router-borne WANs
rtype	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.

```
> 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~ 192.168.1.0/ 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 t_home[on/off/show/help]

ip igmp_proxy query

ip igmp_proxy ppp [0/1]

ip igmp_proxy status

Syntax Description

Parameter	Description
set	It means to enable proxy server.
reset	It means to disable proxy server.
wan	It means to specify WAN interface for IGMP service.
t_home	It means to specify t_home proxy server for using.
On/off/show/help	It means to turn on/off/display or get more information of the T_home service.
query	It means to set IGMP general query interval. The default value is 125000 ms.
ppp	0 - No need to set IGMP with PPP header. 1 - Set IGMP with PPP header.
status	It means to display current status for proxy server.

```
> ip igmp t_home on
%T-Home Setting:
%T-Home Service is turned on.
%WAN1 : Enabled, connection type: PPPoE, without tag for ADSL
%WAN5 : Enabled, connection type: DHCP, tag: 8
%: PVC4(WAN5) is bound to PVC0(WAN1), protocol=MPoA 1483 Bridge
%IGMP Proxy Interface: WAN5(PVC)
%WAN5 for Router-borne Application/ IPTV on/off: ON
> ip igmp_proxy query 130000
This command is for setting IGMP General Query Interval
The default value is 125000 ms
Current Setting is:130000 ms
>
```

Telnet Command: ip dmz

Specify MAC address of certain device as the DMZ host.

Syntax

ip dmz [mac]

Syntax Description

Parameter	Description
mac	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
> ip dmz 11-22-33-44-55-66
> ip dmz ?
% ip dmz <mac>, now : 11-22-33-44-55-66
>
```

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.

Syntax

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]

Parameter	Description
on	It means to turn on session limit for each IP.
off	It means to turn off session limit for each IP.
default [num]	It means to set the default number of session num limit.
Defautlp2p [num]	It means to set the default number of session num limit for p2p.
status	It means to display the current settings.
show	It means to display all session limit settings in the IP range.
timer [num]	It means to set when the IP session block works. The unit is second.

[block/unblock][IP]	It means to 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.
add	It means to add the session limits in an IP range.
del	It means to delete the session limits in an IP range.
IP1-IP2	It means the range of IP address specified for this command.
num	It means the number of the session limits, e.g., 100.
p2pnum	It means the number of the session limits, e.g., 50 for P2P.

```
>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.

Syntax

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]

Parameter	Description
on	It means to turn on the IP bandwidth limit.
off	It means to turn off the IP bandwidth limit.
default [tx_rate][rx_rate]	It means to set default tx and rx rate of bandwidth limit. The range is from 0 - 65535 Kpbs.
status	It means to display the current settings.
show	It means to display all the bandwidth limits settings within the IP range.
add	It means to add the bandwidth within the IP range.
del	It means to delete the bandwidth within the IP range.
IP1-IP2	It means the range of IP address specified for this command.

tx	It means to set transmission rate for bandwidth limit.
rx	It means to set receiving rate for bandwidth limit.
shared	It means that the bandwidth will be shared for the IP range.

```
> 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.

Syntax

ip bindmac on

ip bindmac off

ip bindmac strict_on

ip bindmac show

ip bindmac add [IP][MAC][Comment]

ip bindmac del [IP]/all

Parameter	Description
on	It means to turn on IP bandmac policy. Even the IP is not in the policy table, it can still access into network.
off	It means to turn off all the bindmac policy.
strict_on	It means that only those IP address in IP bindmac policy table can access into network.
show	It means to display the IP address and MAC address of the pair of binded one.
add	It means to add one ip bindmac.
del	It means to delete one ip bindmac.
IP	It means to type the IP address for binding with specified MAC address.
MAC	It means to type the MAC address for binding with the IP address specified.
Comment	It means to type words as a brief description.
AII	It means to delete all the IP bindmac settings.

```
> 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
User no	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: ip6 addr

This command allows users to set the IPv6 address for your router.

Syntax

```
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 type 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.

```
> 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.

Syntax

ip6 dhcp req_opt [LAN/WAN1/WAN2/iface#] [-<command> <parameter>/ ...]

Syntax Description

Parameter	Description	
req_opt	It means option-request.	
LAN/WAN1/WAN2/iface#	It means to specify LAN or WAN interface for such address.	
[<command/> <parameter>]</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.	
-S	It means to ask the SIP.	
-S	It means to ask the SIP name.	
-d	It means to ask the DNS setting.	
-D	It means to ask the DNS name.	
-n	It means to ask NTP.	
-i	It means to ask NIS.	
-1	It means to ask NIS name.	
- <i>р</i>	It means to ask NISP.	
-P	It means to ask NISP name.	
-b	It means to ask BCMCS.	
-В	It means to ask BCMCS name.	
-r	It means to ask refresh time.	
Parameter	the parameter related to the request will be displayed. 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.

Syntax

ip6 dhcp client [WAN1/WAN2/iface#] [-<command> <parameter>/ ...]

Parameter	Description
client	It means the dhcp client settings.

[<command/> <parameter>]</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.
-p [IAID]	It means to request identity association ID for Prefix Delegation.
-n [IAID]	It means to request identity association ID for Non-temporary Address.
-c [parameter]	It means to send rapid commit to server.
-i [parameter]	It means to send information request to server.
-e[parameter]	It means to enable or disable the DHCPv6 client. 1: Enable 0: Disable

```
> 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.

Syntax

ip6 dhcp server [-<command> <parameter>/ ...]

Parameter	Description
server	It means the dhcp server settings.
[<command/> <parameter>]</parameter>	The available commands with parameters are listed below. [] means that you can type in several commands in one line.
<i>-a</i>	It means to show current DHCPv6 status.
-i <pool_min_addr></pool_min_addr>	It means to set the start IPv6 address of the address pool.
-x <pool_max_addr></pool_max_addr>	It means to set the end IPv6 address of the address pool.
-d <addr></addr>	It means to set the first DNS IPv6 address.
-D <addr></addr>	It means to set the second DNS IPv6 address.
-c <parameter></parameter>	It means to send rapid commit to server. 1: Enable 0: Disable
-e <parameter></parameter>	It means to enable or disable the DHCPv6 server. 1: Enable 0: Disable

Telnet Command: ip6 internet

This command allows you to configure settings for accessing Internet.

Syntax

ip6 internet -W n -M n [-<command> <parameter> / ...]

Parameter	Description
-W n	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
-M n	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
[<command/>	The available commands with parameters are listed below.
<pre><parameter>]</parameter></pre>	[] means that you can type in several commands in one line.
-m n	It means to set IPv6 MTU.
	N = any value (0 means "unspecified").
-u <username></username>	It means to set Username.
	<username>= type a name as the username (maximum 63 characters).</username>
-p <password></password>	It means to set Password.
	<pre><password> = type a password (maximum 63 characters).</password></pre>
-s <server></server>	It means to set Tunnel Server IP.

	<server>= IPv4 address or URL (maximum 63 characters).</server>
-d <server></server>	It means to set the primary DNS Server IP. <server>= type an IPv6 address for first DNS server.</server>
-D <server></server>	It means to set the secondary DNS Server IP. <server>= type an IPv6 address for second DNS server.</server>
-t <dhcp none="" ra=""></dhcp>	It means to set IPv6 PPP WAN test mode for DHCP or RADVD. <dhcp none="" ra="">= type IPv6 address.</dhcp>
-V	It means to view IPv6 Internet Access Profile.
-0	It means to set AICCU always on. 1=On, 0=Off

```
> ip6 internet -W 2 -M 2 -u 88886666 -p draytek123456 -s
amsterdam.freenet6.net
This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
> system reboot
```

Telnet Command: ip6 neigh

This command allows you to display IPv6 neighbour table.

Syntax

ip6 neigh -s[inet6_addr] [eth_addr] [LAN/WAN1/WAN2]
ip6 neigh -d [inet6_addr] [LAN/WAN1/WAN2]
ip6 neigh -a [inet6_addr] [-N LAN/WAN1/WAN2]

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.

```
> 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 CONNECTED
                                       00-00-00-00-00 CONNECTED
WAN2 2001:2222:6666::1111
```

WAN2 ::	00-00-00-00-00	CONNECTED
LAN ::		NONE
>		

Telnet Command: ip6 pneigh

This command allows you to add a proxy neighbour.

Syntax

```
ip6 pneigh -s inet6_addr [LAN/WAN1/WAN2]
ip6 pneigh -d inet6_addr [LAN/WAN1/WAN2]
ip6 pneigh -a [inet6_addr] [-N LAN/WAN1/WAN2]
```

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
LAN/WAN1/WAN2	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 -d [prefix] [prefix-length]
ip6 route -a [LAN/WAN1/WAN2/iface#]
```

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 type 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.
LAN/WAN1/WAN2/iface#	It means to specify LAN or WAN interface for such address.

```
> 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 _EXP	IRES	NEXT-HOP_	I/F	METRIC	STATE	FLAGS
FE80::/128			LAN	0	UNICAST	U
	0	::				
FE80::250:7FFF:FE00:0/1	.28		LAN	0	UNICAST	U
	0	::				
FE80::/64			LAN	256	UNICAST	U
	0					
FE80::/16			LAN	1024	UNICAST	UGA
	0	FE80::250:7FF	F:FE12	2:100		
FF02::1/128			LAN	0	UNICAST	UC
	0	FF02::1				
FF00::/8			LAN	256	UNICAST	U
	0					
::/0			LAN	-1	UNREACHABL	E !
	0					

Telnet Command: ip6 ping

This command allows you to pin an IPv6 address or a host.

Syntax

ip6 ping [IPV6 address/Host] [LAN/WAN1/WAN2]

Syntax Description

Parameter	Description
IPV6 address/Host	It means to specify the IPv6 address or host for ping.
LAN/WAN1/WAN2	It means to specify LAN or WAN interface for such address.

```
> 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
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.

Syntax

ip6 tracert [IPV6 address/Host]

Syntax Description

Parameter	Description
IPV6 address/Host	It means to specify the IPv6 address or host for ping.

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
                          330 ms
 7 2001:4860::8:0:2DAF
 8 2001:4860::2:0:66<sup>E</sup>
                          340 ms
 9 Request timed out.
10 2001:4860:4860::8888 350 ms
Trace complete.
```

Telnet Command: ip6 tspc

This command allows you to display TSPC status.

Syntax

ip6 tspc [ifno]

Syntax Description

Parameter	Description
ifno	It means the connection interface.
	Ifno=1 (means WAN1)
	Info=2 (means WAN2)

```
> ip6 tspc 2
Local Endpoint v4 Address : 111.243.177.223
Local Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b9
Router DNS name : 8886666.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

lp6 radvd -s [1/0] [lifetime] ip6 radvd -V

Syntax Description

Parameter	Description
-S	It means to enable or disable the default lifetime of the RADVD server. 1: Enable the RADVD server. 0: Disable the RADVD server.
Lifetime	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. Type the number (unit: second) you want.
-V	It means to show the RADVD configuration.
-r	It means RA default test.
-r [num]	It means RA test for item [num].

Example

```
> ip6 radvd -s 1 1800
> ip6 radvd -V
% IPv6 Radvd Config:
Radvd : Enable, Default Lifetime : 1800 seconds
```

Telnet Command: ip6 mngt

This command allows you to manage the settings for access list.

Syntax

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]

Parameter	Description
list	It means to show the setting information of the access list.
status	It means to show the status of IPv6 management.
add	It means to add an IPv6 address which can be used to execute

	management through Internet.
index	It means the number (1, 2 and 3) allowed to be configured for IPv6 management.
prefix	It means to type the IPv6 address which will be used for accessing Internet.
prefix-length	It means to type a fixed value as the length of the prefix.
remove	It means to remove (delete) the specified index number with IPv6 settings.
flush	It means to clear the IPv6 access table.
http/telnet/ping/https/ssh	These protocols are used for accessing Internet.
on/off	It means to enable (on) or disable (off) the Internet accessing through http/telnet/ping.

```
> 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
FE80::250:7FFF:FE12:1010
                                 128
     FE80::250:7FFF:FE12:1020
                                 128
     FE80::250:7FFF:FE12:2080
                                 128
> ip6 mngt status
% IPv6 Remote Management :
             http: off, ping: off
telnet : off,
```

Telnet Command: ip6 online

This command allows you to check the online status of IPv6 LAN /WAN.

Syntax

ip6 online [ifno]

Syntax Description

Parameter	Description
ifno	It means the connection interface.
	0=LAN1
	1=WAN1
	2=WAN2

```
> ip6 online 0
% LAN 1 online status :
% Interface : UP
% IPv6 DNS Server: :: Static
% IPv6 DNS Server: :: Static
% IPv6 DNS Server: :: Static
```

```
% Tx packets = 408, Tx bytes = 32160, Rx packets = 428, Rx bytes =
33636

> ip6 online 1
% WAN 1 online status :
% IPv6 WAN1 Disabled
% Default Gateway : ::
% UpTime : 0:00:00
% Interface : DOWN
% IPv6 DNS Server: :: Static
% Tx packets = 0, Tx bytes = 0, Rx packets = 0, Rx bytes = 0
```

Telnet Command: ip6 aiccu

This command allows you to set IPv6 settings for WAN interface with connection type of AICCU.

Syntax

ip6 aiccu [ifno]

ip6 aiccu subnet [add <ifno> <prefix> <prefix-length> | remove <ifno> | show <info>]

Syntax Description

Parameter	Description
ifno	It means the connection interface. 1=WAN1 2=WAN2
add	It means to add an IPv6 address which can be used to execute
auu 	management through Internet.
prefix	It means to type the IPv6 address which will be used for accessing Internet.
prefix-length	It means to type a fixed value as the length of the prefix.
remove	It means to remove (delete) the specified index number with IPv6 settings.
show	It means to display the AICCU status.

Example

```
> ip6 aiccu subnet add 2 2001:1111:0000::1111 64
> ip6 aiccu 2
Status: Connecting

>ip6 aiccu subnet show 2
IPv6 WAN2 AICCU Subnet Prefix Config:
2001:1111::1111/64
>
```

Telnet Command: ip6 ntp

This command allows you to set IPv6 settings for NTP (Network Time Protocols) server.

Syntax

```
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: 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.

Syntax

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.

