

DrayTek

Vigor2862 Series VDSL2 Security Firewall

Your reliable networking solutions partner



User's Guide

V1.1

Vigor2862 Series VDSL2 Security Firewall

User's Guide

Version: 1.1

Firmware Version: V3.8.7

(For future update, please visit DrayTek web site)

Date: December 11, 2017

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

Warranty

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

Be a Registered Owner

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

Firmware & Tools Updates

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

<http://www.DrayTek.com>

Table of Contents

Part I Installation	i
I-1 Introduction	1
I-1-1 Indicators and Connectors	2
I-1-1-1 <i>Vigor2862 / Vigor2862B / Vigor2862L</i>	2
I-1-1-2 <i>Vigor2862n/Vigor2862ac/Vigor2862Bn/ Vigor2862Ln / Vigor2862Lac</i>	4
I-1-1-3 <i>Vigor2862Vac</i>	7
I-1-2 Notes for Antenna Installation (for “L” model)	9
I-2 Hardware Installation	11
I-2-1 Installing Vigor Router	11
I-2-2 Wall-Mounted Installation	12
I-2-3 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.....	27
I-5-3 Quick Access for Common Used Menu	28
I-5-4 GUI Map	29
I-5-5 Web Console	30
I-5-6 Config Backup	31
I-5-7 Logout.....	31
I-5-8 Online Status	32
I-5-8-1 <i>Physical Connection</i>	32
I-5-8-2 <i>Virtual WAN</i>	34
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-7 Service Activation Wizard	59
I-8 Registering Vigor Router.....	61
Part II Connectivity	63
II-1 WAN	64
Web User Interface	66
II-1-1 General Setup	66
II-1-1-1 <i>WAN1(ADSL/VDSL2)</i>	67
II-1-1-2 <i>WAN2 (Ethernet)/(Wireless 2.4G/5G)</i>	70
II-1-1-3 <i>WAN3/WAN4 (USB)</i>	72
II-1-2 Internet Access.....	74
II-1-2-1 <i>Details Page for PPPoE in WAN1 (Physical Mode: VDSL2)</i>	76
II-1-2-2 <i>Details Page for MPoA/Static or Dynamic IP in WAN1 (Physical Mode: VDSL2)</i>	79
II-1-2-3 <i>Details Page for PPPoE/PPPoA in WAN1 (Physical Mode: ADSL)</i>	82

II-1-2-4 Details Page for MPoA/Static or Dynamic IP in WAN1 (Physical Mode: ADSL) .	85
II-1-2-5 Details Page for PPPoE in WAN2 (Physical Mode: Ethernet)	89
II-1-2-6 Details Page for Static or Dynamic IP in WAN2 (Physical Mode: Ethernet).....	91
II-1-2-7 Details Page for PPTP/L2TP in WAN2 (Physical Mode: Ethernet)	95
II-1-2-8 Details Page for Static or Dynamic IP in WAN2 (Physical Mode: Wireless 2.4G)	97
II-1-2-9 Details Page for 3G/4G USB Modem (PPP mode) in WAN3/WAN4	100
II-1-2-10 Details Page for 3G/4G USB Modem (DHCP mode) in WAN3/WAN4	102
II-1-2-11 Details Page for IPv6 - Offline in WAN1/WAN2/WAN3/WAN4.....	104
II-1-2-12 Details Page for IPv6 - PPP in WAN1/WAN2	104
II-1-2-13 Details Page for IPv6 - TSPC in WAN1/WAN2/WAN3/WAN4	105
II-1-2-14 Details Page for IPv6 - AICCU in WAN1/WAN2/WAN3/WAN4	107
II-1-2-15 Details Page for IPv6 - DHCPv6 Client in WAN1/WAN2	109
II-1-2-16 Details Page for IPv6 - Static IPv6 in WAN1/WAN2	111
II-1-2-17 Details Page for IPv6 - 6in4 Static Tunnel in WAN1/WAN2	113
II-1-2-18 Details Page for IPv6 - 6rd in WAN1/WAN2	114
II-1-3 Multi-PVC/VLAN	116
II-1-4 WAN Budget.....	123
II-1-4-1 General Setup	123
II-1-4-2 Status	125
Application Notes	126
A-1 How to assign an IPv6 address to LAN clients?.....	126
A-2 How to configure IPv6 on WAN interface?.....	129
II-2 LAN	134
Web User Interface	136
II-2-1 General Setup	136
II-2-1-1 Details Page for LAN1 - Ethernet TCP/IP and DHCP Setup	138
II-2-1-2 Details Page for LAN2 ~ LAN8 and DMZ	140
II-2-1-3 Details Page for IP Routed Subnet	142
II-2-1-4 Details Page for LAN IPv6 Setup	143
II-2-2 VLAN	147
II-2-3 Bind IP to MAC	152
II-2-4 LAN Port Mirror.....	155
II-2-5 Wired 802.1x	156
II-3 Hardware Acceleration.....	157
II-3-1 Setup	157
II-4 NAT	160
Web User Interface	161
II-4-1 Port Redirection.....	161
II-4-2 DMZ Host	165
II-4-3 Open Ports	168
II-4-4 Port Triggering.....	170
II-4-5 ALG.....	172
II-5 Applications	173
Web User Interface	175
II-5-1 Dynamic DNS	175
II-5-2 LAN DNS / DNS Forwarding	179
II-5-3 DNS Security	182

II-5-3-1 General Setup	182
II-5-3-2 Domain Diagnose	183
II-5-4 Schedule	184
II-5-5 RADIUS/TACACS+	186
II-5-5-1 External RADIUS	186
II-5-5-2 Internal RADIUS	187
II-5-5-3 External TACACS+	190
II-5-6 Active Directory/LDAP	191
II-5-6-1 General Setup	191
II-5-6-2 Profiles	192
II-5-7 UPnP	194
II-5-8 IGMP	195
II-5-8-1 General Setting	195
II-5-8-2 Working Group	196
II-5-9 Wake on LAN	197
II-5-10 SMS / Mail Alert Service	198
II-5-10-1 SMS Alert	198
II-5-10-2 Mail Alert	199
II-5-11 Bonjour	200
II-5-12 High Availability	203
II-5-12-1 General Setup	204
II-5-12-2 Config Sync	206
II-5-13 Local 802.1X General Setup	208
Application Notes	210
A-1 How to Implement the LDAP/AD Authentication for User Management?	210
A-2 How to Configure Customized DDNS?	213
II-6 Routing	217
Web User Interface	218
II-6-1 Static Route	218
II-6-2 Load-Balance /Route Policy	223
Diagnose for Route Policy	228
II-6-3 BGP	231
II-6-3-1 Basic Settings	231
II-6-3-1 Static Network	232
Application Notes	233
A-1 How to set up Address Mapping with Route Policy?	233
A-2 How to use destination domain name in a route policy?	235
Part III Wireless LAN	237
III-1 Wireless LAN (2.4GHz/5GHz)	238
Web User Interface	241
III-1-1 Wireless Wizard	241
III-1-2 General Setup	245
III-1-3 Security	246
III-1-4 Access Control	249
III-1-5 WPS	251

III-1-6 WDS	254
III-1-7 Advanced Setting	257
III-1-8 Station Control.....	259
III-1-9 Bandwidth Management.....	260
III-1-10 AP Discovery	261
III-1-11 Airtime Fairness.....	262
III-1-12 Band Steering.....	264
III-1-13 Roaming	268
III-1-14 Station List.....	269
Part IV VPN	271
IV-1 VPN and Remote Access	272
Web User Interface	273
IV-1-1 VPN Client Wizard	273
IV-1-2 VPN Server Wizard	279
IV-1-3 Remote Access Control	283
IV-1-4 PPP General Setup.....	284
IV-1-5 IPsec General Setup	286
IV-1-6 IPsec Peer Identity	287
IV-1-7 Remote Dial-in User.....	289
IV-1-8 LAN to LAN	292
IV-1-9 VPN Trunk Management	303
IV-1-10 Connection Management.....	313
Application Notes	314
<i>A-1 How to Build a LAN-to-LAN VPN Between Vigor Routers via IPsec Main Mode ...</i>	<i>314</i>
<i>A-2 How to Build a LAN-to-LAN VPN Between Vigor Routers via IKEv2</i>	<i>319</i>
IV-2 SSL VPN	322
Web User Interface	323
IV-2-1 General Setup	323
IV-2-2 User Account.....	324
IV-2-3 User Group.....	328
IV-2-4 Online User Status	330
IV-3 Certificate Management.....	331
Web User Interface	332
IV-3-1 Local Certificate	332
IV-3-2 Trusted CA Certificate.....	336
IV-3-3 Certificate Backup.....	338
Part V Security	339
V-1 Firewall.....	340
Web User Interface	342
V-1-1 General Setup	342