Syntax

ipf set [Options]
ipf set [SET_NO] rule [RULE_NO] [Options]

Syntax Description

Parameter	Description
Options	There are several options provided here, such as -v, -c [SET_NO], -d [SET_NO], and etc.
SET_NO	It means to specify the index number (from 1 to 12) of filter set.
RULE_NO	It means to specify the index number (from 1 to 7) of filter rule set.
-V	Type "-v" to view the configuration of general set.
-c [SET_NO]	It means to setup Call Filter, e.g., -c 2. The range for the index number you can type is "0" to "12" (0 means "disable).
-d [SET_NO]	It means to setup Data Filter, e.g., -d 3. The range for the index number you can type is "0" to "12" (0 means "disable).
-I [VALUE]	It means to setup Log Flag, e.g., -1 2 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.
- ρ [VALUE]	It means to setup actions for packet not matching any rule, e.g., -p 1 Type "0" to let all the packets pass; Type "1" to block all the packets.
-M [P2P_NO]	It means to configure IM/P2P for the packets not matching with any rule, e.g., -M 1 Type "0" to let all the packets pass; Type "1" to block all the packets.
-U [URL_NO]	It means to configure URL content filter for the packets not matching with any rule, e.g., -U 1 Type "0" to let all the packets pass; Type "1" to block all the packets.
-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 for session limitation.
-F [VALUE]	It means to configure the load-balance policy.
-Q [VALUE]	It means to set the QoS class.

```
> 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.

Syntax

ipf rule s r [-<command> <parameter> / ...
ipf rule s r -v

Parameter	Description
S	Such word means Filter Set, range form 1~12.
r	Such word means Filter Rule, range from 1~7.
<command/> <parameter></parameter>	The following lists all of the available commands with parameters.
-е	It means to enable or disable the rule setting. 0- disable 1- enable
-s o:g <obj></obj>	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.
-s u <address type=""> <start ip<br="">Address> <end address="" ip=""> <address mask=""></address></end></start></address>	It means to configure source IP address including address type, start IP address, end IP address and address mask. u - It means "user defined". Address Type - Type 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
-d u <address type=""> <start ip<br="">Address> <end address="" ip=""> <address mask=""></address></end></start></address>	It means to configure destination IP address including address type, start IP address, end IP address and address mask.
<addi ess="" iviask=""></addi>	u - It means "user defined".
	Address Type - Type 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
-d o:g <obj></obj>	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.</obj>
-S o:g <obj></obj>	It means to specify Service Type 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 1-96. For example, "-S 0 1" means the first service type object profile.</obj>
-S u <protocol> <source_portvalue></source_portvalue></protocol>	It means to configure advanced settings for Service Type, such as protocol and port range.
<pre><destination_port_vale></destination_port_vale></pre>	u - it means "user defined".
	<pre><pre><pre><pre><pre><pre><pre><pre></pre></pre></pre></pre></pre></pre></pre></pre>
	<pre><source_portvalue> -</source_portvalue></pre>
	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>:</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.
-F	It means the Filter action you can specify. 0 -Pass Immediately,
	1 - Block Immediately,
	i - Diock infinediately,

	2 Dogs if we frusther meetals
	2 - Pass if no further match,
	3 - Block if no further match.
-q	It means the classification for QoS.
	1- Class 1,
	2 - Class 2,
	3 - Class 3,
	4 - Other
-/	It means load balance policy.
	Such function is used for "debug" only.
-E	It means to enable APP Enforcement.
-a <index></index>	It means to specify which APP Enforcement profile will be applied.
	<index> - Available settings range from 0 ~ 32. "0" means no profile will be applied.</index>
-u <index></index>	It means to specify which URL Content Filter profile will be applied.
	<index> - Available settings range from 0 ~ 8. "0" means no profile</index>
	will be applied.
-C	It means to set code page. Different number represents different
	code page. 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=""></windows>	It means to set Window size and Session timeout (Minute).
<session_timeout></session_timeout>	<windows size=""> - Available settings range from 1 ~ 65535.</windows>
	<session_timeout> - Make the best utilization of network resources.</session_timeout>
-V	It is used to show current filter/rule settings.

```
> ipf rule 2 1 -e 1 -s "o 1" -d "o 2" -S "o 1" -F 2
> ipf rule 2 1 -v
Filter Set 2 Rule 1:
```

```
Status : Enable
```

Comments: xNetBios -> DNS

Index(1-15) in Schedule Setup: <null>, <null>, <null>, <null>,

: LAN -> WAN Direction Source IP : Group1, Destination IP: Group2,

Service Type : TCP/UDPGroup1, Fragments : Don't Care

Pass or Block : Block Immediately

Branch to Other Filter Set: None Max Sessions Limit : 32000 Current Sessions : 0

: Non-Strict Mac Bind IP

Oos Class : None URL Content Filter : None
Load-Ralan : None

Load-Balance policy : Auto-select

: Disable

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.

Syntax

ipf flowtrack set [-re]

ipf flowtrack view [-f]

ipf flowtrack [-i][-p][-t]

Parameter	Description
-r	It means to refresh the flowtrack.
-е	It means to enable or disable the flowtrack. 0: Disable 1: Enable
-f	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.
-b	It means to show all of IP sessions state.
- i [IP address]	It means to specify IP address (e.g., -i 192.168.2.55).
-p[value]	It means to type a port number (e.g., -p 1024). Available settings are 0 ~ 65535.
-t [value]	It means to specify a protocol (e.g., -t tcp). Available settings include: tcp udp icmp

```
>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
            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:
                                               53 ,ifno=0
              8.8.8.8: 53 ->
REPLY >>
                                192.168.1.11:15073 ,ifno=3
     proto=17, age=93025100(2000), flag=203
ORIGIN>> 192.168.1.11: 7247 ->
                                     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
```

Telnet Command: Log

This command allows users to view log for WAN interface such as call log, IP filter log, flush log buffer, etc.

Syntax

log [-cfhiptwx?] [-F a | c | f | w]

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.
- <i>р</i>	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.

```
> log -w
25:36:25.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
      Client IP
                  = 0.0.0.0
                   = 0.0.0.0
      Your IP
      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: mngt ftpport

This command allows users to set FTP port for management.

Syntax

mngt ftpport [FTP port]

Syntax Description

Parameter	Description
FTP port	It means to type 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.

Syntax

mngt httpport [Http port]

Syntax Description

Parameter	Description
Http port	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.

Syntax

mngt httpsport [Https port]

Syntax Description

Parameter	Description
Https port	It means to type 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.

Syntax

mngt telnetport [Telnet port]

Syntax Description

Parameter	Description
Telnet port	It means to type 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.

Syntax

mngt sshport [ssh port]

Syntax Description

Parameter	Description
ssh port	It means to type the number for SSH port. The default setting is 22.

Example

```
> mngt sshport 23
% Set ssh port to 23 done.
```

Telnet Command: mngt ftpserver

This command can enable/disable FTP server.

Syntax

mngt ftpserver [enable] mngt ftpserver [disable]

Syntax Description

Parameter	Description
enable	It means to activate FTP server function.
disable	It means to inactivate FTP server function.

Example

```
> mngt ftpserver enable
%% FTP server has been enabled.

> mngt ftpserver disable
%% FTP server has been disabled.
```

Telnet Command: mngt noping

This command is used to pass or block Ping from LAN PC to the internet.

Syntax

mngt noping [on]
mngt noping [off]
mngt noping [viewlog]
mngt noping [clearlog]

Syntax Description

Parameter	Description
on	All PING packets will be forwarded from LAN PC to Internet.
off	All PING packets will be blocked from LAN PC to Internet.
viewlog	It means to display a log of ping action, including source MAC and source IP.
clearlog	It means to clear the log of ping action.

> mngt noping off
No Ping Packet Out is OFF!!

Telnet Command: mngt defenseworm

This command can block specified port for passing through the router.

Syntax

mngt defenseworm [on]
mngt defenseworm [off]
mngt defenseworm [add port]
mngt defenseworm [del port]
mngt defenseworm [viewlog]
mngt defenseworm [clearlog]

Syntax Description

Parameter	Description
on	It means to activate the function of defense worm packet out.
off	It means to inactivate the function of defense worm packet out.
add port	It means to add a new TCP port for block.
del port	It means to delete a TCP port for block.
viewlog	It means to display a log of defense worm packet, including source MAC and source IP.
clearlog	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.

Syntax

mngt rmtcfg [status]
mngt rmtcfg [enable]
mngt rmtcfg [disable]
mngt rmtcfg [http/https/ftp/telnet/ssh/tr069] [on/off]

Parameter	Description
status	It means to display current setting for your reference.
enable	It means to allow the system administrators to login from the Internet.
disable	It means to deny the system administrators to login from the

	Internet.
http/https/ftp/telnet/ssh/t r069	It means to specify one of the servers/protocols for enabling or disabling.
on/off	on - enable the function. off - disable the function.

```
> 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.

Syntax

```
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
-e[0/1]	It means to enable/disable the function.
	0-disable the function.
	1-enable the function.
-s[value]	It means to specify service offered.
	Available values include:
	FTP, HTTP, HTTPS, TELNET, SSH, None, All
-i[value]	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.
-f	It means to flush all of the settings.
-d	It means to restore the factory default settings.
-V	It means to view current settings.
-h	It means to get the usage of such command.

```
> 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.

Syntax

mngt echoicmp [enable]
mngt echoicmp [disable]

Syntax Description

Parameter	Description
enable	It means to accept the echo ICMP packet.
disable	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.

Syntax

```
mngt accesslist list
mngt accesslist add [index][ip addr][mask]
mngt accesslist remove [index]
mngt accesslist flush
```

Syntax Description

Parameter	Description
list	It can display current setting for your reference.
add	It means adding a new entry.
index	It means to specify the number of the entry.
ip addr	It means to specify an IP address.
mask	It means to specify the subnet mask for the IP address.
remove	It means to delete the selected item.
flush	It means to remove all the settings in the access list.

Example

Telnet Command: mngt snmp

This command allows you to configure SNMP for management.

Syntax

mngt snmp [-<command> <parameter> / ...]

Syntax Description

Parameter	Description
[<command/> <parameter>]</parameter>	The available commands with parameters are listed below. [] means that you can type in several commands in one line.
-e <1/2>	 Enable the SNMP function. Disable the SNMP function.
-g <community name=""></community>	It means to set the name for getting community by typing a proper character. (max. 23 characters)
-s <community name=""></community>	It means to set community by typing a proper name. (max. 23 characters)
-m <ip address=""></ip>	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=""></community>	It means to set trap community by typing a proper name. (max. 23 characters)
-n <ip address=""></ip>	It means to set the IPv4 address of the host that will receive the trap community.
-T <seconds></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.

Syntax

msubnet switch [2/3/4/5/6][On/Off]

Syntax Description

Parameter	Description
2/3/4/5/6	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6
On/Off	On means turning on the subnet for the specified LAN interface. Off means turning off the subnet.

Example

```
> msubnet switch 2 On % LAN2 Subnet On!

This setting will take effect after rebooting.

Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet addr

This command is used to configure IP address for the specified LAN interface.

Syntax

msubnet addr [2/3/4/5/6][IP address]

Parameter	Description
2/3/4/5/6	It means LAN interface.
	2=LAN2
	3=LAN3
	4=LAN4
	5=LAN5
	6=LAN6

```
> msubnet 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: msubnet nmask

This command is used to configure net mask address for the specified LAN interface.

Syntax

msubnet nmask [2/3/4/5/6][IP address]

Syntax Description

Parameter	Description
2/3/4/5/6	It means LAN interface.
	2=LAN2
	3=LAN3
	4=LAN4
	5=LAN5
	6=LAN6
IP address	Type 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.

Syntax

msubnet status [2/3/4/5/6]

Syntax Description

Parameter	Description
2/3/4/5/6	It means LAN interface.
	2=LAN2
	3=LAN3
	4=LAN4
	5=LAN5
	6=LAN6

```
> 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.

Syntax

msubnet dhcps [2/3/4/5/6][On/Off]

Syntax Description

Parameter	Description
2/3/4/5/6	It means LAN interface.
	2=LAN2
	3=LAN3
	4=LAN4
	5=LAN5
	6=LAN6
On/Off	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.

Syntax

msubnet nat [2/3/4/5/6] [On/Off]

Syntax Description

means LAN interface.
means LAN interrace.
-LAN2
-LAN3
-LAN4
-LAN5
LAN6
n - It means the subnet will be configured for NAT usage. Ff - It means the subnet will be configured for Routing usage.
= =

```
>> msubnet 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: msubnet gateway

This command is used to configure an IP address as the gateway used for subnet.

Syntax

msubnet gateway [2/3/4] [Gateway IP]

Syntax Description

Parameter	Description
2/3/4/5/6	It means LAN interface.
	2=LAN2
	3=LAN3
	4=LAN4
	5=LAN5
	6=LAN6
Gateway IP	Specify an IP address as the gateway IP.

Example

```
> msubnet 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: msubnet ipcnt

This command is used to defined the total number allowed for each LAN interface.

Syntax

msubnet ipcnt [2/3/4] [IP counts]

Syntax Description

Parameter	Description
2/3/4/5/6	It means LAN interface.
	2=LAN2
	3=LAN3
	4=LAN4
	5=LAN5
	6=LAN6
IP counts	Specify a total number of IP address allowed for each LAN interface. The available range is from 0 to 220.

```
> 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.

Syntax

msubnet talk [1/2/3/4/5/6] [1/2/3/4/5/6] [On/Off]

Syntax Description

Parameter	Description
1/2/3/4/5/6	It means LAN interface.
	1=LAN1
	2=LAN2
	3=LAN3
	4=LAN4
	5=LAN5
	6=LAN6
On/Off	On - It means
	Off - It means

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 <1/2/3/4/5/6> <1/2/3/4/5/6> <0n/Off>
% where 1:LAN1, 2:LAN2, 3:LAN3, 4:LAN4, 5:LAN5, 6:LAN6
% Now:
            LAN1 LAN2 LAN3
                              LAN4 LAN5 LAN6
% LAN1
% LAN2
                   V
% LAN3
                         V
% LAN4
                               V
% LAN5
                                     V
% LAN6
                                           V
```

Telnet Command: msubnet startip

This command is used to configure a starting IP address for DCHP.

Syntax

msubnet startip [2/3/4/5/6] [Gateway IP]

Parameter	Description

2/3/4/5/6	It means LAN interface.
	2=LAN2
	3=LAN3
	4=LAN4
	5=LAN5
	6=LAN6
Gateway IP	Type an IP address as the starting IP address for a subnet.

```
> 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 <2/3/4/5/6> <Gateway IP>
% Now: LAN2 192.168.2.90; LAN3 192.168.3.10; LAN4 192.168.4.10; LAN5 192.168.5.1
0; LAN6 192.168.6.10
```

Telnet Command: msubnet pppip

This command is used to configure a starting IP address for PPP connection.

Syntax

msubnet pppip [2/3/4/5/6] [Start IP]

Syntax Description

Parameter	Description
2/3/4/5/6	It means LAN interface.
	2=LAN2
	3=LAN3
	4=LAN4
	5=LAN5
	6=LAN6
Start IP	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 <2/3/4/5/6> <Start IP>
% Now: LAN2 192.168.2.250; LAN3 192.168.3.200; LAN4 192.168.4.200; LAN5 192.168.5.200; LAN6 192.168.6.200
```

Telnet Command: msubnet nodetype

This command is used to specify the type for node which is required by DHCP option.

Syntax

msubnet nodetype [2/3/4/5/6][count]

Syntax Description

Parameter	Description
2/3/4/5/6	It means LAN interface.
	2=LAN2
	3=LAN3
	4=LAN4
	5=LAN5
	6=LAN6
count	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 <2/3/4/5/6> <count>
% Now: LAN2 0; LAN3 0; LAN4 0; LAN5 0; LAN6 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 ?
% msubnet nodetype <2/3/4/5/6> <count>
% Now: LAN2 1; LAN3 0; LAN4 0; LAN5 0; LAN6 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.

Syntax

msubnet primWINS [2/3/4/5/6] [WINS IP]

Parameter	Description
2/3/4/5/6	It means LAN interface.
	2=LAN2
	3=LAN3
	4=LAN4

	5=LAN5
	6=LAN6
WINS IP	Type the IP address as the WINS IP.

```
>> msubnet primWINS ?
% msubnet primWINS <2/3/4/5/6> <WINS IP>
% Now: LAN2 0.0.0.0; LAN3 0.0.0.0; LAN4 0.0.0.0; LAN5 0.0.0.0; LAN6 0.0.0.0

> msubnet primWINS 2 192.168.3.5
% Set LAN2 Dhcp Primary WINS IP done !!!

> msubnet primWINS ?
% msubnet primWINS <2/3/4/5/6> <WINS IP>
% Now: LAN2 192.168.3.5; LAN3 0.0.0.0; LAN4 0.0.0.0; LAN5 0.0.0.0; LAN6 0.0.0.0
```

Telnet Command: msubnet secWINS

This command is used to configure secondary WINS server.

Syntax

msubnet secWINS [2/3/4/5/6] [WINS IP]

Syntax Description

Parameter	Description
2/3/4/5/6	It means LAN interface.
	2=LAN2
	3=LAN3
	4=LAN4
	5=LAN5
	6=LAN6
WINS IP	Type the IP address as the WINS IP.

```
>> msubnet secWINS 2 192.168.3.89
% Set LAN2 Dhcp Secondary WINS IP done !!!

> msubnet secWINS ?
% msubnet secWINS <2/3/4/5/6> <WINS IP>
% Now: LAN2 192.168.3.89; LAN3 0.0.0.0; LAN4 0.0.0.0; LAN5 0.0.0.0; LAN6 0.0.0.0
```

Telnet Command: msubnet tftp

This command is used to set TFTP server for multi-subnet.

Syntax

msubnet tftp [2/3/4/5/6] [TFTP server name]

Syntax Description

Parameter	Description
2/3/4/5/6	It means LAN interface.
	2=LAN2
	3=LAN3
	4=LAN4
	5=LAN5
	6=LAN6
TFTP server name	Type a name to indicate the TFTP server.

Example

```
> msubnet tftp ?
% msubnet tftp <2/3/4/5/6> <TFTP server name>
% Now: LAN2
     LAN3
     LAN4
     LAN5
     LAN6
> msubnet tftp 2 publish
% Set LAN2 TFTP Server Name done !!!
> msubnet tftp ?
% msubnet tftp <2/3/4/5/6> <TFTP server name>
% Now: LAN2 publish
     LAN3
     LAN4
     LAN5
     LAN6
```

Telnet Command: msubnet mtu

This command allows you to configure MTU value for LAN/DMZ/IP Routed Subnet.

Syntax

msubnet mtu [interface][value]

Syntax Description

Parameter	Description
interface	Available settings include LAN1~LAN6, IP_Routed_Subnet, and DMZ.
value	1000 ~ 1508 (Bytes), default: 1500 (Bytes)

```
> msubnet mtu LAN1 1492
> msubnet mtu ?
Usage:
 >msubnet mtu <interface> <value>
 <interface>: LAN1~LAN6,IP_Routed_Subnet,DMZ
 <value>: 1000 ~ 1508 (Bytes), default: 1500 (Bytes)
 e.x: >msubnet mtu LAN1 1492
Current Settings:
  LAN1 MTU:
                   1492 (Bytes)
  LAN2 MTU:
                   1500 (Bytes)
                   1500 (Bytes)
  LAN3 MTU:
  LAN4 MTU:
                   1500 (Bytes)
                  1500 (Bytes)
  LAN5 MTU:
                   1500 (Bytes)
  LAN6 MTU:
  DMZ MTU:
                   1500 (Bytes)
  IP Routed Subnet MTU: 1500 (Bytes)
```

Telnet Command: object ip obj

This command is used to create an IP object profile.

Syntax

```
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]
```

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX	It means the index number of the specified object profile.
-V	It means to view the information of the specified object profile. Example: object ip obj 1 -v
-n NAME	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: object ip obj 9 -n bruce
-i INTERFACE	It means to define an interface for the IP object. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=3, means WAN Example: object ip obj 8 -i 0

-s INVERT	It means to set invert seletion for the object profile. INVERT=0, means disableing the function. INVERT=1, means enabling the function. Example: object ip obj 3 -s 1
-a TYPE	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: object ip obj 3 -a 2
[START_IP]	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.

```
> 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.

Syntax

```
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
```

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX	It means the index number of the specified group profile.
- <i>V</i>	It means to view the information of the specified group profile. Example: $object\ ip\ grp\ 1\ -v$
-n NAME	It means to define a name for the IP group. NAME: Type a name with less than 15 characters. Example: object ip grp 8 -n bruce
-i INTERFACE	It means to define an interface for the IP group.

	INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=2, means WAN
	Example: object ip grp 3 -i 0
-a IP_OBJ_INDEX	It means to specify IP object profiles for the group profile.
	Example: :object ip grp 3 -a 1 2 3 4 5
	The IP object profiles with index number 1,2,3,4 and 5 will be group under such profile.

```
> 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 comman is used to create an IP object profile.

Syntax

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
setdefault	It means to return to default settings for all profiles.
INDEX	It means the index number of the specified object profile.
-V	It means to view the information of the specified object profile. Example: $object\ ip\ obj\ 1\ -v$
-n NAME	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: object ip obj 9 -n bruce
-i INTERFACE	It means to define an interface for the IP object. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=3, means WAN Example: object ip obj 8 -i 0
-s INVERT	It means to set invert seletion for the object profile. INVERT=0, means disableing the function. INVERT=1, means enabling the function. Example: object ip obj 3 -s 1
-a TYPE	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: object ip obj 3 -a 2
[START_IP]	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.

```
> 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.

Syntax

```
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
setdefault	It means to return to default settings for all profiles.
INDEX	It means the index number of the specified group profile.
-V	It means to view the information of the specified group profile. Example: $object\ ip\ grp\ 1\ -v$
-n NAME	It means to define a name for the IP group. NAME: Type a name with less than 15 characters. Example: object ip grp 8 -n bruce
-i INTERFACE	It means to define an interface for the IP group. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=2, means WAN Example: object ip grp 3 -i 0
-a IP_OBJ_INDEX	It means to specify IP object profiles for the group profile. Example: :object ip grp 3 -a 1 2 3 4 5 The IP object profiles with index number 1,2,3,4 and 5 will be group under such profile.

```
> 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]
```

```
[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.

Syntax

```
object service obj setdefault
object service obj /NDEX -v
object service obj /NDEX -n NAME
object service obj /NDEX -p PROTOCOL
object service obj /NDEX -s CHK [START_P] [END_P]
object service obj /NDEX -d CHK [START_P] [END_P]
```

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX	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: object service obj 1 -v
-n NAME	It means to define a name for the IP object.
	NAME: Type a name with less than 15 characters.
	Example: object service obj 9 -n bruce
-i PROTOCOL	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: object service obj 8 -i 0
СНК	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.
-s CHK [START_P] [END_P]	It means to set souce port check and configure port range (1~65565) for TCP/UDP.
	END_P, type a port number to indicate source port.
	Example: object service obj 3 -s 0 100 200
-d CHK [START_P] [END_P]	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: object service obj 3 -d 1 100 200

```
> 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:[!=]
```

Telnet Command: object service grp

This command is used to integrate several service objects under a service group profile.

Syntax

object service grp setdefault object service grp INDEX -v object service grp INDEX -n NAME object service grp INDEX -a SER_OBJ_INDEX

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX	It means the index number of the specified group profile.
-V	It means to view the information of the specified group profile. Example: object service grp 1 -v
-n NAME	It means to define a name for the service group.

	NAME: Type a name with less than 15 characters. Example: object service grp 8 -n bruce
-a SER_OBJ_INDEX	It means to specify service object profiles for the group profile.
	Example: :object service grp 3 -a 1 2 3 4 5
	The service object profiles with index number 1,2,3,4 and 5 will be group under such profile.

```
>object service grp 1 -n Grope_1
Service Group Profile 1
       :[Grope_1]
Name
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.

Syntax

```
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
```

Parameter	Description
setdefault	It means to return to default settings for all profiles.
show PAGE	It means to show the contents of the specified profile.

	PAGE: type the page number.
show	It means to show the contents for all of the profiles.
INDEX	It means the index number of the specified keyword profile.
-V	It means to view the information of the specified keyword profile.
-n NAME	It means to define a name for the keyword profile. NAME: Type a name with less than 15 characters.
-a CONTENTS	It means to set the contents for the keyword profile. Example: object kw obj 40 -a test

```
> 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.

Syntax

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*

Parameter	Description
show	It means to show the contents for all of the profiles.
setdefault	It means to return to default settings for all profiles.
INDEX	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.
-n NAME	It means to define a name for the file extension object profile. NAME: Type a name with less than 15 characters.
-е	It means to enable the specific CATEGORY or FILE_EXTENSION.

-d	It means to disable the specific CATEGORY or FILE_EXTENSION
CATEGORY FILE_EXTENSION	CATEGORY:
	Image, Video, Audio, Java, ActiveX, Compression, Executation
	Example: object fe obj 1 -e Image
	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

> object	fe obj 1	-n music	!				
> object	fe obj 1	-e Audio)				
> object	fe obj 1	-v					
Profile I	index: 1						
Profile N	Jame:[mus	ic]					
Image cate							
		[].gif					[].pct
[].pcx	[].pic	[].pict	[].png	[].tlI	[].tlii		
Video cate	egory:						
[].asf	[].avi	[].mov	[].mpe	[].mpeg	[].mpg	[v].mp4	[].qt
[].rm	[v].wmv	[].3gp	[].3gpp	[].3gpp2	2 [].3g2		
Audio cate	egory:						
		[v].au	[v].mp3	[v].m4a	[v].m4p	[v].ogg	[v].ra
		[v].wav					
Java categ							
		[].jar	[].jav	[].java	[].jcm	[].js	[].jse
[].jsp							
ActiveX ca	tegory:						
[].alx	[].apb	[].axs	[].ocx	[].olb	[].ole	[].tlb	[].viv
[].vrm							
Compression	n categor	v:					
[].ace	_	_	[].bz2	[].cab	[].qz	gizp.[]	[].rar
[].sit		<u>-</u> -			- 5	- 5 F	

Executation	n categor	cy:					
[].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, 5, 6, wan2, all] [AN, 100F, 100H, 10F, 10H, status]
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,sta tus]	
802.1x[enable,disable,status,addport,delport]	
wanfc	It means to set WAN flow control.

Example

```
> port 1 100F
%Set Port 1 Force speed 100 Full duplex OK !!!
```

Telnet Command: portmaptime

This command allows you to set a time of keeping the session connection for specified protocol.

Syntax

portmaptime [-<command> <parameter> | ...]

Parameter	Description
[<command/> <parameter>]</parameter>	The available commands with parameters are listed below. [] means that you can type in several commands in one line.
-t <sec></sec>	It means "TCP" protocol. <sec>: Type a number to set the TCP session timeout.</sec>

-U <sec></sec>	It means "UDP" protocol. <sec>: Type a number to set the UDP session timeout.</sec>
-i <sec></sec>	It means "IGMP" protocol. <sec>: Type a number to set the IGMP session timeout.</sec>
-W <sec></sec>	It means "TCP WWW" protocol. <sec>: Type a number to set the TCP WWW session timeout.</sec>
-s <sec></sec>	It means "TCP SYN" protocol. <sec>: Type a number to set the TCP SYN session timeout.</sec>
-f	It means to flush all portmaps (useful for diagnostics).
-I <list></list>	List all settings.

```
> portmaptime -t 86400 -u 300 -i 10
> portmaptime -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: prn

This command allows you to view current status (interface and driver) of USB printer.

Syntax

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

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>]</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></mode>	It means to define which traffic the QoS control settings will apply to and eable 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></bandwidth>	It means to set inbound bandwidth in kbps (Ethernet WAN only) The available setting is from 1 to 100000.	
-o <bandwidth></bandwidth>	It means to set outbound bandwidth in kbps (Ethernet WAN only). The available setting is from 1 to 100000.	
-r <index:ratio></index:ratio>	It means to set ratio for class index, in %.	
-u <mode></mode>	It means to enable bandwidth control for UDP. 0: disable 1: enable Default is disable.	
-p <ratio></ratio>	It means to enable bandwidth limit ratio for UDP.	
-t <mode></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.	

```
> qos setup -m 3 -i 9500 -o 8500 -r 3:20 -u 1 -p 50 -t 1

WAN1 QOS mode is both
Wan 1 is XDSL model ,don,t need to set up
Wan 1 is XDSL model ,don,t need to set up
WAN1 class 3 ratio set to 20
WAN1 udp bandwidth control set to enable
WAN1 udp bandwidth limit ratio set to 50
WAN1 Outbound TCP ACK Prioritizel set to enable
QoS WAN1 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> / ...]