V-1-2 Filter Setup	347
V-1-3 DoS Defense	357
V-1-4 Diagnose	361
Application Notes	364
<i>A-1 How to Configure Certain Computers Accessing to Internet</i>	<i>364</i>
V-2 Central Security Management (CSM)	368
Web User Interface	369
V-2-1 APP Enforcement Profile	369
V-2-2 APPE Signature Upgrade	373
V-2-3 URL Content Filter Profile	375
V-2-4 Web Content Filter Profile	379
V-2-5 DNS Filter Profile	383
Application Notes	385
<i>A-1 How to Create an Account for MyVigor</i>	<i>385</i>
<i>A-2 How to Block Facebook Service Accessed by the Users via Web Content Filter / URL Content Filter</i>	<i>393</i>
Part VI Management	399
VI-1 System Maintenance	400
Web User Interface	401
VI-1-1 System Status	401
VI-1-2 TR-069	403
VI-1-3 Administrator Password	406
VI-1-4 User Password	408
VI-1-5 Login Page Greeting	411
VI-1-6 Configuration Backup	413
VI-1-7 Syslog/Mail Alert	417
VI-1-8 Time and Date	419
VI-1-9 SNMP	420
VI-1-10 Management	422
VI-1-11 Self-Signed Certificate	426
VI-1-12 Reboot System	428
VI-1-13 Firmware Upgrade	429
VI-1-14 Firmware Backup	430
VI-1-15 Modem Code Upgrade	430
VI-1-16 Activation	430
VI-1-17 Internal Service User List	432
VI-1-18 Dashboard Control	433
VI-2 Bandwidth Management	434
Web User Interface	436
VI-2-1 Sessions Limit	436
VI-2-2 Bandwidth Limit	438

VI-2-3 Quality of Service	440
VI-2-4 APP QoS	447
Application Notes	449
<i>A-1 How to Optimize the Bandwidth through QoS Technology</i>	<i>449</i>
VI-3 User Management	453
Web User Interface	454
VI-3-1 General Setup	454
VI-3-2 User Profile	456
VI-3-3 User Group.....	461
VI-3-4 User Online Status	462
Application Notes	464
<i>A-1 How to authenticate clients via User Management</i>	<i>464</i>
<i>A-2 How to use Landing Page Feature</i>	<i>473</i>
VI-4 Hotspot Web Portal.....	477
Web User Interface	477
VI-4-1 Profile Setup.....	477
<i>VI-4-1-1 Login Modes</i>	<i>478</i>
<i>VI-4-1-2 Steps for Configuring a Web Portal Profile</i>	<i>480</i>
VI-4-2 Users Information.....	493
<i>VII-4-2-1 User Info</i>	<i>493</i>
<i>VII-4-2-2 Database Setup</i>	<i>495</i>
Application Notes	496
<i>A-1 How to create Facebook APP for Web Portal Authentication?</i>	<i>496</i>
<i>A-2 How to create Google APP for Web Portal Authentication?</i>	<i>502</i>
VI-5 Central Management (VPN)	504
Web User Interface	505
VI-5-1 General Setup	505
<i>VI-5-1-1 General Settings.....</i>	<i>505</i>
<i>VI-5-1-2 IPsec VPN Settings</i>	<i>506</i>
VI-5-2 CPE Management.....	507
<i>VI-5-2-1 Managed Device List</i>	<i>507</i>
<i>VI-5-2-2 CPE Maintenance</i>	<i>510</i>
<i>VI-5-2-3 Google Map.....</i>	<i>512</i>
VI-5-3 VPN Management.....	514
VI-5-4 Log & Alert	515
Application Notes	516
<i>A-1 CVM Application - How to manage the CPE (router) through Vigor2862 series? ..</i>	<i>516</i>
<i>A-2 CVM Application - How to build the VPN between remote devices and Vigor2862</i>	<i>520</i>
<i>series?</i>	<i>520</i>
<i>A-3 CVM Application - How to upgrade CPE firmware through Vigor2862 series?</i>	<i>522</i>
VI-6 Central Management (AP).....	525
Web User Interface	526
VI-6-1 Dashboard.....	526
VI-6-2 Status	527
VI-6-3 WLAN Profile.....	528

VI-6-4 AP Maintenance.....	533
VI-6-5 AP Map	534
VI-6-6 Traffic Graph	539
VI-6-7 Temperature Sensor	540
VI-6-8 Rogue AP Detection.....	540
VI-6-9 Event Log	543
VI-6-10 Total Traffic	543
VI-6-11 Station Number	544
VI-6-12 Load Balance	544
VI-6-13 Function Support List	546
Application Notes	547
<i>A-1 How to use AP Management function (in Vigor2862) to check AP status and deploy WLAN profile</i>	<i>547</i>
VI-7 Central Management (Switch).....	550
VI-7-1 Status	550
<i>VI-7-1-1 Switch Status</i>	<i>550</i>
<i>VI-7-1-2 Switch Hierarchy</i>	<i>552</i>
VI-7-2 Profile	553
VI-7-3 Group	556
VI-7-4 Maintenance.....	558
VI-7-5 Alert and Log.....	559
<i>VI-7-5-1 Alert Setup.....</i>	<i>559</i>
<i>VI-7-5-2 Switch and Port Setup.....</i>	<i>560</i>
<i>VI-7-5-3 Alert Logs</i>	<i>562</i>
VI-7-6 Database Setup	563
VI-7-7 Support List.....	564
VI-7 Central Management (External Devices)	565
Part VII Others.....	567
VII-1 Objects Settings.....	568
Web User Interface	569
VII-1-1 IP Object	569
VII-1-2 IP Group.....	573
VII-1-3 IPv6 Object.....	574
VII-1-4 IPv6 Group	576
VII-1-5 Service Type Object.....	577
VII-1-6 Service Type Group	579
VII-1-7 Keyword Object.....	581
VII-1-8 Keyword Group	583
VII-1-9 File Extension Object	584
VII-1-10 SMS/Mail Service Object	586
VII-1-11 Notification Object.....	591
VII-1-12 String Object	593

VII-1-13 Country Object	594
Application Notes	596
<i>A-1 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection</i>	596
VII-2 USB Application	600
Web User Interface	601
VII-2-1 USB General Settings	601
VII-2-2 USB User Management	602
VII-2-3 File Explorer	604
VII-2-4 USB Device Status	605
VII-2-5 Temperature Sensor	606
VII-2-6 Modem Support List	608
VII-2-7 SMB Client Support List	609
Application Notes	610
<i>A-1 How can I get the files from USB storage device connecting to Vigor router? ...</i>	610
Part VIII Troubleshooting	613
VIII-1 Diagnostics	614
Web User Interface	615
VIII-1-1 Dial-out Triggering	615
VIII-1-2 Routing Table	616
VIII-1-3 ARP Cache Table	617
VIII-1-4 IPv6 Neighbour Table	618
VIII-1-5 DHCP Table	619
VIII-1-6 NAT Sessions Table	620
VIII-1-7 DNS Cache Table	621
VIII-1-8 Ping Diagnosis	622
VIII-1-9 Data Flow Monitor	623
VIII-1-10 Traffic Graph	625
VIII-1-11 VPN Graph	626
VIII-1-12 Trace Route	627
VIII-1-13 Syslog Explorer	628
VIII-1-14 IPv6 TSPC Status	629
VIII-1-15 DSL Status	630
VIII-1-16 High Availability Status	630
VIII-1-17 Authentication Information	632
VIII-1-18 DoS Flood Table	634
VIII-1-19 Route Policy Diagnosis	636
VIII-2 Checking If the Hardware Status Is OK or Not	638
VIII-3 Checking If the Network Connection Settings on Your Computer Is OK or Not	639
VIII-4 Pinging the Router from Your Computer	642
VIII-5 Checking If the ISP Settings are OK or Not	644

VIII-6 Problems for 3G/4G Network Connection	645
VIII-7 Backing to Factory Default Setting If Necessary	646
VIII-8 Contacting DrayTek	647
Appendix I: VLAN Applications on Vigor Router	648
Part IX Telnet Commands.....	657
Accessing Telnet of Vigor2862	658
Index	877

Part I Installation



Installation

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

I-1 Introduction

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

Vigor2862 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 4-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 (Vigor2862n/ac) each of the wireless SSIDs can also be grouped within one of the VLANs.

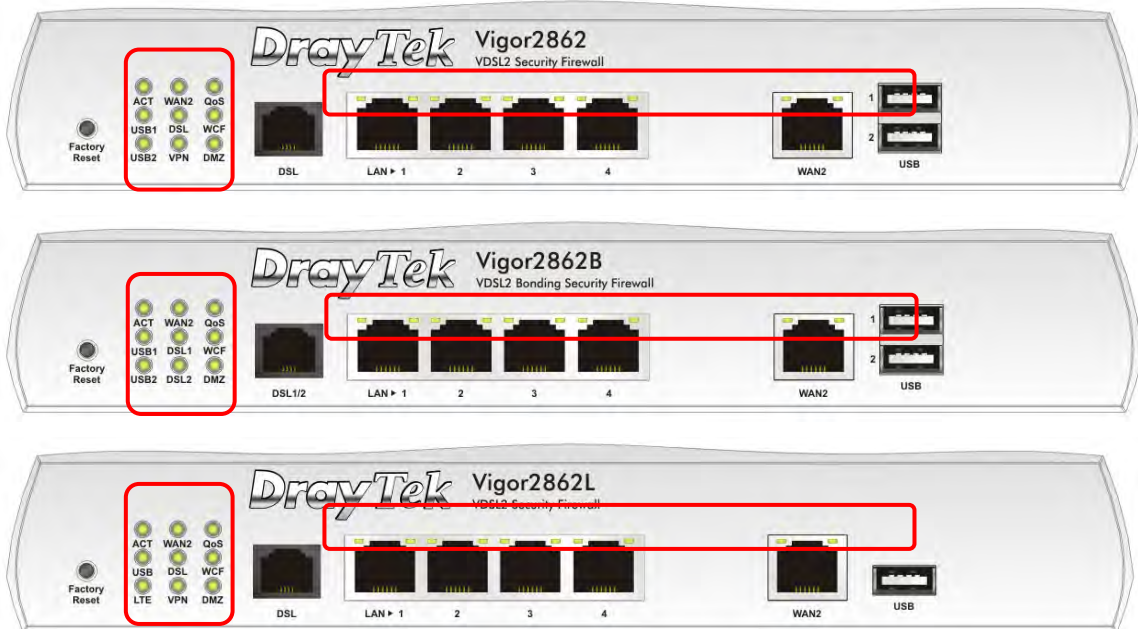
In addition, Vigor2862 series supports USB interface for connecting USB printer to share printing function or 3G USB modem for network connection.