Parameter	Description
[<command/> <parameter>]</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></no>	Specify the inde number for the class. Available value for <no> contains 1, 2 and 3. The default setting is class 1.</no>
-n <name></name>	It means to type a name for the class.
-a	It means to add rule for specified class.
-e <no></no>	It means to edit specified rule. <no>: type the index number for the rule.</no>
-d <no></no>	It means to delete specified rule. <no>: type the index number for the rule.</no>
-m <mode></mode>	It means to enable or disable the specified rule. 0: disable, 1: enable
-l <addr></addr>	Set the local address. Addr1 - It means Single address. Please specify the IP address directly, for example, "-I 172.16.3.9". addr1:addr2 - It means Range address. Please specify the IP addresses, for example, "-I 172.16.3.9: 172.16.3.50."
	addr1:subnet - It means the subnet address with start IP address. Please type the subnet and the IP address, for example, "-I 172.16.3.9:255.255.0.0".0
	any - It means Any address. Simple type "-I" to specify any address for this command.
-r <addr></addr>	Set the remote address.
	addr1 - It means Single address. Please specify the IP address directly, for example, "-I 172.16.3.9".
	addr1:addr2 - It means Range address. Please specify the IP addresses, for example, "-I 172.16.3.9: 172.16.3.50."
	addr1:subnet - It means the subnet address with start IP address. Please type the subnet and the IP address, for example, "-I 172.16.3.9:255.255.0.0".0
	any - It means Any address. Simple type "-I" to specify any address for this command.
-p <dscp id=""></dscp>	Specify the ID.
-s <service type=""></service>	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

-S <d s=""></d>	Show the content for specified DSCP ID/Service type.		
-V <1/2/3>	Show the rule in the specified class.		
[]	It means that you can type in several commands in one line.		

```
> 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>].

Parameter	Description	
-a <name></name>	It means to add rule.	
-e <no></no>	It means to edit user defined service type. "no" means the index number. Available numbers are 1~40.	
-d <no></no>	It means to delete user defined service type. "no" means the index number. Available numbers are 1~40.	
-n <name></name>	It means the name of the service.	
-t <type></type>	It means protocol type. 6: tcp(default) 17: udp 0: tcp/udp <1~254>: other	
-p <port></port>	It means service port. The typing format must be [start:end] (ex., 510:330).	
-1	List user defined types. "no" means the index number. Available numbers are 1~40.	

```
> 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: quit

This command can exit the telnet command screen.

Telnet Command: show lan

This command displays current status of LAN IP address settings.

> show lan			
The LAN settings:			
ip	mask dhc	p star_ip	pool gateway
[V]LAN1 192.168.1.1 192.168.1.1	255.255.255.0	[V] 192.168.1.10	200
[X]LAN2 192.168.2.1 192.168.2.1	255.255.255.0	[V] 192.168.2.10	100
[X]LAN3 192.168.3.1 192.168.3.1	255.255.255.0	[V] 192.168.3.10	100
[X]LAN4 192.168.4.1 192.168.4.1	255.255.255.0	[V] 192.168.4.10	100
[X]LAN5 192.168.5.1 192.168.5.1	255.255.255.0	[V] 192.168.5.10	100
[X]LAN6 192.168.6.1 192.168.6.1	255.255.255.0	[V] 192.168.6.10	100
[X]Route 192.168.0.1	255.255.255.0	[V] 0.0.0.0	192.168.0.1

Telnet Command: show dmz

This command displays current status of DMZ host.

Example

Telnet Command: show dns

This command displays current status of DNS setting

Example

```
> show dns
% Domain name server settings:
% Primary DNS: [Not set]
% Secondary DNS: [Not set]
```

Telnet Command: show openport

This command displays current status of open port setting.

Example

Telnet Command: show nat

This command displays current status of NAT.

```
> show nat
Port Redirection Running Table:
Index Protocol Public Port Private IP
                                     Private Port
         0
                   0.0.0.0
                                           0
         0
                   0.0.0.0
                                           0
                   0.0.0.0
3
         0
                                           0
4
         0
                   0.0.0.0
                                           0
                   0.0.0.0
5
         0
                                           0
6
         0
                   0.0.0.0
                                           0
7
         0
                   0.0.0.0
                                           0
8
         0
                   0
                     0.0.0.0
                                           0
9
         0
                  0.0.0.0
                                           0
10
                   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
Mo	ORE ['q'	: Quit,	'Enter': New Lines,	'Space Bar': Next Page]

Telnet Command: show portmap

This command displays the table of NAT Active Sessions.

Example

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: 10000
% Maximum Session Usage: 49
% Current Session Usage: 0
% Current Session Used(include waiting for free): 0
% WAN1 Current Session Usage: 0
```

Telnet Command: show status

This command displays current status of LAN and WAN connections.

```
> show status
System Uptime:20:36:35
LAN Status
Primary DNS:8.8.8.8 Secondary DNS:8.8.4.4
IP Address:192.168.1.1
                       Tx Rate:12923 Rx Rate:8152
WAN 1 Status: Disconnected
                       Name:tcom
Enable:Yes
           Line:xDSL
Mode:Static IP Up Time:0:00:00 IP:172.16.3.221 GW
IP:172.16.3.2
TX Packets:0
           TX Rate:0 RX Packets:0 RX Rate:0
ADSL Information: ADSL Firmware Version:05-04-04-04-00-01
                 State:TRAINING TX Block:0 RX Block:0
Mode:
Corrected Blocks:0 Uncorrected Blocks:0
UP Speed:0 Down Speed:0 SNR Margin:0 Loop Att.:0
```

Telnet Command: show adsl

This command displays current status of ADSL.

Example

```
> Vigor> show adsl
 ----- ATU-R Info (hw: annex A, f/w: annex A) ------
 Running Mode : T1.413 State : TRAINING
DS Actual Rate : 0 bps US Actual Rate : 0
                      0 bps US Actual Rate : 0 bps
 DS Attainable Rate : 0 bps US Attainable Rate :
DS Path Mode : Fast US Path Mode :
                        0 bps US Attainable Rate :
                                                   0 bps
                                                  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
 ADSL Firmware Version : 05-04-04-04-00-01
 ----- ATU-C Info ------
 Far Current Attenuation : 0 dB Far SNR Margin : 0 dB
 DSLAM CHIPSET VENDOR : < ADI >
```

Telnet Command: show statistic

This command displays statistics for WAN interface.

Syntax

show statistic

show statistic reset [interface]

Syntax Description

Parameter	Description
reset	It means to reset the transmitted/received bytes to Zero.
interface	It means to specify WAN1 ~WAN5 (including multi-PVC) interface for displaying related statistics.

```
> 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

>
```

Telnet Command: srv dhcp badip

This command is reserved for future using.

Syntax

srv dhcp badip

Example

```
> srv dhcp badip
>
```

Telnet Command: srv dhcp public

This command allows users to configure DHCP server for second subnet.

Syntax

```
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]
srv dhcp public del [MAC Addr XX-XX-XX-XX-XX/AII/ALL]
```

Syntax Description

Parameter	Description
start	It means the starting point of the IP address pool for the DHCP server.
IP address	It means to specify an IP address as the starting point in the IP address pool.
cnt	It means the IP count number.
IP counts	It means to specify the number of IP addresses in the pool. The maximum is 10.
status	It means the execution result of this command.
add	It means creating a list of hosts to be assigned.
del	It means removing the selected MAC address.
MAC Addr	It means to specify MAC Address of the host.
all/ALL	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.

Syntax

srv dhcp dns1 [?]

srv dhcp dns1 [DNS IP address]

Syntax Description

Parameter	Description	
?	It means to display current IP address of DNS 1 for the DHCP server.	
DNS IP address	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.

Syntax

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.
DNS IP address	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).

```
> 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.

Syntax

srv dhcp frcdnsmanl [on]
srv dhcp frcdnsmanl [off]

Syntax Description

Parameter	Description	
?	It means to display the current status.	
on	It means to use manual setting for DNS setting.	
Off	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.

Syntax

srv dhcp gateway [?]
srv dhcp gateway [Gateway IP]

Syntax Description

Parameter	Description	
?	It means to display current gateway that you can use.	
Gateway IP	It means to specify a gateway address used for DHCP server.	

```
> 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.

Syntax

srv dhcp ipcnt [?]
srv dhcp ipcnt [IP counts]

Syntax Description

Parameter	Description
?	It means to display current used IP count number.
IP counts	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.

Syntax

srv dhcp relay servip [server ip]
srv dhcp relay subnet [index]

Syntax Description

Parameter	Description
server ip	It means the IP address that you want to used as DHCP server.
Index	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

Syntax

srv dhcp startip [?]
srv dhcp startip [IP address]

Syntax Description

Parameter	Description
?	It means to display current used start IP address.
IP address	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.

```
> 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.

Syntax

srv dhcp leasetime [?]
srv dhcp leasetime [Lease Time (sec)]

Syntax Description

Parameter	Description
?	It means to display current leasetime used for the DHCP server.
Lease Time (sec)	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.

Syntax

srv dhcp nodetype <count>

Syntax Description

Parameter	Description
count	It means to specify a type for node.
	1. B-node
	2. P-node
	4. M-node
	8. H-node

```
> 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.

Syntax

srv dhcp primWINS [WINS IP address] srv dhcp primWINS clear

Syntax Description

Parameter	Description
WINS IP address	It means the IP address of primary WINS server.
clear	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.

Syntax

srv dhcp secWINS [WINS IP address] srv dhcp secWINS clear

Syntax Description

Parameter	Description
WINS IP address	It means the IP address of secondary WINS server.
clear	It means to remove the IP address settings of second WINS server.

```
> 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.

Syntax

srv dhcp expRecycleIP <sec time>

Syntax Description

Parameter	Description
sec time	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.

Syntax

srv dhcp tftp <TFTP server name>

Syntax Description

Parameter	Description
TFTP server name	It means to type 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.

Syntax

```
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 unmber]
```

Parameter	Description
-h	It means to display usage of this command.
-1	It means to display all the user defined DHCP options.
-d[idx]	It means to delete the option number by specifying its index number.
-e [1 or 0]	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.
idx number	It means the index number of the option value.

```
> srv dhcp option -e 1 -c 18 -v /path
> srv dhcp option -l
% state idx interface opt type data
% enable 1 ALL LAN 18 ASCII /path
```

Telnet Command: srv nat dmz

This command allows users to set DMZ host. Before using this command, please set WAN IP Alias first.

Syntax

srv nat dmz n m [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
n	It means to map selected WAN IP to certain host.
	1: wan1
	2: wan2
m	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.
[<command/>	The available commands with parameters are listed below.
<pre><parameter>]</parameter></pre>	[] means that you can type in several commands in one line.
-е	It means to enable/disable such feature.
	1:enable
	0:disable
-i	It means to specify the private IP address of the DMZ host.
-r	It means to remove DMZ host setting.
-V	It means to display current status.

Example

Telnet Command: srv nat ipsecpass

This command allows users to enable or disable IPSec ESP tunnel passthrough and IKE source port (500) preservation.

Syntax

srv nat ipsecpass [options]

Parameter	Description
[options]	The available commands with parameters are listed below.
on	It means to enable IPSec ESP tunnel passthrough and IKE source port (500) preservation.
off	It means to disable IPSec ESP tunnel passthrough and IKE source port (500) preservation.

status	It means to display current status for checking.
--------	--

```
> 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.

Syntax

srv nat openport n m [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
n	It means the index number for the profiles. The range is from 1 to 20.
m	It means to specify the sub-item number for this profile. The range is from 1 to 10.
[<command/> <parameter>]</parameter>	The available commands with parameters are listed below. [] means that you can type in several commands in one line.
-a <enable></enable>	It means to enable or disable the open port rule profile. 0: disable 1:enable
-c <comment></comment>	It means to type the description (less than 23 characters) for the defined network service.
-i <local ip=""></local>	It means to set the IP address for local computer. Local ip: Type an IP address in this field.
-w <idx></idx>	It means to specify the public IP. 1: WAN1 Default, 2: WAN1 Alias 1, and so on.
-p <protocol></protocol>	Specify the transport layer protocol. Available values are TCP, UDP and ALL.
-s <start port=""></start>	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=""></end>	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></remove>	It means to delete the specified open port setting. remove: Type the index number of the profile.
-f <flush></flush>	It means to return to factory settings for all the open ports profiles.

```
> 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
******************
    TCP
             23
                       83
%% Status: Disable
%% Comment:
%% Private IP address: 0.0.0.0
Index Protocal Start Port End Port
******************
%% Status: Disable
%% Comment:
%% Private IP address: 0.0.0.0
Index Protocal Start Port End Port
******************
```

Telnet Command: srv nat portmap

This command allows users to set port redirection table for NAT server.

Syntax

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

Parameter	Description
Add[idx]	It means to add a new port redirection table with an index number. Available index number is from 1 to 10.
serv name	It means to type one name as service name.
proto	It means to specify TCP or UDP as the protocol.
pub port	It means to specify which port can be redirected to the specified Private IP and Port of the internal host.
pri ip	It means to specify the private IP address of the internal host providing the service.
pri port	It means to specify the private port number of the service offered by the internal host.
wan1/wan2	It means to specify WAN interface for the port redirection.
del [idx]	It means to remove the selected port redirection setting.
disable [idx]	It means to inactivate the selected port redirection setting.
enable [idx]	It means to activate the selected port redirection setting.
flush	It means to clear all the port mapping settings.

```
> 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 ifno
1
      game
                        6
                                   80
                                        192.168.1.11
                                                             100
-1
 2
                       0
                                   0
                                                          0
                                                                 -2
 3
                        0
                                    0
                                                          0
                                                                 -2
 4
                                    0
                                                          0
                                                                 -2
 5
                                    0
                                                          0
                                                                 -2
                        0
 6
                                    0
                                                          0
                                                                 -2
                        0
 7
                                    0
                                                          0
                                                                 -2
                        0
 8
                        0
                                   0
                                                          0
                                                                 -2
 9
                        0
                                   0
                                                          0
                                                                 -2
10
                        0
                                    0
                                                           0
                                                                 -2
                                                           0
                                                                 -2
11
                        0
                                    0
12
                        0
                                    0
                                                                 -2
13
                                                           0
                                                                 -2
14
                        0
                                    0
                                                           0
                                                                 -2
15
                        0
                                    0
                                                           0
                                                                 -2
16
                        0
                                    0
                                                           0
                                                                 -2
                                                           0
                                                                 -2
17
                        0
                                    0
18
                        0
                                    0
                                                           0
                                                                 -2
19
                                    0
                                                                 -2
20
                                    0
                                                                 -2
Protocol: 0 = Disable, 6 = TCP, 17 = UDP
```

Telnet Command: srv nat status

This command allows users to view NAT Port Redirection Running Table.

> srv nat status NAT Port Redirection Running Table:				
Index	Protocol	Public Po	rt 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
MOF	RE ['q':	: Quit,	'Enter': New Lin	es, '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 $\ensuremath{\mathsf{DMZ}}$ settings.

Example

> srv	nat sho	owall ?		
Index	Proto	WAN IP:Port	Private IP:Port	Act
*****	*****	*******	*******	*****

R01	TCP	0.0.0.0:80	192.168.1.11:100	Y
001	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	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]

Parameter	Description
switch idx_no	It means the index number of the switch profile.
option	The available commands with parameters are listed below. cmd acc

	traffic [on/off/status/tx/rx]
cmd	It means to send command to the client.
acc	It means to set the client authentication account and password.
traffic [on/off/status/tx/rx]	It means to turn on/off or display the data transmission from the client.

```
> switch -i 1 traffic on
External Device NO. 1 traffic statistic function is enable
```

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

Telnet Command: switch clear

This command is used to reset the switch table and reboot the router.

Syntax

switch clear [idx]

Parameter	Description
idx	It means the index number of each item shown on the table. The range is from 1 to 8.
-f	It means to clear all of the data.

```
> 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 and specify LDAP server. The server will authenticate the local user who wants to access into the web user interface of Vigor router.

Syntax

sys adminuser [option]
sys adminuser edit [index] username password

Syntax Description

Parameter	Description
option	Available options includes: Local [0-1] LDAP [0-1] edit [INDEX] delete [INDEX] view [INDEX]
Local [0-1]	0 - Disable the local user. 1 - Enable the local user.
LDAP [0-1]	0 - Disable the LDAP. 1 - Enable the LDAP.
edit [INDEX] username password	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.
delete [INDEX]	Delete a local user account.
view [INDEX]	Show the user account/password detail information.

```
> > sys adminuser Local 1
```

```
Local User has enabled!
> sys adminuser LDAP 1
LDAP 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.

Syntax

sys bonjour [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
-e <enable></enable>	It is used to disable/enable bonjour service (0: disable, 1: enable).
-h <enable></enable>	It is used to disable/enable http (web) service (0: disable, 1: enable).
-t <enable></enable>	It is used to disable/enable telnet service (0: disable, 1: enable).
-f <enable></enable>	It is used to disable/enable FTP service (0: disable, 1: enable).
-s <enable></enable>	It is used to disable/enable SSH service (0: disable, 1: enable).
-p <enable></enable>	It is used to disable/enable printer service (0: disable, 1: enable).
-6 <enable></enable>	It is used to disable/enable IPv6 (0: disable, 1: enable).

```
> 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.

Syntax

sys cfg default sys cfg status

Syntax Description

Parameter	Description
default	It means to reset current settings with default values.
status	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.

Syntax

sys ftpd *on* sys ftpd *off*

Syntax Description

Parameter	Description
on	It means to turn on the FTP server of the system.
off	It means to turn off the FTP server of the system.

```
> 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.

Syntax

sys domainname [wan1/wan2] [Domain Name Suffix] sys domainname [wan1/wan2] clear

Syntax Description

Parameter	Description
wan1/wan2	It means to specify WAN interface for assigning a name for it.
Domain Name Suffix	It means the name for the domain of the system. The maximum number of characters that you can set is 40.
clear	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.

```
> sys iface
Interface 0 Ethernet:
Status: UP
IP Address: 192.168.1.1
                           Netmask: 0xFFFFFF00 (Private)
IP Address: 0.0.0.0
                            Netmask: 0xFFFFFFF
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: 0x0000000
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
```

>

Telnet Command: sys name

This command can set and remove the name for the router when DHCP mode is selected for WAN.

Syntax

sys name [wan1] [ASCII string]
sys name [wan1] clear

Syntax Description

Parameter	Description
wan1	It means to specify WAN interface for assigning a name for it.
ASCII string	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
ASCII string	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.

```
> sys reboot
>
```

Telnet Command: sys autoreboot

This command allows users to restart the router automatically within a certain time.

Syntax

sys autoreboot [on/off/hour(s)]

Syntax Description

Parameter	Description
on/off	On - It means to enable the function of auto-reboot.
	Off - It means to disable the function of auto-reboot.
hours	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: Vigor2860Vn+ 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 grybuf

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#:
Buf KMC1016 (1016B), used#: 7, cached#:
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.

Syntax

```
sys pollbuf [on]
sys pollbuf [off]
```

Parameter	Description
on	It means to turn on pulling buffer.

off	It means to turn off pulling buffer.

```
> 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.

Syntax

sys britask [on]
sys britask [off]

Syntax Description

Parameter	Description
on	It means to turn on the bridge task for improving the triple play quality.
off	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.

Syntax

```
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]
```

Parameter	Description
get [parm] [option]	It means to get parameters for tr-069.
	option= <nextlevel>: only gets nextlevel for GetParameterNames.</nextlevel>

	It	
set [parm] [value]	It means to set parameters for tr-069.	
getnoti [parm]	It means to get parameter notification value.	
setnoti [parm] [value]	It means to set parameter notification value.	
log	It means to display the TR-069 log.	
debug [on/off]	on: turn on the function of sending debug message to syslog. off: turn off the function of sending debug message to syslog.	
save	It means to save the parameters to the flash memory of the router.	
Inform [event code]	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"	
port [port num]	It means to change tr069 listen port number.	
cert_auth [on/off]	on: turn on certificate-based authentication. off: turn off certificate-based authentication.	

```
> 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.

Syntax

```
sys sip_alg [1]
sys sip_alg [0]
```

Syntax Description

Parameter	Description
1	It means to turn on SIP ALG.
0	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

Parameter	Description
licmsg	It means to display license message.
licauth	It means the license authentication time setting.
regser	It means the license register server setting.
licera	It means to erase license setting.
licifno	It means license and signature download interface setting.
lic_wiz [set/reg/qry]	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
dev_chg	It means to change the device key.
dev_key	It means to show device key.

> sys license licifno

License and Signature download interface setting:
licifno [AUTO/WAN#]

Ex: licifno wan1

Telnet Command: sys diag_log

This command is used for RD debug.

Download interface is "auto-selected" now.

Syntax

sys diag_log [status| enable| disable| flush| lineno [w] | level [x] | feature [on|off] [y]| log|

Syntax Description

Parameter	Description	
status	It means to show the status of diagnostic log.	
enable	It means to enable the function of diag_log.	
disable	It means to disenable the function of diag_log.	
flush	It means the flush log buffer.	
lineno [w]	It means the total lines for displaying message. w - Available value ranges from 100 to 50000.	
level[x]	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.	
feature [on/off][y]	It is used to specify the function of the log. Supported features include SYS and DSL (Case-Insensitive). Default setting is "on" for "DSL".	
voip_feature [on/off][vf_name]	It means VoIP feature. Type on to enable the feature or type off to disable the feature.	
	vf_name: available settings include DRVTAPI, DRVVMMC, DRVMPS, DRVFXO, DRVHAL, PSMPHONE, PSMSUPP, PSM, FXO, PSMISDN, DTMFPSER, CALLERID (Case-Insensitive).	
log	It means the dump log buffer.	

```
> 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)
          [DSL] Line state has changed: 00000000 -> 000000FF
0:00:02
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)
          [DSL] >> nXtseA=0d, nXtseB=00, nXtseV=07, nFwFeatures=5
0:00:05
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: 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.

```
>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<</pre>
InternalPort >>21<<, ExternalPort >>21<<</pre>
PortMapProtocol >>TCP<<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
Ftp Example [MICROSOFT]
((1))
InternalClient >>0.0.0.0<</pre>, RemoteHost >>0.0.0.0<</pre>
InternalPort >>0<<, ExternalPort >>0<<</pre>
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>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.

```
> upnp on
UPNP start.
> upnp service
>>>> SERVICE TABLE1 <
 serviceType urn:schemas-microsoft-com:service:OSInfo:1
 serviceId urn:microsoft-com:serviceId:OSInfol
 SCPDURL
            /upnp/OSInfo.xml
 controlURL /OSInfol
 eventURL
            /OSInfoEvent1
           uuid:774e9bbe-7386-4128-b627-001daa843464
 UDN
>>>> 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.

```
real_addr >>192.168.1.10<<, pseudo_addr >>172.16.3.229<</pre>
real_port >>0<<, pseudo_port >>0<</pre>
hit_portmap_index >>0<</pre>
The protocol >>TCP<</pre>
time >>0<</pre>
((1))
real_addr >>0.0.0.0<<, pseudo_addr >>0.0.0.0<</pre>
real_port >>0<<, pseudo_port >>0<</pre>
hit_portmap_index >>0<</pre>
The protocol >>0<</pre>
time >>0<</pre>
The protocol >>0<</pre>
The protocol >>0<</pre>
time >>0<</pre>
--- 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.

Syntax

upnp wan [n]

Syntax Description

Parameter	Description
n	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.

> usb list	t ?			
Brand	Module	Standard		
Aiko	Aiko 83D	3.5G	Y	
BandRich	Bandluxe C170	3.5G	Y	
BandRich	Bandluxe C270	3.5G	Y	
BandRich	Bandluxe C321	3.5G	Y	
BandRich	Bandluxe C330	3.5G	Y	
BandRich	Bandluxe C331	3.5G	Y	
BandRich	Bandluxe 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 Erics	s 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': 1	New Lines,	'Space Bar': Next Page] -

Telnet Command: vigbrg on

This command can make the router to be regarded as a modem but not a router.

Example

```
> vigbrg on
%Enable Vigor Bridge Function!
```

Telnet Command: vigbrg off

This command can disable vigor bridge function.

Example

```
> vigbrg off
%Disable Vigor Bridge Function!
```

Telnet Command: vigbrg status

This command can show whether the Vigor Bridge Function is enabled or disabled.

```
> vigbrg status
%Vigor Bridge Function is enable!
%Wanl 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.

Syntax

vigbrg cfgip [IP Address]

Syntax Description

Parameter	Description
IP Address	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 wan1on

This command is used to enable the bridge WAN1 management.

Example

```
> vigbrg wanlon
%Enable Vigor Bridge Wanl management!
```

Telnet Command: vigbrg wan1off

This command is used to disable the bridge WAN1 management.

Example

```
> vigbrg wanloff

%Disable Vigor Bridge Wanl management!
```

Telnet Command: vpn I2lset

This command allows users to set advanced parameters for LAN to LAN function.

Syntax

```
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]
```

Parameter	Description
list index	It means the index number of L2L (LAN to LAN) profile.
peerid	It means the peer identity for aggressive mode.
localid	It means the local identity for aggressive mode.
main	It means to choose proposal for main mode.
auto index	It means to choose default proposals.
proposal index	It means to choose specified proposal.
aggressive	It means the chosen DH group for aggressive mode
pfs	It means "perfect forward secrete".
on/off	It means to turn on or off the PFS function.
phase1	It means phase 1 of IKE.
lifetime	It means the lifetime value (in second) for phase 1 and phase 2.
phase2	It means phase 2 of IKE.

> VPN 121set 1 peerid 10226

Telnet Command: vpn I2IDrop

This command allows users to terminate current LAN to LAN VPN connection.

Example

> vpn 121Drop >

Telnet Command: vpn dinset

This command allows users to configure setting for remote dial-in VPN profile.

Syntax

vpn dinset t index>
vpn dinset t index> <on/off>
vpn dinset t index> motp <on/off>
vpn dinset t index> pin_secret <pin> <secret>

Parameter	Description
t index>	It means the index number of the profile.
<on off=""></on>	It means to enable or disable the profile. on - Enable. off - Disable.
motp <on off=""></on>	It means to enable or disable the authentication with mOTP function. on - Enable. off - Disable.
pin_secret <pin> <secret></secret></pin>	It means to set PIN code with secret.

<pre><pin> - Type the code for authentication (e.g, 1234).</pin></pre>
<secret> - Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6)</secret>

```
> 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.

Syntax

vpn subnet [index] [1/2/3/4/5/6]

Parameter	Description
<index></index>	It means the index number of the VPN profile.

.1 /2 /2 /4 /5 //.	1 it means LAN1
<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.

```
> vpn subnet 1 2
>
```

Telnet Command: vpn setup

This command allows users to setup VPN for different types.