Vigor2862 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

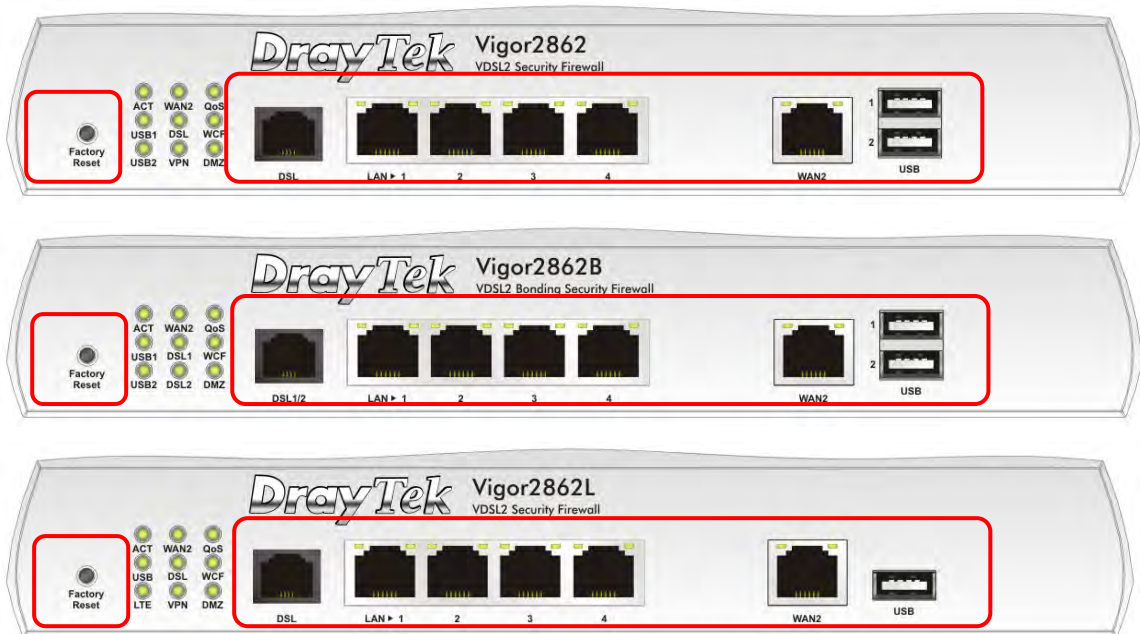
Before you use the Vigor router, please get acquainted with the LED indicators and connectors first.

I-1-1-1 Vigor2862 / Vigor2862B / Vigor2862L



LED	Status	Explanation
ACT (Activity)	Off	The router is powered off.
	Blinking	The router is powered on and running normally.
WAN2	On	Internet connection is ready.
	Off	Internet connection is not ready.
	Blinking	The data is transmitting.
QoS	On	The QoS function is active.
	Off	The QoS function is inactive.
USB1~2 / USB	On	USB device is connected and ready for use.
	Off	No USB device is connected.
	Blinking	The data is transmitting.
DSL/DSL 1/2	On	The router is ready to access Internet through DSL link.
	Blinking	Slowly: The DSL connection is ready. Quickly: The DSL connection is establishing.
WCF	On	The Web Content Filter is active. (It is enabled from Firewall >> General Setup).
	Off	WCF is disabled.
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.
VPN	On	The VPN tunnel is active.
	Off	VPN services are disabled
	Blinking	Traffic is passing through VPN tunnel.
DMZ	On	The DMZ function is enabled.

		Off	The DMZ function is disabled.
		Blinking	The data is transmitting.
LED on Connector			
LAN 1~4	Left LED	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
WAN2	Left LED	On	The port is connected with 1000Mbps.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
WAN2	Right LED	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps



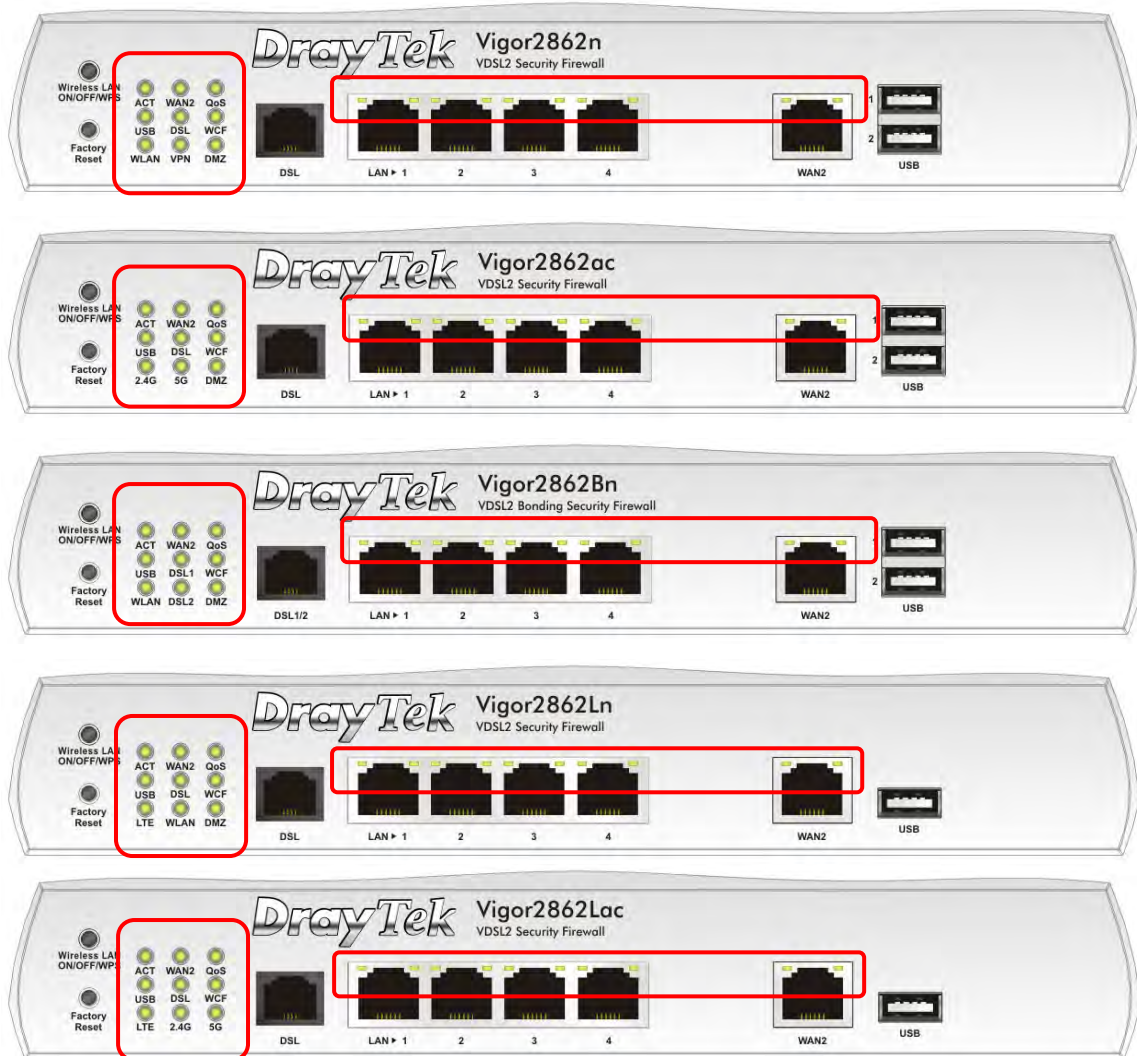
Switch on Rear Side



(Available for Vigor2862L)

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.
DSL / DSL 1/2	Connector for accessing the Internet.
LAN 1~4	Connectors for local network devices.
WAN2	Connector for local network devices or modem for accessing Internet.
USB 1~2	Connector for a USB device (for 3G/4G USB Modem or printer or thermometer).
PWR	Connector for a power adapter.
ON/OFF	Power Switch.