Syntax

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>

Parameter	Description
For PPTP Dial-Out	
<index></index>	It means the index number of the profile.
<name></name>	It means the name of the profile.
<ip></ip>	It means the IP address to dial to.
<usr> <pwd></pwd></usr>	It means the user and the password required for the PPTP connection.
<nip> <nmask></nmask></nip>	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></index>	It means the index number of the profile.
<name></name>	It means the name of the profile.
<ip></ip>	It means the IP address to dial to.
<key></key>	It means the value of IPsec Pre-Shared Key.
<nip> <nmask></nmask></nip>	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></index>	It means the index number of the profile.
<name></name>	It means the name of the profile.
<ip></ip>	It means the IP address to dial to.
<usr> <pwd></pwd></usr>	It means the user and the password required for the L2TP connection.
<nip> <nmask></nmask></nip>	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></index>	It means the index number of the profile.
<name></name>	It means the name of the profile.
<ip></ip>	It means the IP address allowed to dial in.
<usr> <pwd></pwd></usr>	It means the user and the password required for the PPTP/L2TP connection.
<key></key>	It means the value of IPsec Pre-Shared Key.
<nip> <nmask></nmask></nip>	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

```
> 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.

Syntax

vpn option <index> <cmd1>=<param1> [<cmd2>=<para2> | ...]

Parameter	Description
<index></index>	It means the index number of the profile.

	Available index numbers:
	1 ~ 32
For Common Settings	
<index></index>	It means the index number of the profile.
pname	It means the name of the profile.
ena	It means to enable or disable the profile.
	on - Enable
	off - Disable
thr	It means the way that VPN connection passes through. Available
	settings are wlf, wlo, w2f, and w2o. w1f - WAN1 First.
	w1o - WAN1 Only.
	w2f - WAN2 First.
	w2o - WAN2 Only.
nnpkt	It means the NetBios Naming Packet.
	on - Enable the function to pass the packet.
	off - Disable the function to block the packet.
dir	It means the call direction. Available settings are b, o and i.
	b - Both
	o - Dial-Out i - Dial-In.
idla fualual	
idle=[value]	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.
palive	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	
ctype	It means "Type of Server I am calling".
	"ctype=t" means PPTP.
	"ctype=s" means IPSec.
	"ctype= I" means L2TP(IPSec Policy None). "ctype= I1" means L2TP(IPSec Policy Nice to Have).
	"ctype= 12" means L2TP(IPSec Policy Must).
dialto	It means Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89).
Itype	It means Link Type.
•	"Itype=0" means "Disable".
	"Itype=1" means "64kbps".
	"Itype=2" means "128kbps".
	"Itype=3" means "BOD".
oname	It means Dial-Out Username.
	"oname=admin" means to set Username = admin.
opwd	It means Dial-Out Password
	"opwd=1234" means to set Password = 1234.
pauth	It means PPP Authentication.

PPP Authentication = PAP&CHAP. PP Authentication = PAP Only hable/disable VJ Compression.
· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · · ·
ey.
t IKE Pre-Shared Key = abcd.
ethod.
eans ESP DES without/with
eans ESP 3DES without/with
ans ESP AES without/with Authentication.
hedule Setup.
1->3->5->7
to Callback.
enable/disable Set Require Remote to
ocal ID = vigor.
ype. Available settings include:
one).
ice to Have).
ust).
Server IP for Remote VPN Gateway.
ns to allow VPN dial-in with IP address of
note IP is allowed to dial in.
lemote VPN Gateway. e word is used as local ID.
est veername as "admin"
set username as "admin".
t managed on #1224#
t password as "1234".
able /disable VJ Compression.
ey. IKE Pre-Shared Key = abcd.
ethod
AH".
DES".
3DES".
AES.

	"mywip=1.2.3.4" means to set My WAN IP as "1.2.3.4".
rgip	It means Remote Gateway IP.
	"rgip=1.2.3.4" means to set Remote Gateway IP as "1.2.3.4".
rnip	It means Remote Network IP.
	"rnip=1.2.3.0" means to set Remote Network IP as "1.2.3.0".
rnmask	It means Remote Network Mask.
	"rnmask=255.255.255.0" means to set Remote Network Mask as "255.255.255.0".
rip	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".
mode	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.
droute	It means to Change default route to this VPN tunnel (Only single WAN supports this).
	droute=on/off means to enable/disable the function.

```
> 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.

Syntax

vpn mroute <index> list
vpn mroute <index> add <network ip>/<mask>
vpn mroute <index> del <network ip>/<mask>

Syntax Description

Parameter	Description
list	It means to display all of the route settings.
add	It means to add a new route.
del	It means to delete specified route.
<index></index>	It means the index number of the profile. Available index numbers: 1 ~ 32
<network ip="">/<mask></mask></network>	Type the IP address with the network mask address.

```
> 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.

Syntax

vpn list <index> all
vpn list <index>com
vpn list<index>out
vpn list <index> in
vpn list<index>net

Syntax Description

Parameter	Description
all	It means to list configuration of the specified profile.
com	It means to list common settings of the specified profile.
out	It means to list dial-out settings of the specified profile.
in	It means to list dial-in settings of the specified profile.
net	It means to list Network Settings of the specified profile.
<index></index>	It means the index number of the profile. Available index numbers: 1 ~ 32

```
> 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
                    : PPTP
% Type of Server
% 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
```

Telnet Command: vpn remote

This command allows users to enable or disable PPTP/IPSec/L2TP VPN service.

Syntax

vpn remote [PPTP/IPSec/L2TP] [on/off]

Syntax Description

Parameter	Description
PPTP/IPSec/L2TP	There are four types to be selected.
on/off	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.

Syntax

vpn 2ndsubnet *on* vpn 2ndsubnet *off*

Parameter	Description
on/off	It means to enable or disable second subnet.

```
> vpn 2ndsubnet on
%Enable second subnet IP as VPN server IP!
```

Telnet Command: vpn NetBios

This command allows users to enable or disable NetBios for Remote Access User Accounts or LAN-to-LAN Profile.

Syntax

vpn NetBios set <H2I/L2I> <index> <Block/Pass>

Syntax Description

Parameter	Description
<h2i l2i=""></h2i>	H2I means Remote Access User Accounts.
	L2I means LAN-to-LAN Profile.
	Specify which one will be applied by NetBios.
<index></index>	The index number of the profile.
<block pass=""></block>	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 H2l 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.

Syntax

vpn mss show

vpn mss default

vpn mss set <connection type> <TCP maximum segment size range>

Parameter	Description
show	It means to display current setting status.
default	TCP maximum segment size for all the VPN connection will be set as 1360 bytes.
set	Use it to specify the connection type and value of MSS.
<connection type=""></connection>	1~4 represent various type.

	1 - PPTP 2 - L2TP 3 - IPSec 4 - L2TP over IPSec
<tcp maximum="" range="" segment="" size=""></tcp>	Each type has different segment size range. PPTP - 1 ~ 1412 L2TP - 1 ~ 1408 IPSec - 1 ~ 1381 L2TP over IPSec - 1 ~ 1361

```
>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.

Syntax

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.

Syntax

vpn Multicast set <H2I/L2I> <index> <Block/Pass>

- ·	B
Parameter	Description
	2 3 3 3 1 5 1 5 1 5 1 5 1 5 1 5 1 5 1 5 1

<h2i l2i=""></h2i>	H2I means Host to LAN (Remote Access User Accounts). L2I means LAN-to-LAN Profile.
<index></index>	The index number of the profile.
<block pass=""></block>	Set Block/Pass the Multicast Packets. The default is Block.

```
> vpn Multicast set L2l 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.

Syntax

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.

Syntax

vpn pass2nat [on]
vpn pass2nat [off]

Syntax Description

Parameter	Description
on/off	on - the packets can pass through NAT.
	off - the packets cannot pass through NAT.

Telnet Command: wan ppp_mru

This command allows users to adjust the size of PPP LCP MRU. It is used for specific network.

Syntax

wan ppp_mru <WAN interface number> <MRU size >

Syntax Description

Parameter	Description
<wan interface="" number=""></wan>	Type a number to represent the physical interface. For Vigor130, the number is 1 (which means WAN1).
<mru size=""></mru>	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 for WAN1/WAN2.

Syntax

wan mtu [value]
wan mtu2 [value]

Syntax Description

Parameter	Description
value	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.

```
> 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)

Syntax

wan DF_check [on] wan DF_check [off]

Syntax Description

Parameter	Description
on/off	It means to enable or disable DF.

Example

```
> wan DF_check on

%DF bit check enable!

> wan DF_check off

%DF bit check disable (reset DF bit)!
```

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 disable 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.

Syntax

wan forward [on] wan forward [off]

Syntax Description

Parameter	Description
on/off	It means to enable or disable WAN forward.

```
> 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 modem / wan modem2

This command, wan modem, allows you to configure 3G/4G USB Modem (PPP mode) of WAN3.

The command, wan modem2, allows you to configure 3G/4G USB Modem (PPP mode) of WAN4.

Syntax

```
wan modem [init/init2/dial/pin][string]
wan modem paponly [on/off]
wan modem backup_wait [value]
wan modem pipe [Int][Din][Dout] (for USB WAN3 only)
wan modem wakeup [on/off/value] (for USB WAN3 only)
wan modem vid [id]
wan modem pid [id]
wan modem status
```

Parameter	Description
init	Set initial modem AT command (default value is "AT&FE0V1X1&D2&C1S0=0").
Init2	Set the second initial modem AT command.
dial	Set dial modem AT command (default value is "ATDT*99#").
pin	Set PIN code for SIM card. "0":disable
paponly	It means PAP Only. Set the PPP authentication of the USB WAN. on: None. off: PAP or CHAP.
backup_wait	Set waiting time after boot if USB WAN is in backup mode. This waiting time is reserved for the dial of main WANs so that the backup USB WAN will not go up first. Available setting is from 1 to 255. Unit is second.
pipe	It is for RD debug only. Please don't use it without our advice.
wakeup [on/off]	It is for RD debug only. Please don't use it without our advice.
vid	Set VID of VID/PID match to bind the USB modem to specify WAN interface. By default, this match is not set (0x0/0x0) and the router specifies WAN interface by USB port.
pid	Set PID of VID/PID match to bind the USB modem to specify WAN interface. By default, this match is not set (0x0/0x0) and the router specifies WAN interface by USB port.
status	Display current status of USB modem.

- > wan modem pin 0000
- > wan modem status

Modem Link Speed=0

Current Signal Strength=0

Last Fail Message:

Current Connect Stage:

Telnet Command: wan vdsl

This command allows you to configure display current VDSL status and configure the fallback mode for WAN connection.

Syntax

wan vdsl [show basic]
wan vdsl[fbk_mode]

Parameter	Description
show basic	It means to display current VDSL status.
fbk_mode	It means to display current status of Fallback Mode used. Available modes to be set as fallback mode include, Auto Vdsl_only

Adsl_only

Example

```
> wan vdsl show basic
ADSL
Link Status: TRAINING
Firmware Version: 05-04-04-04-00-01
ADSL Profile:
Basic Status Upstream
                                          Unit
                           Downstream
Actual Data Rate: 0
                           0
                              Kb/s
SNR:
                    0.1dB
> wan vdsl fbk mode vdsl only
Set VDSL fallback mode to VDSL ONLY
Reboot system to take effect
```

Telnet Command: wan Ite

This command allows you to configure LTE WAN (for L model only).

Syntax

```
wan Ite auth [0/1]
wan Ite band
wan Ite del [index #/all]
wan Ite pass [string]
wan Ite quota [-<command><parameter>|...|
wan Ite read [index #/all]
wan Ite reboot [-<command><parameter>|...|
wan Ite reply [-<command><parameter>|...|
wan Ite send [number][message]
wan Ite stus
wan Ite tag [index #/all]
wan Ite user [string]
wan Ite wms [send[cdma/gwpp]/recv[cdma/gwgw]/setting]
```

Parameter	Description
auth [0/1]	Set PPP authentication of LTE WAN.
	0: None.
	1: PAP or CHAP.
band	Display working band information for LTE network connection.
del [index #/all]	Delete an SMS from the LTE SIM card by specifying the index number. Use "all" to delete all.
pass	Set the password of LTE WAN.
quota	Set settings of SMS Quota Limit function.
[- <command/> <parameter>l</parameter>	Available commands with parameter are listed below:
<i>I</i>	[] means that you can type in several commands in one line.

	-a <0/1>: Set whether to send an e-mail alert when SMS quota exceeded. (0: no 1: yes)
	-c <cycle>: Set the order of today in refresh cycle.</cycle>
	-d <day>: Set the refresh day.</day>
	-e <0/1>: Enable or disable SMS Quota Limit function. (0: disable 1: enable)
	-h <hour>: Set the refresh hour.</hour>
	-m <0/1/2>: Set SMS quota refresh mode. (0: None 1: monthly 2: periodically)
	-n <number>: Set SMS quota. The avaible number is between 1 and 1000000.</number>
	-s <0/1>: Set whether to stop sending SMS after SMS quota exceeded. (0: no 1: yes)
read	Display information of an SMS in the LTE SIM card by specifying the index number. Use "all" to display all.
reboot	Set settings of Reboot on SMS Message function.
	<pre><command/> <parameter> </parameter></pre>
	The available commands with parameters are listed below.
	[] means that you can type in several commands in one line.
	-a <0/1>: Enable or disable Access Control List. (0: disable 1: enable)
	-e <0/1>: Enable or disable Reboot on SMS Message function. (0: disable 1: enable)
	-p <password>: Set the Password / PIN. This setting is necessary if this function is enabled.</password>
	-x <number>: Set the first phone number in Access Control List.</number>
	-y <number>: Set the second phone number in Access Control List.</number>
	-z <number>: Set the third phone number in Access Control List.</number>
reply	Set settings of Reply with Router Status Message function.
	<command/> <parameter> </parameter>
	The available commands with parameters are listed below.
	[] means that you can type in several commands in one line.
	-a <0/1>: Enable or disable Access Control List. (0: disable 1: enable)
	-c <0/1>: Set whether to reply with MAC address. (0: no 1: yes)
	-e <0/1>: Enable or disable Reboot on SMS Message function. (0: disable 1: enable)
	-f <0/1>: Set whether to reply with WAN1 IP address. (0: no 1: yes)
	-g <0/1>: Set whether to reply with WAN2 IP address. (0: no 1: yes)
	-h <0/1>: Set whether to reply with LTE WAN IP address. (0: no 1: yes)
	-i <0/1>: Set whether to reply with WAN4 IP address. (0: no 1: yes)
	-j <0/1>: Set whether to reply with WAN1 data usage. (0: no 1: yes)
	-k <0/1>: Set whether to reply with WAN2 data usage. (0: no 1: yes)
	-I <0/1>: Set whether to reply with LTE WAN data usage. (0: no 1: yes)
	-m <0/1>: Set whether to reply with WAN4 data usage. (0: no 1: yes)
	-n <0/1>: Set whether to reply with Router name. (0: no 1: yes)
	-p <password>: Set the Password / PIN. This setting is necessary if</password>
	 -p <password>: set the Password / Pin. This setting is necessary if this function is enabled.</password> -u <0/1>: Set whether to reply with Router system uptime. (0: no 1:
	this function is enabled.

	 -x <number>: Set the first phone number in Access Control List.</number> -y <number>: Set the second phone number in Access Control List.</number> -z <number>: Set the third phone number in Access Control List.</number>
send	Send an SMS message to the specified phone number through the LTE SIM card.
stus	Display status of LTE connection.
tag	Set an SMS in the LTE SIM card as read state by specifying the index number. Use "all" to set all SMS as read state.
user	Set the UserName of LTE WAN.
wms	This command is for RD debug only. We use it to test new USB modems. Please don't use it without our advice.