I-1-1-2 Vigor2862n/Vigor2862ac/Vigor2862Bn/ Vigor2862Ln / Vigor2862Lac



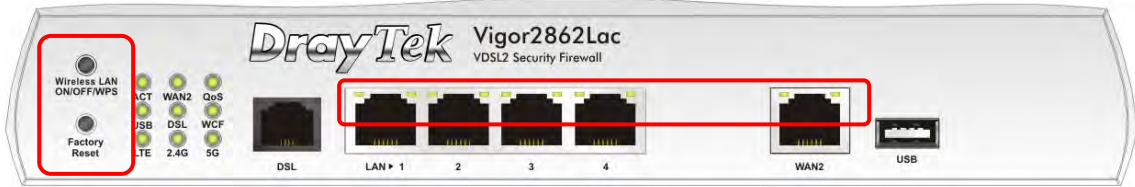
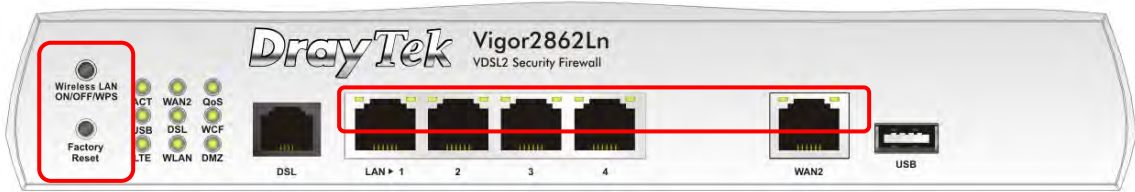
LED	Status	Explanation
ACT (Activity)	Off	The router is powered off.
	Blinking	The router is powered on and running normally.
WAN2	On	Internet connection is ready.
	Off	Internet connection is not ready.
	Blinking	The data is transmitting.
QoS	On	The QoS function is active.
	Off	The QoS function is inactive.
USB	On	USB device is connected and ready for use.
	Off	No USB device is connected.
	Blinking	The data is transmitting.
DSL / DSL 1/2	On	The router is ready to access Internet through DSL link.
	Blinking	Slowly: The DSL connection is ready. Quickly: The DSL connection is establishing.
WCF	On	The Web Content Filter is active. (It is enabled from Firewall >> General Setup).
	Off	WCF is disabled.
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.
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.
	Off	Wireless function is disabled.
	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.
DMZ	On	The DMZ function is enabled.
	Off	The DMZ function is disabled.
	Blinking	The data is transmitting.

LED on Connector

LAN 1~4	Left LED	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps
		Blinking	The data is transmitting.
WAN2	Left LED	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps





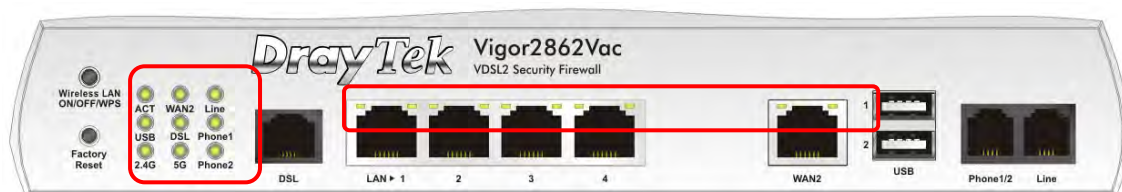
Switch on Rear Side



(Available for Vigor2862Ln/Lac)

Interface	Description
Wireless LAN ON/OFF/WPS	<p>For Vigor2862n/Vigor2862Bn :</p> <ul style="list-style-type: none"> ● 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. <p>For Vigor2862ac/Vigor2862Ln/Vigor2862Lac::</p> <p>Wireless band will be switched /changed according to the button pressed and released. For example,</p> <ul style="list-style-type: none"> ● 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. <p>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.</p>
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 1-2	Connector for a USB device (for 3G/4G USB Modem or printer or thermometer).
DSL / DSL 1/2	Connector for accessing the Internet.
LAN 1~4	Connectors for local network devices.
WAN2	Connector for local network devices or modem for accessing Internet.
PWR	Connector for a power adapter.
ON/OFF	Power Switch.

I-1-1-3 Vigor2862Vac



LED	Status	Explanation
ACT (Activity)	Off	The router is powered off.
	Blinking	The router is powered on and running normally.
USB	On	USB device is connected and ready for use.
	Off	No USB device is connected.
	Blinking	The data is transmitting.
WAN2	On	Internet connection is ready.
	Off	Internet connection is not ready.
	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.
2.4G/5G	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.)
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.
Phone 1/2	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.

LED on Connector

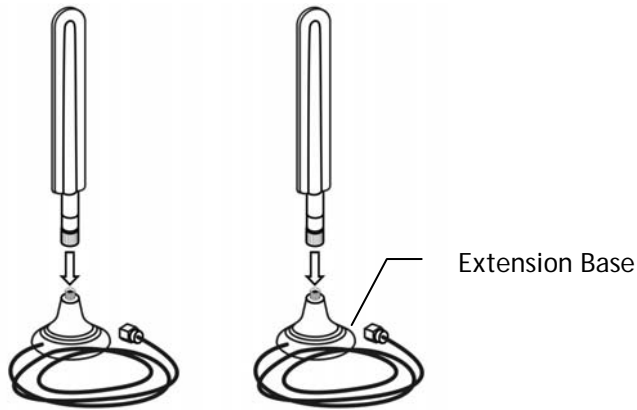
LAN 1~4	Left LED	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps
		Blinking	The data is transmitting.
WAN2	Left LED	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps
		Blinking	The data is transmitting.



Interface	Description
Wireless LAN ON/OFF/WPS	Wireless band will be switched /changed according to the button pressed and released. For example, <ul style="list-style-type: none"> ● 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.
DSL	Connector for accessing the Internet.
LAN 1~4	Connectors for local network devices.
WAN2	Connector for local network devices or modem for accessing Internet.
USB 1~2	Connector for a USB device (for 3G/4G USB Modem or printer or thermometer).
Phone 1/2	Connector for analog phone(s).
Line	Connector for PSTN life line.
PWR	Connector for a power adapter.
ON/OFF	Power Switch.

I-1-2 Notes for Antenna Installation (for "L" model)

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

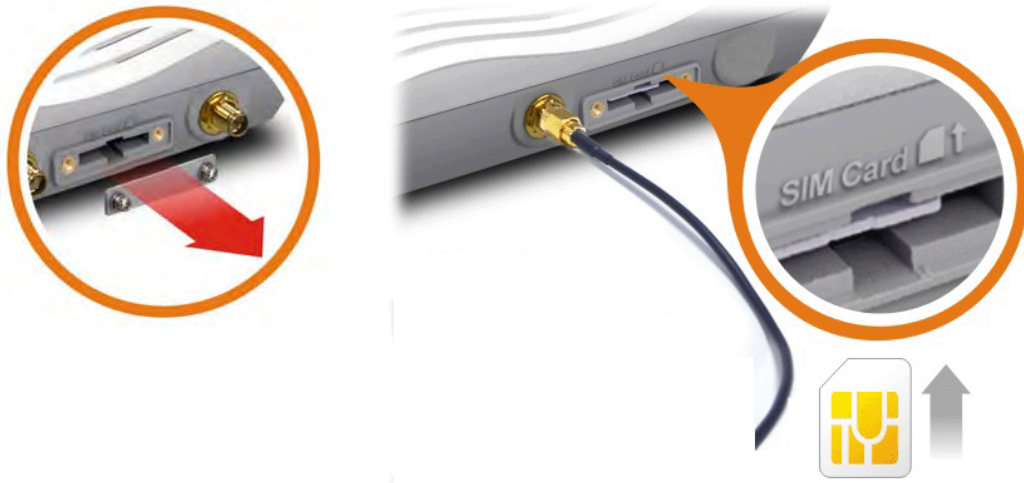


There are two mounting holes for installing antennas with extension base on Vigor router. Please install them as shown below.

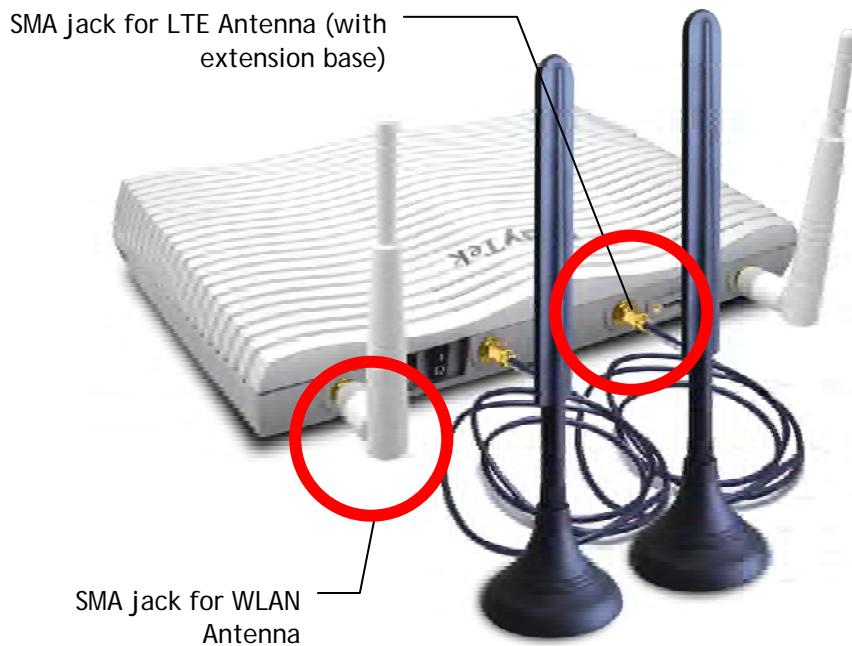


Note, if only one antenna shall be installed, please use the mounting hole (major signal transmitted hole) near to the SIM card slot.

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 Vigor2862Ln/Vigor2862Lac, 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.