```
> wan lte band
Access technology : LTE
Access band information : E-UTRA Op Band 3
Interfere with 2.4G WLAN: NO
Active channel: 1725
>wan lte stus
Status: Operational. (Online)
Access Tech: LTE
Band: E-UTRA Op Band 3
ISP: Chunghwa
MCC: 466, MNC: 92, LAC: 65534, Cell ID: 81023501
Max Channel TX Rate: 50000000 bps
Max Channel RX Rate: 100000000 bps
IMEI: 356318040749422
IMSI: 466924200859808
RSSI: -61 dBm
Unread SMS: 4
SMSC address: +886932400821
SMS service status : Ready
Number of SMS sent : 0
```

Telnet Command: wan detect

This command allows you to configure WAN connection detection. When Ping Detection is enabled (for Static IP or DHCP or PPPoE mode), Router pings specified IP addresses to detect the WAN connection.

Syntax

```
wan detect [wan1/wan2/wan3/wan4][on/off/always_on]
wan detect [wan1/wan2/wan3/wan4] target [ip addr]
wan detect [wan1/wan2/wan3/wan4] target2[ip addr]
wan detect [wan1/wan2/wan3/wan4] target_gw [1/0]
wan detect [wan1/wan2/wan3/wan4] ttl [value]
wan detect [wan1/wan2/wan3/wan4] interval [interval]
wan detect [wan1/wan2/wan3/wan4] retry [retry]
wan detect status
```

Syntax Description

Parameter	Description
on	Enable ping detection. The IP address of the target shall be set.
off	Enable ARP detection (default).
always_on	Disable link detect, always connected(only support static IP)
target	Set the ping target.
Target2	Set the secondary ping target.
Target_gw	Set whether to use gateway as ping target. (1: yes 0: no) Note that USB WAN (PPP mode) cannot support PING gateway
ip addr	It means the IP address used for detection. Type an IP address in this field.
ttl	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.
interval [interval]	Set the interval between each ping operation. Available setting is between 1 and 3600. The unit is second. [interval]: Type a value.
retry [retry]	Set how many ping operations are retried before the Router judges that the WAN connection is disconnected. Available setting is between 1 and 255. The unit is times. [retry]: Type a number.
status	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.

Syntax

wan lb [wan1/wan2/...] on

wan lb [wan1/wan2/...] off wan lb status

Syntax Description

Parameter	Description
wan1/wan2	Specify which WAN will be applied with load balance.
on	Make WAN interface as the member of load balance.
off	Cancel WAN interface as the member of load balance.
status	Show the current status.

Example

```
> wan lb status
WAN1: on
WAN2: on
WAN3: on
WAN4: on
WAN5: 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.

Syntax

wan mvlan [pvc_no/status/save/enable/disable] [on/off/clear/tag tag_no] [service type/vlan priority] [px ...]

wan mvlan keeptag[pvc_no][on/off]

Parameter	Description
pvc_no	It means index number of PVC. There are 10 PVC, 0(Channel-1) to 9(Channel-9) allowed to be configured. However, bridge mode can be set on PVC number 2 to 9.
status	It means to display the whole Bridge status.
save	It means to save the configuration into flash of Vigor router.
enable/disable	It means to enable/disable the Multi-VLAN function.
on/off	It means to turn on/off bridge mode for the specific channel.
clear	It means to turn off/clear the port.
tag tag_no	It means to tag a number for the VLAN1: No need to add tag number. 1-4095: Available setting numbers used as tagged number.
service type	It means to specify the service type for VLAN. 0: Normal. 1: IGMP.
vlan priority	It means to specify the priority for the VALN setting.

	Range is from 0 to 7.
рх	It means LAN port. Available setting number is from 2 to 4. Port number 1 is locked for NAT usage.
keeptag	It means Multi-VLAN packets will keep their VLAN headers to LAN.

PVC 7 will map to LAN port 2/3/4 in bridge mode; service type is Normal. No tag added.

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.

Syntax

wan multifno [channel #] [WAN interface #]
wan multifno status

Syntax Description

Parameter	Description
channel #	There are 4 (?) channels including VLAN and PVC. Available settings are: 1=Channel 1 3=Channel 3 4=Channel 4
	5=Channel 5
WAN interface #	Type a number to indicate the WAN interface. 1=WAN1 2=WAN2
status	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 configure the VLAN tag of WAN1 or WAN2.

Syntax

wan vlan wan [#] tag [value] wan vlan wan [#] [enable/disable] wan vlan stat

Syntax Description

Parameter	Description
wan [#]	Specify which WAN interface will be tagged.
tag [value]	Type a number for tagging on WAN interface.
enable/disable	Enable: Specified WAN interface will be tagged. Disable: Disable the function of tagging on WAN interface.
stat	Display current VLAN status.

Example

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

Parameter	Description
wan[#]	Specify the WAN interface.
rdate	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 monthy 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
enable/disable	enable - Enable the function of wan budget.
	disable - Disable the function of wan budget.
thres [budget limit (MB)]	Specify the maximum value for WAN budget limit. (Unit: MB)
	budget limit - Type a number.
gthres [budget limit (GB)]	Specify the maximum value of wan budget limit. (Unit: GB) budget limit - Type a number.
mode [monthly/periodic/none]	Specify the calculation mode (monthly, periodically, or none) for WAN budget.
psday [th day in periodic]	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 \rightarrow It means "today" is the 5 th day in the billing cycle.
action [action bitmap]	Determine the action to be performed when it reaches the WAN budget limit.
	action bitmap - Type a total number of actions to be executed.
	Different numbers represent different actions. 1: shotdown 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 shotdown is detected.
status	Display current configuration status of WAN budget.

```
> 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
-w [number]	Specify the WAN interface. Value: Type the number of WAN interface. 1: WAN1; 2:WAN2and etc.
-I [Host/IP address]	Specify the IPv4 target to detect. If can be an IPv4 address or domain name. Host/IP address: Type the IP address/domain name of the target.
-s [base_size]	Set the MTU size base for Discovery. base_size: Available setting is 1000 ~ 1500.
-d [decrease size]	Set the MTU size to decrease between detections. decrease size: Available setting is 1 ~ 100.
-c [count]	Set the maximum times of ping failure during a Discovery. count: Available settings are 1 ~ 10. Default value is 3.

```
> 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
-w [number]	Specify the WAN interface number: Type the number of WAN interface. 1: WAN1; 2:WAN2and
	etc.
-I [IPv6 address]	Specify the IPv6 target to detect. It must be an IPv6 IP address.
	IPv6 address: Type the IPv6 address of the target.
-s [base_size]	Specify the size of MTU.
	base_size: Available setting is 1000 ~ 1500.

Example

```
> wan detect_mtu6 -w 2 -i 2404:6800:4008:c06::5e -s 1500 >
```

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

Parameter	Description
enable [ssid1 ssid2 ssid3 ssid4]	It means to enable the settings for SSID1, SSID2, SSID3 and SSID4.
disable [ssid1 ssid2 ssid3 ssid4]	It means to disable the settings for SSID1, SSID2, SSID3 and SSID4.
add [MAC] [ssid1 ssid2 ssid3 ssid4] [isolate]	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 or xx:xx:xx:xx:xx or xx.xx.xx.xx.xx.xx
del [MAC]	It means to delete a MAC address entry defined in the access control list.

mode [ssid1 ssid2 ssid3 ssid4] [white/black]	It means to set white/black list for each SSID.
wl acl show	It means to show access control status.
wl acl showmode	It means to show the mode for each SSID.
wl acl clean	It means to clean all access control setting.

```
> > 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
                  00:50:70:ff:12:70 ssid1 ssid2 ssid3 ssid4
  0
             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.

Syntax

```
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]
```

Parameter	Description
mode[value]	It means to select connection mode for wireless connection. Available settings are: "11bgn", "11gn", "11n", "11bg", "11g", or "11b".
mode show	It means to display what the current wireless mode is.

channel [number]	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.
preamble [enable]	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.
txburst [enable]	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.
ssid[ssid_num enable ssid_name [hidden_ssid]]	It means to set the name of the SSID, hide the SSID if required. ssid_num: Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. ssid_name: Give a name for the specified SSID. hidden_ssid: Type 0 to hide the SSID or 1 to display the SSID
Security [SSID_NUMBER] [mode][key][index]	It means to configure security settings for the wirelesss connection. SSID_NUMBER: Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. mode: 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: WPA2/PSK wpamixpsk: WEP key, index: Moreover, you have to add keys for wpapsk, wpa2psk, wpamixpsk and wep, 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.
ratectl [ssid_num enable upload download]	It means to set the rate control for the specified SSID. ssid_num: Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. enable: It means to enable the function of the rate control for the specified SSID. 0: disable and 1:enable. upload: It means to configure the rate control for data upload. The unit is kbps. download: It means to configure the rate control for data download. The unit is kbps.
isolate [ssid_num lan member]	It means to isolate the wireless connection for LAN and/or Member. Ian - It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other. member - 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
            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.

Syntax

wl set [SSID] [CHAN[En]] wl set txburst [enable]

Syntax Description

Parameter	Description
SSID	It means to type the SSID for the router. The maximum character that you can use is 32.
CHAN[En]	It means to specify required channel for the router. CHAN: The range for the number is between 1 ~ 13. En: type on to enable the function; type off to disable the function.
txburst [enable]	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.

```
> 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.

Syntax

wl act [En]

Syntax Description

Parameter	Description
En	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 scan

This command allows users to perform AP scanning.

Syntax

wl scan [start]

wl scan set [wlist/blist/stime][MAC]

wl scan del [wlist/blist] [MAC]

wl scan filter [ssid/channel/mac]

wl scan *show* [0/1/2/3]

Parameter	Description
start	It means to start AP scanning.
set [wlist/blist/stime] [MAC]	Set white list/block list/scan time. wlist - It means to set white list for passing. MAC address must be added in the end. e.g., wl scan set wlist 001122aabbcc blist - It means to set black list for blocking. MAC address must be added in the end. stime - It means to set scanning time. Time value (2~5 second) must be added in the end. e.g., wl scan set time 5
del	Remove white list/block list. e.g., wl scan del wlist 001122aabbcc
filter	Set which filter you want. ssid - scanning the AP based on SSID setting. channel - scanning the AP based on channel setting. mac - scanning the AP based on MAC address setting.
show [0/1/2/3]	It is used to show AP list. 0 - display white list

1 - display block list,
2 - display gray/unknown list,
3 - display all list

```
> wl scan set wlist 001122aabbcc
> wl scan start
> wl scan show 3
>
```

Telnet Command: wl stamgt

This command is used to configure connection time and reconnection time for each SSID that wireless client used for accessing into Internet.

Syntax

```
wl stamgt [enable/disable] [ssid_num].
wl stamgt [show] [ssid_num].
wl stamgt set [ssid_num] [c] [r]
wl stamgt reset [ssid_num].
```

Syntax Description

Parameter	Description
enable/disable	It means to enable/disable the station management control.
ssid_num	It means channel selection. Available channel for 2.4G: 0/1/2/3 Available channel for 5G: 4/5/6/7.
show	It means to display status or configuration of the selected channel.
С	It means connection time. The unit is minute.
r	It means reconnection time. The unit is minute.

Example

```
> wl stamgt enable 1
% Station Management Status: enabled
> wl stamgt set 1 60 60
> wl stamgt show 1
NO. SSID BSSID Connect time Reconnect time
1. Draytek 00:11:22:aa:bb:cc 0d:0:58:26 0d:0:0
```

Telnet Command: wl iso_vpn

This command allows users to activate the function of VPN isolation.

Syntax

wl iso_vpn [ssid] [En]

Parameter	Description

ssid	It means the number of SSID. 1: SSID1 2: SSID2 3: SSID3 4: SSID4
En	It means to enable or disable the function of VPN isolation. 0: disable 1: enable

```
> wl iso_vpn 1 on
% ssid: 1 isolate vpn on :1
```

Telnet Command: wl wpa

This command allows you to configure WPA wireless settings.

Syntax

wl wpa 1/2/3

Syntax Description

Parameter	Description
wl wpa	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).

Syntax

wl wmm ap *Queldx Aifsn Cwmin Cwmax Txop ACM*wl wmm bss *Queldx 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*

Syntax Description

wl wmm show

Parameter	Description
ар	It means to set WMM for access point.
bss	It means to set WMM for wireless clients.

ack	It means to map to the Ack policy settings of AP WMM.	
enable	It means to enable the WMM for each SSID. 0: disable 1: enable	
Apsd [value]	It means to enable / disable the ASPD(automatic power-save delivery) function. 0: disable 1: enable	
show	It displays current status of WMM.	
Queldx	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.	
Aifsn	It controls how long the client waits for each data transmission.	
Cwmin/ Cwmax	CWMin means contention Window-Min and CWMax means contention Window-Max. Specify the value ranging from 1 to 15.	
Тхор	It means transmission opportunity. Specify the value ranging from 0 to 65535.	
ACM	It can restrict stations from using specific category class if it is enabled. 0: disable 1: enable	

```
> 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.

Syntax

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
wl ht bw value	The value you can type is 0 (for BW_20) and 1 (for BW_40).
wl ht gi value	The value you can type is 0 (for GI_800) and 1 (for GI_4001)
wl ht badecline value	The value you can type is 0 (for disabling) and 1 (for enabling).
wl ht autoba value	The value you can type is 0 (for disabling) and 1 (for enabling).
wl ht rdg value	The value you can type is 0 (for disabling) and 1 (for enabling).
wl ht msdu value	The value you can type is 0 (for disabling) and 1 (for enabling).
wl ht txpower value	The value you can type ranges from 1 - 6 (level).
wl ht antenna value	The value you can type ranges from 0-3.
	0: 2T3R
	1: 2T2R
	2: 1T2R
	3: 1T1R
wl ht greenfield value	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 btnctl

This command allows you to enable or disable wireless button control.

Syntax

wl btnctl [value]

Parameter	Description
value	0: disable
	1: enable