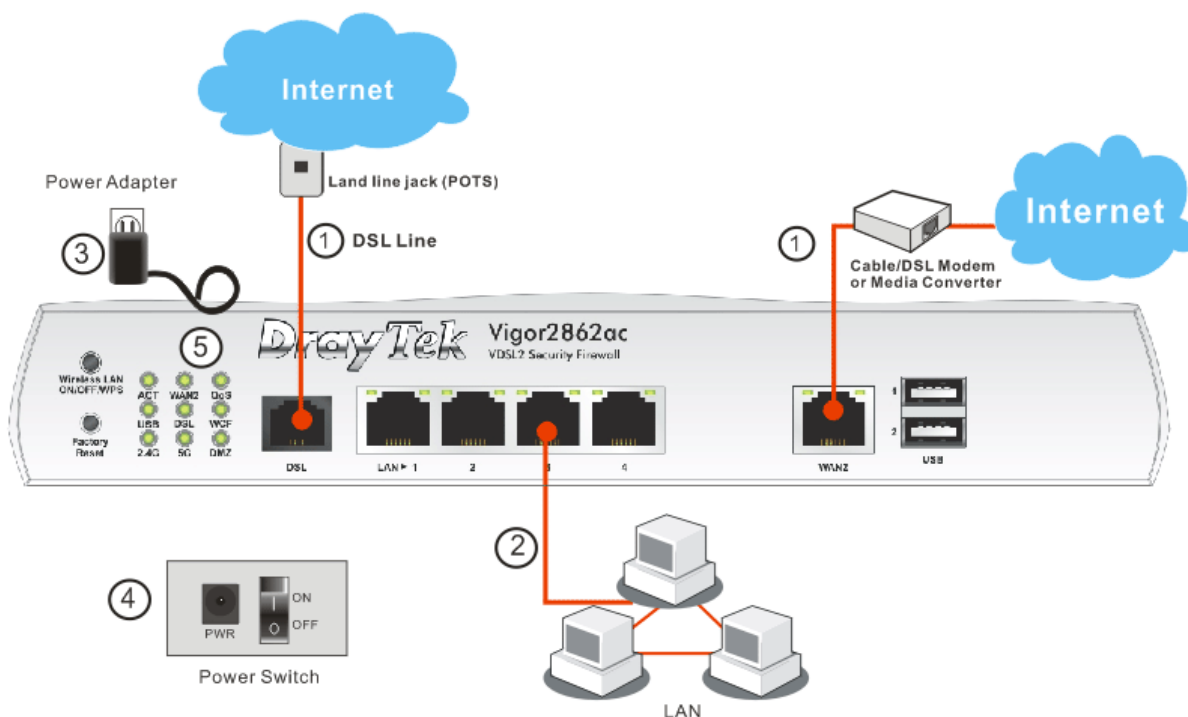
I-2 Hardware Installation

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

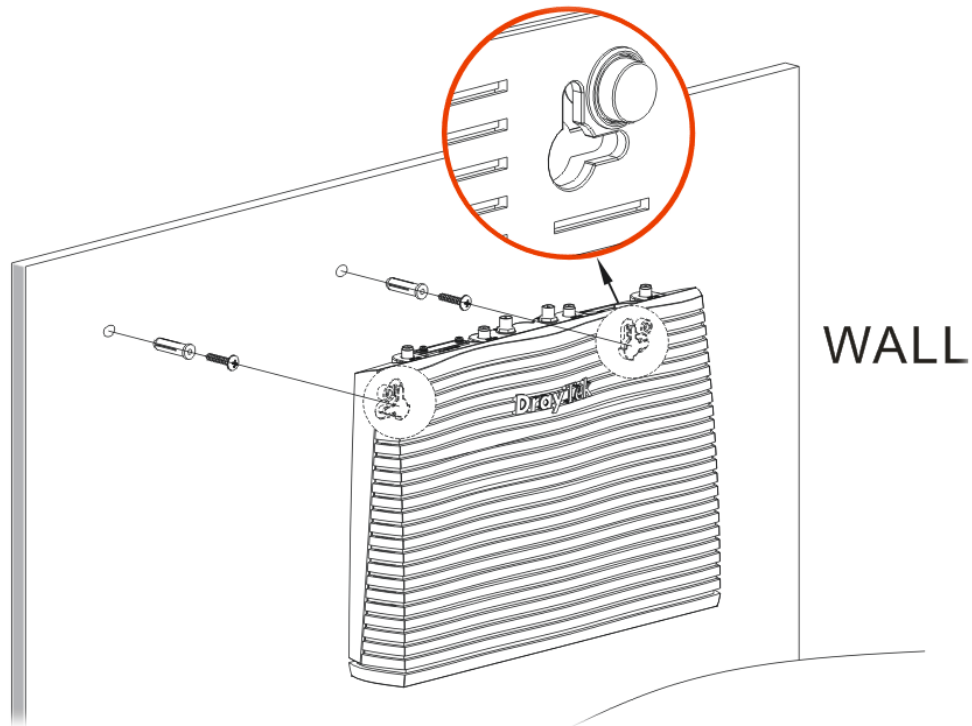
(For the hardware connection, we take "ac" model as an example.)



I-2-2 Wall-Mounted Installation

Vigor router has keyhole type mounting slots on the underside.

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



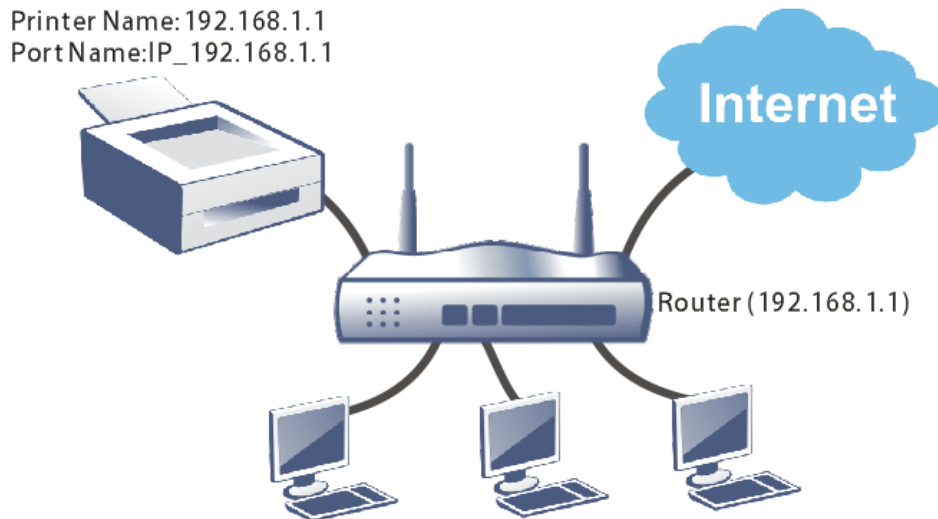
Info

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

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

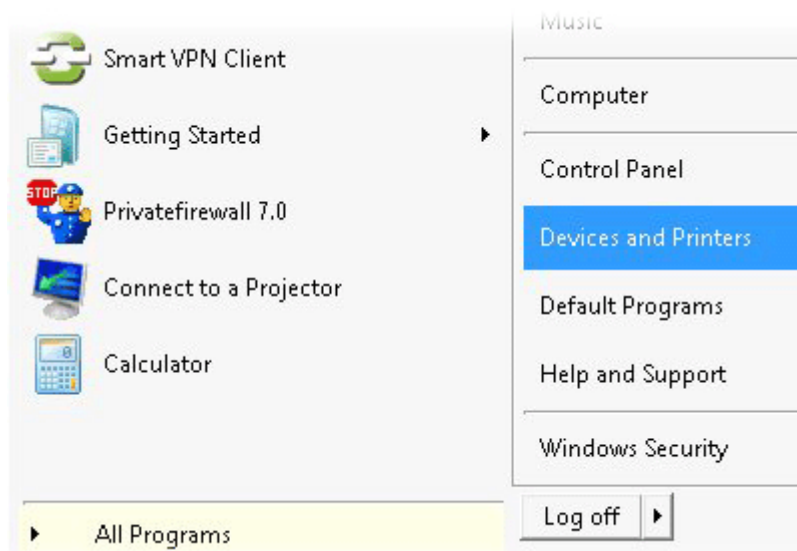
I-2-3 Installing USB Printer to Vigor Router

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

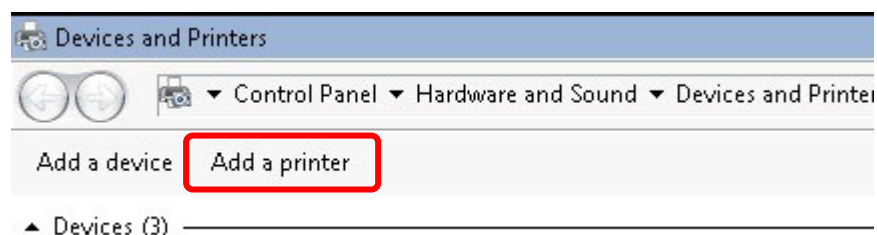


Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

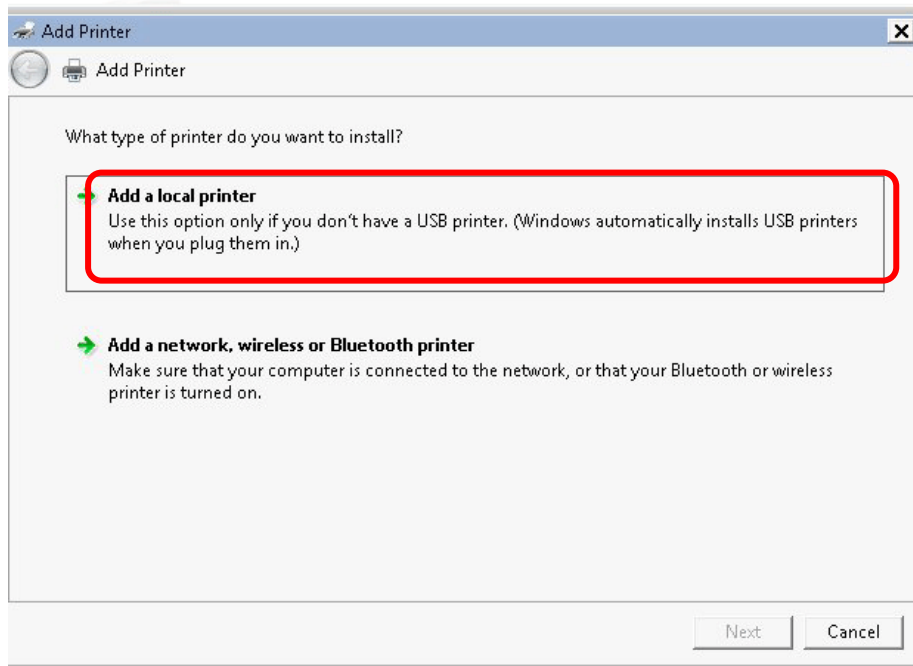
1. Connect the printer with the router through USB/parallel port.
2. Open All Programs>>Getting Started>>Devices and Printers.



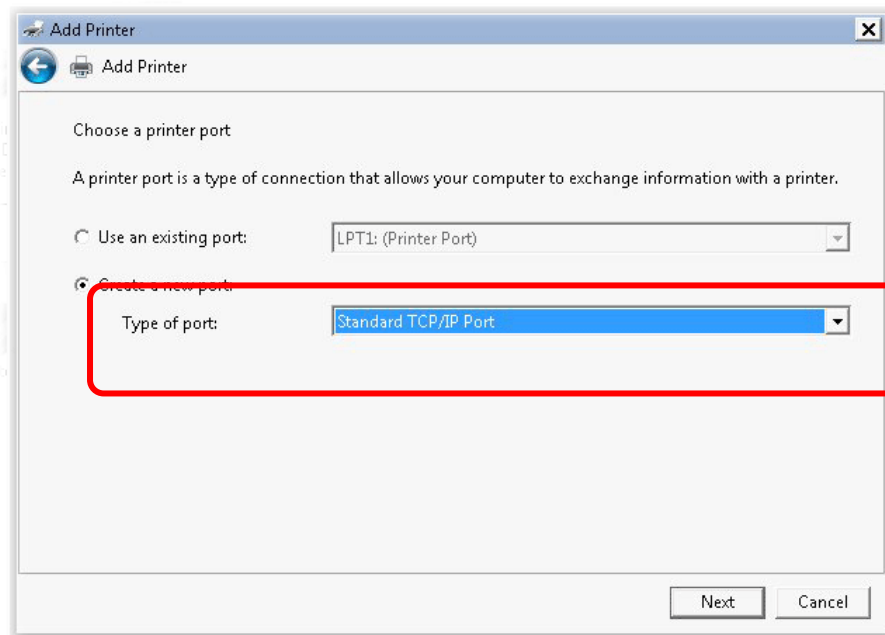
3. Click Add a printer.



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



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



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

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

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

Buttons: Next, Cancel

7. Click Standard and choose Generic Network Card.

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

Additional port information required

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

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

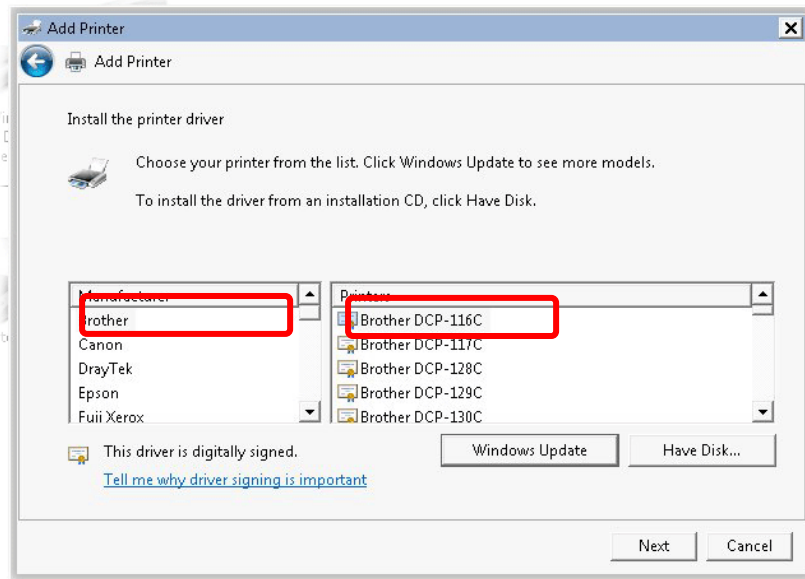
If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.

Device Type

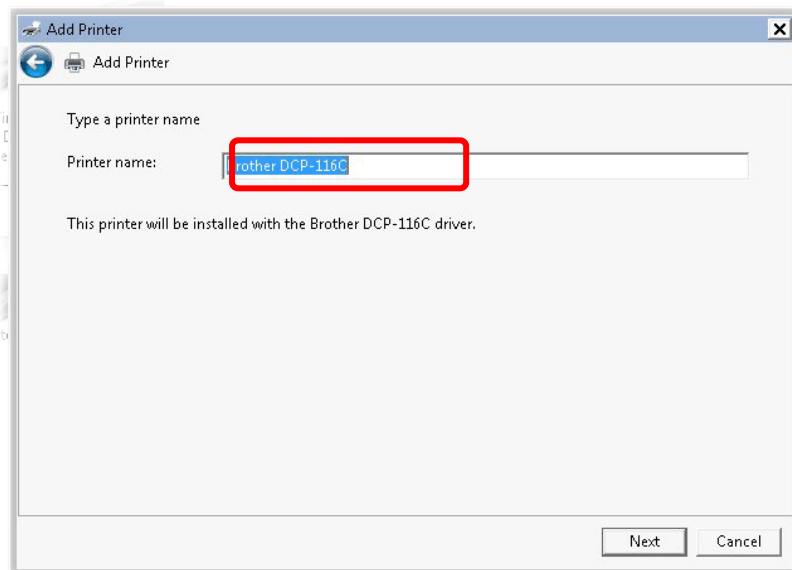
- Standard: Generic Network Card
- Custom: Settings...

Buttons: Next, Cancel

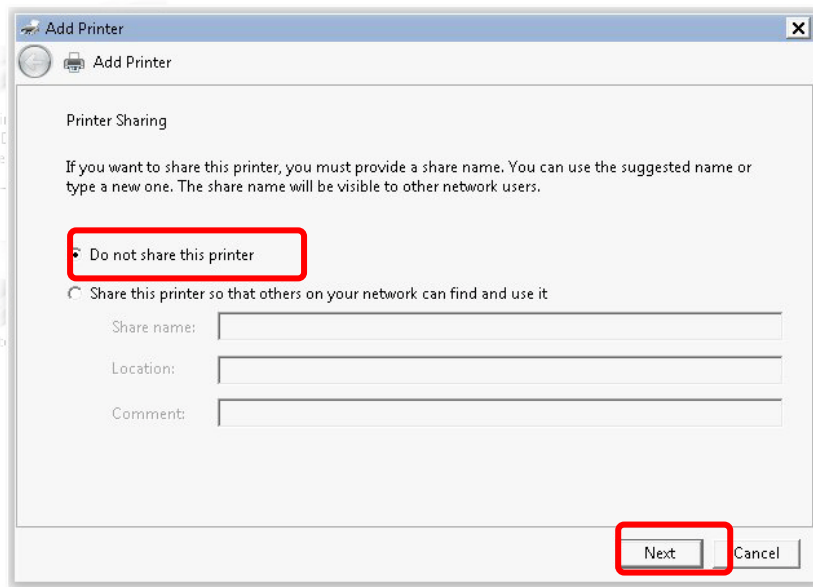
8. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.



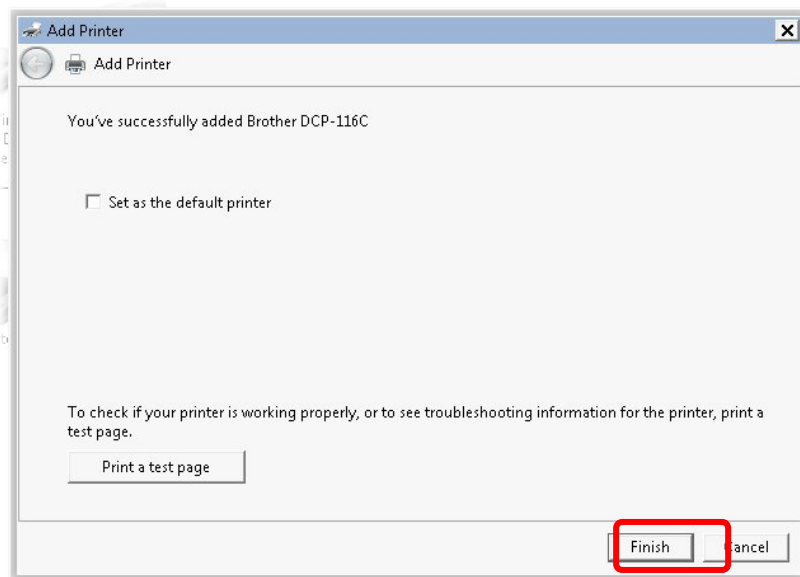
9. Type a name for the chosen printer. Click **Next**.