```
> wl btnctl 1
Enable wireless botton control
Current wireless botton control is on
>
```

Telnet Command: wl iwpriv & wl wlanconfig

These two commands are reserved for RD debug. Do not use them.

Telnet Command: wl efuse

This command is used to configure parameters related to wireless RF hardware. At present, it is not allowed for end user to operate.

Telnet Command: wan vlan

This command allows you to tag packets on WAN VLAN with specified number.

Syntax

wan vlan wan [#] tag [value]
wan vlan wan [#] [enable|disable]
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.
stat	It means to display the table of WAN VLAN status.

Example

Telnet Command: wol

This command allows Administrator 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	
MAC Address	It means the MAC address of the host.	
IP address	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).	
on/off/any	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.	
[idx][ip address] [mask]	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. ip address - It means the WAN IP address. mask - 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

sser set [-e/-d/-c/-l/-o/-a/-r/-b]user edit $[PROFILE_IDX]$ [-e/-d/-n/-p/-t/-u/-i/-q/-r/-w/-s/-m/-x/-v]user account $[USER_NAME]$ [-t/-d/-q/-r/-w]

Parameter	Description	
set	It means to configure general setup for the user management.	
edit	It means to modify the selected user profile.	
account	It means to set time and data quota for specified user account.	
User Set		
-е	Enable User management function.	
-d	Disable User management function.	
-a[Profile idx][User name][IP_Address]	It means to pass an IP Address. Profile idx- type the index number of the selected profile. User name- type the user name that you want it to pass. IP_Address- type the IP address that you want it to pass.	
-l all -l userl	Show online user. all - all of the users will be displayed on the screen.	

-I ip	user name - type the user name that you want to view on the screen.		
	<i>ip</i> - type the IP address that you want to view on the screen.		
-0	It means to show user account information.		
	e.g.,-o		
-c[user name]	Clear the user record.		
-c all	user name - type the user name that you want to get clear		
	corresponding record. all - all of the records will be removed.		
-buser [user name]	Block specifies user or IP address.		
-b ip [ip address]	user name - type the user name that you want to block.		
	ip address type the IP address that you want to block.		
-u user [user name]	Unblock specifies user or IP address.		
-u ip [ip address]	user name - type the user name that you want to unblock.		
	ip address — type the IP address that you want to unblock.		
-r [user name all]	Remove the user record. user name - type the name of the user profile.		
	all - all of the user profile settings will be removed.		
-q	It means to trigger the alert tool to do authentication.		
-S	It means to set login service.		
3	0:HTTPS		
	1:HTTP		
	e.g.,-s 1		
User edit			
PROFILE_IDX	Type the index number of the profile that you want to edit.		
-е	Enable User profile function.		
-d	Disable User profile function.		
-n	It means to set a user name for a profile.		
	e.g.,-n fortest		
-р	It means to configure user password.		
	e.g., -p 60fortest		
<i>-t</i>	It means to enable /disable time quota limitation for user profile		
	0:Disable		
	1:Enable		
-U	It means to enable /disable data quota limitation for user profile 0:Disable		
	1:Enable		
-i	It means to set idle time.		
,	e.g., -i 60		
-q	set time quota		
,	It means to set time quota of the user profile.		
	e.g., <i>-q 200</i>		
-r	It means to set data quota.		
	e.g., <i>-r 1000</i>		
-W	It means to specify the data quota unit (MB/GB).		
	e.g., -w MB		
-S	It means to set schedule index. Available settings are"		
	sch_idx1,sch_idx2,sch_idx3, and sch_idx4.		

-m	It means to set the maximum login user number.		
	e.g., <i>-m 200</i>		
-X	It means to set external server authentication		
	0: None		
	1: LDAP		
	2: Radius		
	3: TACAS		
	e.g., -x 2		
-V	It means to view user profile(s).		
User account	User account		
USER_NAME	It means to type a name of the user account.		
-d	It means to enable /disable data quota limitation for user account.		
	0:Disable		
	1:Enable		
-q	It means to set account time quota.		
	e.g., <i>-q 200</i>		
-r	It means to set account data quota.		
	e.g., <i>-r 1000</i>		
-t	It means to enable /disable time quota limitation for user account.		
	0:Disable		
	1:Enable		
-W	It means to set data quota unit (MB/GB).		

```
> user account admin -d 1
Enable the [admin] data quota limited
```

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.

Syntax

nand bad

nand usage

Example

>nand usage					
Show NAND	Show NAND Flash Usage:				
Partition	n Total	Used	Available	Use%	
cfg	4194304	7920	4186384	0%	
bin_web	33554432	11869493	21684939	35%	
cfg-bak	4194304	7920	4186384	0%	
bin_web-b	oak 33554432	11869493	21684939	35%	
> nand ba	> nand bad				
Show NAND	Show NAND Flash Bad Blocks:				
Block A	ddress	Partition			
1020 03	x07f80000	unused			
1021 03	x07fa0000	unused			
1022 03	x07fc0000	unused			
1023 02	x07fe0000	unused			

Telnet Command: apm show /clear/discover/query

The apm command(s) is use to display, remove, discover or query the information of VigorAP registered to Vigor2860.

Syntax

apm show

apm clear

apm discover

apm query

Syntax Description

Parameter	Description
show	It displays current information of APM profile.
clear	It is used to remove all of the APM profile.
discover	It is used to search VigorAP on LAN.
query	It is used to query any VigorAP which has been registered to APM (Central AP Management) in Vigor2860. Information related to the registered AP will be send back to Vigor2860 for updating the web page of Central AP Management.

```
> apm clear ?
Clear all clients ... done
```

Telnet Command: apm profile

This command allows to configure wireless profiles to be used in Central AP Management.

Syntax

apm profile clone [from index][to index][[new name]
apm profile del [index]
apm profile reset
apm profile summary
apm profile [show [profile index]]
apm profile apply [profile index] [client index1 [index2 .. index5]]

Syntax Description

Parameter	Description
clone	It is used to copy the same parameters settings from one profile to another APM profile.
del	It is used to delete a specified APM profile. The default (index #1) should not be deleted.
reset	It is used to reset to factory settings for WLAN profile.
summary	It is used to list all of the APM profiles with required information.
show	It is used to display specified APM profile.
apply	It is used to apply the selected APM profile onto specified VigorAP.
from index	Type an index number in this field. It is the original APM profile to be cloned to other APM profile.
to index	Type an index number in this file. It is the target profile which will clone the parameters settings from an existed APM profile.
new name	Type a name for a new APM profile.
profile index	Type the index number of existed profile.
client index1/2/3/4/5	It is useful for applying the selected APM profile to the specified VigorAP.

> apm profile (Done)	clone 1 2 forcar	rie		
> apm profile	summary			
# Name	SSID	Security	ACL	RateCtrl(U/D)
0 Default	DrayTek-LAN-A	WPA+WPA2/F	SK x	- / -
	DrayTek-LAN-B	WPA+WPA2/E	PSK x	- / -
1 -	-	-	-	-
2 forcarrie	DrayTek	Disable	х	- / -
3 -	-	-	_	-
4 -	-	-	_	-

Telnet Command: apm cache

This command is used to display or remove the information of registered VigorAP, including MAC address, name, and authentication. Up to 30 entries of registered information can be stored and displayed.

Syntax

apm cache [show]
apm cache clear

Syntax Description

Parameter	Description
show	It means to display the information related to VigorAP registered Vigor2860.
clear	It means to remove the information related to VigorAP registered Vigor2860.

Example

> apm	cache show	
MAC	Name	Auth
>		

Telnet Command: apm lbcfg

This command allows to set parameters related to AP management control.

Syntax

apm lbcfg [set] [value]
apm lbcfg[show]

Parameter	Description
set	It means to set the load balance configuration file for APM.
Show	It shows the configuration value.
[value]	You need to type 10 numbers in this field. Each number represents different setting value.
	[1] - The first number means the load balance function. Type
	1 - enable load balance,
	0 - disable load balance.
	[2] - The second number means the station limit function. Type
	1 -enable station limit,
	0 - disable station limit.
	[3] - The third number means the traffic limit function. Type
	1 - enable traffic limit,
	0 - disable traffic limit.
	[4] - The forth number means the limit num of station. Available range is 3~64.
	[5] - The fifth number means the upload limit function. Type
	1 - enable upload limit,

```
0 - disable upload limit.
[6] - The sixth number means the download limit function.
     Type
1 - enable download limit,
0 - disable download limit.
[7] - The seventh number means disassociation by idle time.
1 - enable disassociation,
0 - disable disassociation.
[8] - The eighth number means to enable or disable disassociation
by signal strength. Type
1 - enable disassociation,
0 - disable disassociation.
[9] - The ninth number means to determine the unit of traffic
     limit (for upload)
      1 - Mbps
     0 - kbps
[10] - The tenth number means to determine the unit of traffic
limit (for download)
      1 - Mbps
     0 - kbps
```

```
> apm lbcfg show
apm LoadBalance Config:
1. Enable LoadBalance : 0
2. Enable station limit: 0
3. Enable traffic limit: 0
4. limit Number: 64
5. Upload limit: 0
6. Download limit: 0
7. Enable disassociation by idle time : 0
8. Enable disassociation by Signal strength : 0
9. Traffic limit unit (upload)
10. Traffic limit unit (download) : 0
flag: 0
> apm lbcfg set 1 1 0 15 0 0 0 0 1 1
> apm lbcfq show
apm LoadBalance Config:
1. Enable LoadBalance: 1
2. Enable station limit: 1
3. Enable traffic limit: 0
4. limit Number: 15
5. Upload limit: 0
6. Download limit: 0
7. Enable disassociation by idle time : 0
8. Enable disassociation by Signal strength: 0
9. Traffic limit unit (upload)
10.Traffic limit unit (download) : 1
flag : 49
```

Telnet Command: apm napdetect

This command is used to enable/disable AP detection function.

Syntax

apm napdetect [get]

apm napdetect [set] [enable/disable AP Detection 1/0][Refresh Time].

Syntax Description

Parameter	Description
get	It is used to get AP detection data from VigorAP (e.g., AP900).
set	It allows to set detect configuration to VigorAP.
enable/disable AP Detection 1/0	It is used to enable or disable the AP detection function. 0 - disable the function. 1 - enable the function.
Refresh Time	Available values are 1, 3 or 5 (minutes).

Example

Note: To check the scanning result of AP detection, use the command of "wl scan show".

```
> apm napdetect set 1 1
> wl scan show 3
Sta Ch SSID BSSID BssType Security Siganl(%) Beacon
Period First Detected Last Detected

11 DrayTek-LAN-B 02:1d:aa:4c:bd:a8 AP Mixed 26 100

11 DrayTek-LAN-A 00:1d:aa:4f:bd:a8 AP Mixed 42 100
Dec 09,10:35:44 Dec 09,10:35:44
```

Telnet Command: apm apsyslog

This command is used to display the AP syslog data coming form VigorAP.

Syntax

apm apsyslog [AP_Index]

Syntax Description

Parameter	Description
AP_Index	Specify the index number which represents VigorAP.

```
> apm apsyslog 1

8d 02:46:09 syslog: [APM] Send Rogue AP Detection data.

8d 02:53:04 syslog: [APM] Run AP Detection / Discovery.

8d 02:56:09 syslog: [APM] Send Rogue AP Detection data.

8d 03:00:42 kernel: 60:fa:cd:55:f5:ea had disassociated.

8d 03:03:12 syslog: [APM] Run AP Detection / Discovery.

8d 03:06:09 syslog: [APM] Send Rogue AP Detection data.

8d 03:13:21 syslog: [APM] Run AP Detection / Discovery.

8d 03:16:10 syslog: [APM] Send Rogue AP Detection data.

8d 03:16:41 kernel: 60:fa:cd:55:f5:ea had associated successfully
```

```
8d 03:16:55 kernel: 60:fa:cd:55:f5:ea had disassociated.
```

Telnet Command: apm syslog

This command is used to display related syslog data from central AP management.

Syntax

apm syslog

Example

```
> apm syslog

"2015-11-04 12:24:21", "[APM] [VigorAP900_01daa902080] Get Rogue AP Detection
Data from AP"

2015-11-04 12:24:56", "[APM] [VigorAP900_01daa902080] Get Rogue AP Detection
Data from AP Success"

2015-11-04 12:34:21", "[APM] [VigorAP900_01daa902080] Get Rogue AP Detection
Data from AP"

2015-11-04 12:34:57", "[APM] [VigorAP900_01daa902080] Get Rogue AP Detection
Data from AP Success"
```

Telnet Command: apm stanum

This command is used to display the total number of the wireless clients, no matter what mode of wireless connection (2.4G WLAN or 5G WLAN) used by wireless clients to access into Internet through VigorAP.

Syntax

apm stanum [AP_Index]

Syntax Description

Parameter	Description
AP_Index	Specify the index number which represents VigorAP.

Example

```
> apm stanum

% Show the APM AP Station Number data.
% apm stanum AP_Index.
% ex: apm stanum 1
% Idx Nearby(2.4/5G) Conn(2.4/5G)
% 1 2 5 0 0 0
% 2 2 5 1 0
% 3 2 5 1 0
```

Telnet Command: swm show

This command is used to display general setting of VigorSwitch which connecting to Vigor router in LAN.

Syntax

swm show [LAN_port]

Daramatar	Description
Parameter	Description

LAN_port	Specify the LAN port number (1 to 6).

Telnet Command: swm get

This command is used to get configuration information of VigorSwitch which connecting to Vigor router in LAN.

Syntax

swm get [LAN_port]

Syntax Description

Parameter	Description
LAN_port	Specify the LAN port number (1 to 6).

Example

```
> swm get 1
Start get cfg from LAN (1) external switch
Please wait a few seconds...
Result: [OK].
>
```

Telnet Command: swm post

This command is used to transfer switch configuration to VigorSwitch which connecting to Vigor router in LAN.

Syntax

swm post [LAN_port]

Syntax Description

Parameter	Description
LAN_port	Specify the LAN port number (1 to 6).

```
> swm post 1
Start post cfg to LAN (1) external switch with currect settings.
Please wait a few seconds...
```

```
Result: [OK]
>
```

Telnet Command: swm auth

This command is used to display or remove the authentication record for external switch.

Syntax

swm auth [show/clear]

Syntax Description

Parameter	Description
show	Display recorded external switch MAC address list.
clear	Clear specific index of authentication record table. Index range: (1 - 30)

Example

Telnet Command: swm extvlan

This command is used to configure port VLAN of VigorSwitch.

Syntax

swm extvlan [LAN_Port][VLAN_idx][Port_Description]

Syntax Description

Parameter	Description
LAN_Port	Setting range is from 1 to 6.
VLAN_idx	Index number range for VLAN is from 0 to 7.
Port_Description	Setting range is from 1 to 24.

Example

```
> swm extvlan 1 1 13
Set OK.
> swm post 1
Start post cfg to LAN (1) external switch with currect settings.//post cfg
Please wait a few seconds...
Result: [OK].
```

System will cover the original VLAN settings on your VigorSwitch. Please backup the configuration file before you run this function.

System also will select the physical connect port as trunk port and let it join each VLAN group.