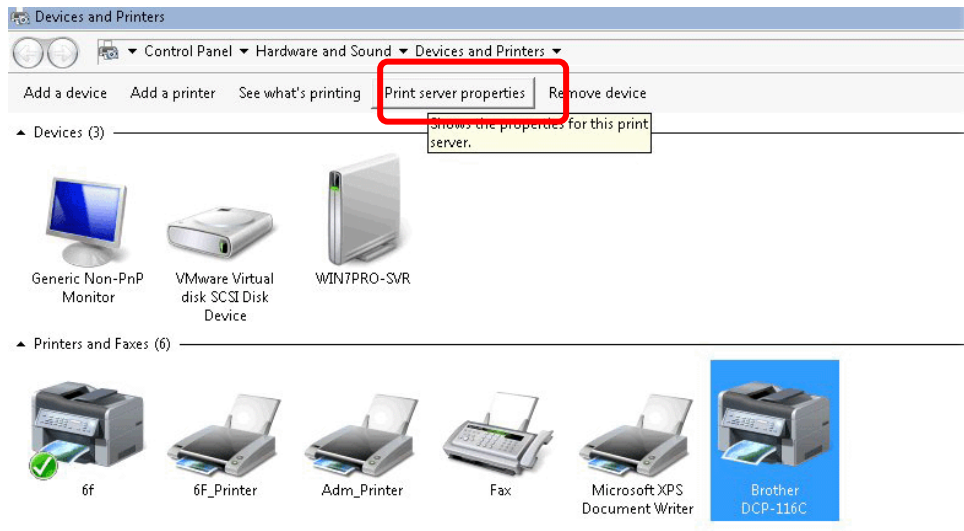
10. Choose **Do not share this printer** and click **Next**.



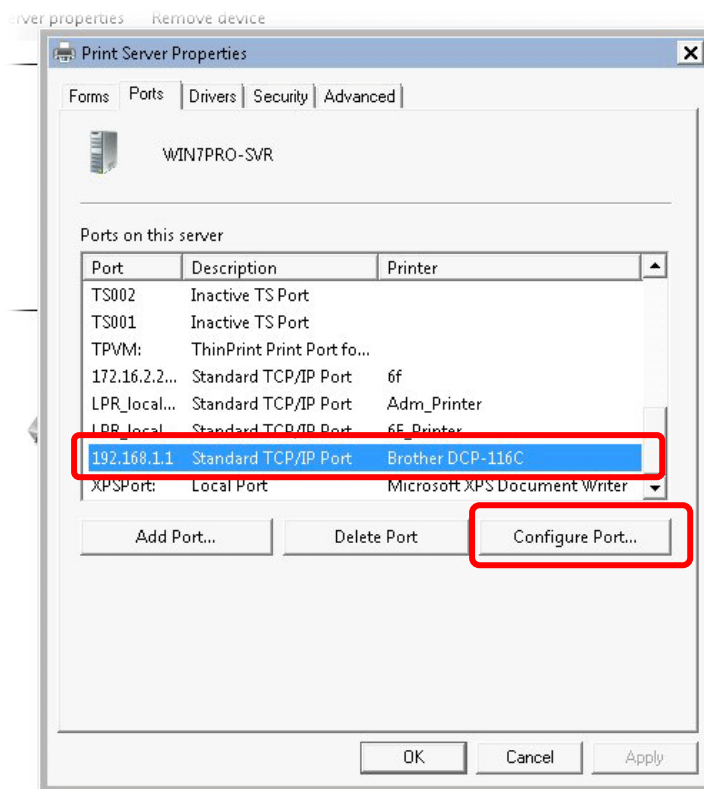
11. Then, in the following dialog, click **Finish**.



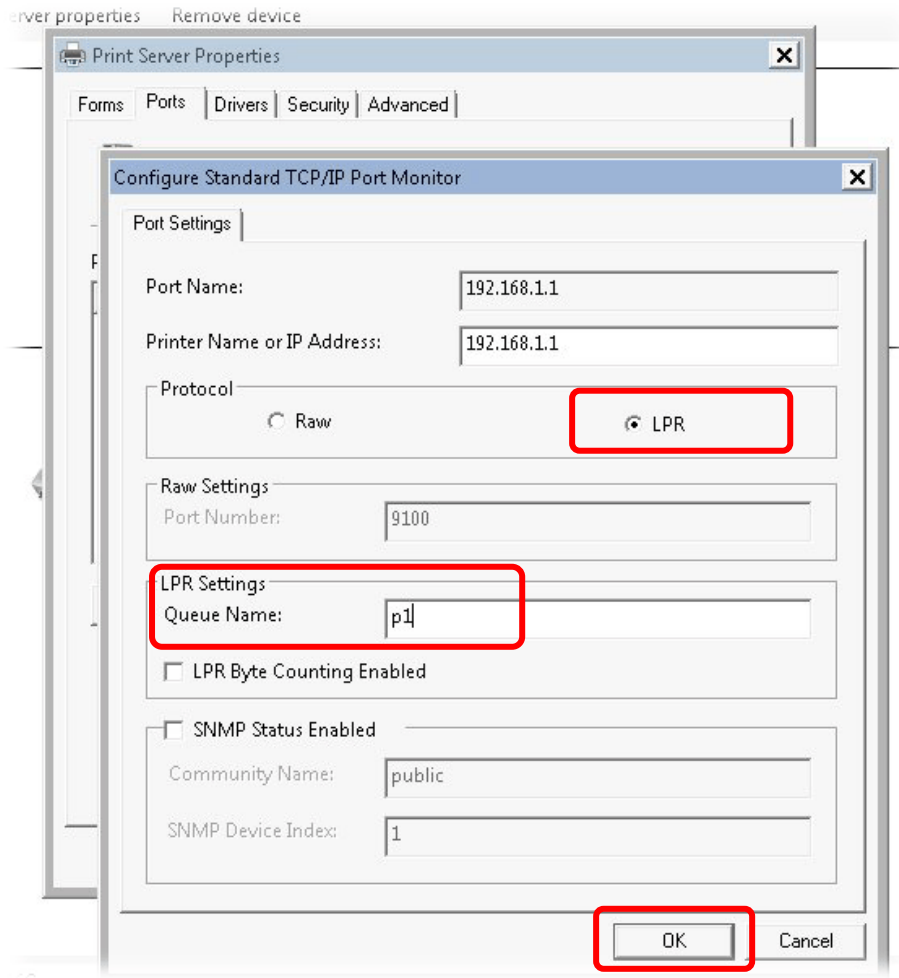
12. The new printer has been added and displayed under **Printers and Faxes**. Click the new printer icon and click **Printer server properties**.



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.

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.



DrayTek Vigor2862 Series

Login

Username

Password

Login

Copyright © 2000- 2016 DrayTek Corp. All Rights Reserved.

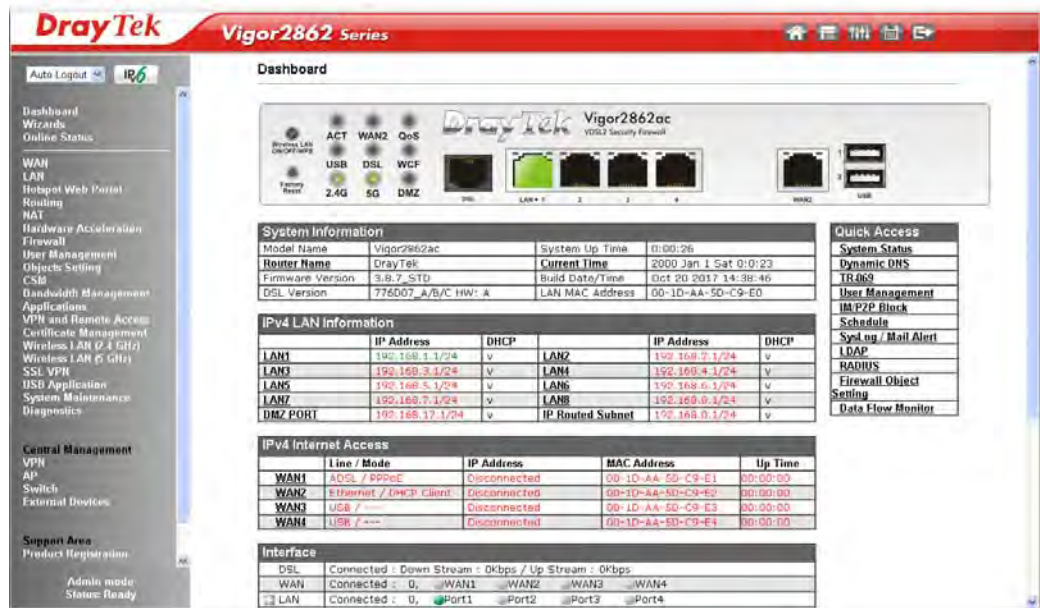
3. Please type "admin/admin" as the Username/Password and click Login.



Info

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

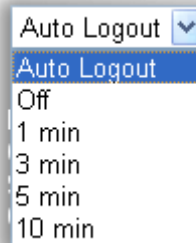
- Now, the Main Screen will appear. Take Vigor2862ac as an example.



Info

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

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



I-4 Changing Password

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

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

System Maintenance >> Administrator Password Setup

Administrator Password

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

Note:

Password can contain only a-z A-Z 0-9 ; : . " < > * + = | ? @ # ^ ! ()

Administrator Local User

<input type="checkbox"/> Local User				
Local User List				
<table border="1"><thead><tr><th>Index</th><th>User Name</th></tr></thead><tbody><tr><td> </td><td> </td></tr></tbody></table>	Index	User Name		
Index	User Name			
Specific User				
User Name: <input type="text"/>				
Password: <input type="text"/> Confirm Password: <input type="text"/>				
(Max.15 characters for User Name and Password)				
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				
<input checked="" type="checkbox"/> Enable 'admin' account login to Web UI from the Internet				

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



Info

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

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

Login

Username
Password

Login

Copyright © 2000- 2016 DrayTek Corp. All Rights Reserved.



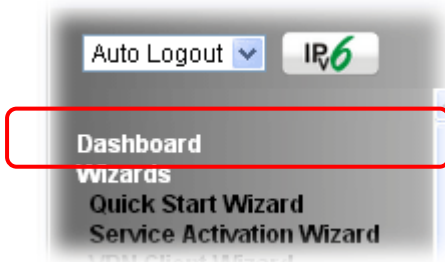
Info

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

I-5 Dashboard

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

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



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

Dashboard



System Information			
Model Name	Vigor2862ac	System Up Time	0:00:35
Router Name	DrayTek	Current Time	2000 Jan 1 Sat 0:0:28
Firmware Version	3.8.7_RC3_STD	Build Date/Time	Sep 29 2017 14:06:14
DSL Version	776D07_A/B/C HW: A	LAN MAC Address	00-1D-AA-5D-C9-E0

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

IPv4 LAN Information					
	IP Address	DHCP		IP Address	DHCP
LAN1	192.168.1.1/24	v	LAN2	192.168.2.1/24	v
LAN3	192.168.3.1/24	v	LAN4	192.168.4.1/24	v
LAN5	192.168.5.1/24	v	LAN6	192.168.6.1/24	v
LAN7	192.168.7.1/24	v	LAN8	192.168.8.1/24	v
DMZ PORT	192.168.17.1/24	v	IP Routed Subnet	192.168.0.1/24	v

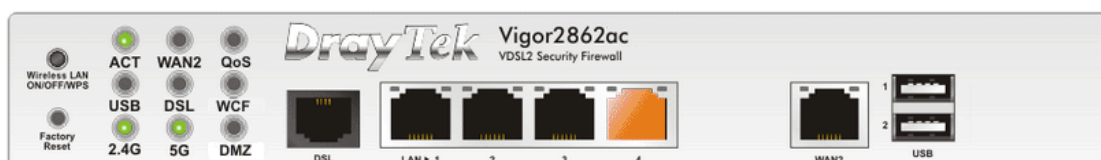
IPv4 Internet Access				
	Line / Mode	IP Address	MAC Address	Up Time
WAN1	ADSL / PPPoE	Disconnected	00-1D-AA-5D-C9-E1	00:00:00
WAN2	Ethernet / DHCP Client	Disconnected	00-1D-AA-5D-C9-E2	00:00:00
WAN3	USB / ---	Disconnected	00-1D-AA-5D-C9-E3	00:00:00
WAN4	USB / ---	Disconnected	00-1D-AA-5D-C9-E4	00:00:00

Interface	
DSL	Connected : Down Stream : 0Kbps / Up Stream : 0Kbps
WAN	Connected : 0, <input type="radio"/> WAN1 <input type="radio"/> WAN2 <input type="radio"/> WAN3 <input type="radio"/> WAN4

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.
LAN 1 ~ 4	Black	LAN port is disconnected.
	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., [Router Name](#), [Current Time](#), [WAN1~4](#) and etc.) below means you can click it to open the configuration page for modification.

System Information			
Model Name	Vigor2862ac	System Up Time	0:00:35
Router Name	DrayTek	Current Time	2000 Jan 1 Sat 0:0:28
Firmware Version	3.8.7_RC3_STD	Build Date/Time	Sep 29 2017 14:06:14
DSL Version	776D07_A/B/C HW: A	LAN MAC Address	00-1D-AA-5D-C9-E0

IPv4 LAN Information					
	IP Address	DHCP		IP Address	DHCP
LAN1	192.168.1.1/24	v	LAN2	192.168.2.1/24	v
LAN3	192.168.3.1/24	v	LAN4	192.168.4.1/24	v
LAN5	192.168.5.1/24	v	LAN6	192.168.6.1/24	v
LAN7	192.168.7.1/24	v	LAN8	192.168.8.1/24	v
DMZ PORT	192.168.17.1/24	v	IP Routed Subnet	192.168.0.1/24	v

IPv4 Internet Access				
	Line / Mode	IP Address	MAC Address	Up Time
WAN1	ADSL / PPPoE	Disconnected	00-1D-AA-5D-C9-E1	00:00:00
WAN2	Ethernet / DHCP Client	Disconnected	00-1D-AA-5D-C9-E2	00:00:00
WAN3	USB / ---	Disconnected	00-1D-AA-5D-C9-E3	00:00:00
WAN4	USB / ---	Disconnected	00-1D-AA-5D-C9-E4	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**.

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

The function links of System Status, Dynamic DDNS, TR-069, User Management, IM/P2P Block, Schedule, Syslog/Mail Alert, 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.

DMZ PORT	192.168.17.1/24	v	IP Routed Subnet	192.168.0.1/24	v
-----------------	-----------------	---	-------------------------	----------------	---

IPv4 Internet Access				
	Line / Mode	IP Address	MAC Address	Up Time
WAN1	ADSL / ---	Disconnected	00-1D-AA-F7-C0-F1	00:00:00
WAN2	Ethernet / DHCP Client	Disconnected	00-1D-AA-F7-C0-F2	00:00:00
WAN3	USB / ---	Disconnected	00-1D-AA-F7-C0-F3	00:00:00
WAN4	USB / ---	Disconnected	00-1D-AA-F7-C0-F4	00:00:00

Interface	
DSL	Connected : Down Stream : OKbps / Up Stream : OKbps
WAN	Connected : 0, <input type="radio"/> WAN1 <input type="radio"/> WAN2 <input type="radio"/> WAN3 <input type="radio"/> WAN4
<input checked="" type="checkbox"/> LAN	Connected : 0, <input type="radio"/> Port1 <input type="radio"/> Port2 <input type="radio"/> Port3 <input checked="" type="radio"/> Port4
<input checked="" type="checkbox"/> WLAN	Connected : 0
<input checked="" type="checkbox"/> WLAN5G	Connected : 0
USB	Connected : 0, <input type="radio"/> USB 1 0, <input type="radio"/> USB 2

Security	
<input checked="" type="checkbox"/> VPN	Connected : 0 Remote Dial-in User / LAN to LAN
<input checked="" type="checkbox"/> AntiVigor	Activate : 0
<input checked="" type="checkbox"/> DoS	Attack Detected :

System Resource	
Current Status	CPU Usage: <div style="width: 10%; height: 10px; background-color: blue;"></div> 01%
	Memory Usage: <div style="width: 50%; height: 10px; background-color: blue;"></div> 54%

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.

Interface	
DSL	Connected : Down Stream : 0Kbps / Up Stream : 0Kbps
WAN	Connected : 0, <input type="radio"/> WAN1 <input type="radio"/> WAN2 <input type="radio"/> WAN3 <input type="radio"/> WAN4
+ LAN	Connected : 0, <input type="radio"/> Port1 <input type="radio"/> Port2 <input type="radio"/> Port3 <input checked="" type="radio"/> Port4
+ WLAN	Connected : 0
+ WLAN5G	Connected : 0
USB	Connected : 0, <input type="radio"/> USB 1 0, <input type="radio"/> USB 2

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

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

I-5-4 GUI Map



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

GUI Map

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

I-5-5 Web Console



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

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

A screenshot of a web browser window displaying the Web Console interface. The browser's address bar shows "192.168.1.1/doc/console.htm" and the page title is "192.168.1.1/doc/console.htm". The main content area shows a command-line interface with the following text:

```
Type ? for command help
> ?

% Valid commands are:
adsl          vdsl          bpa           csm           ddns          dos
exit          internet      ip            ip6           ipf           log
ldap          tacacsplus    mngt          msubnet      object        port
portmuptime  ppa          prn           qos           quit          show
smb           srv           switch        sys           testmail     fs
upnp          usb           vigrbg        vlan          vpn           wan
hsportal      radius        local_8021x   wol           user          appqos
nand          apm           sfp           ethoam        ha           swm
backupmode
> █
```

I-5-6 Config Backup



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

Simply click the icon on the top of the main screen and a pop up dialog will appear.



Click Save to store the setting.

I-5-7 Logout



Click this icon to exit the web user interface.

I-5-8 Online Status

Online Status
Physical Connection
Virtual WAN

I-5-8-1 Physical Connection

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

Physical Connection for IPv4 Protocol

Online Status

Physical Connection						System Uptime: 0day 0:9:21
IPv4			IPv6			
LAN Status						
IP Address	TX Packets	RX Packets	Router Primary DNS:	Router Secondary DNS:		
192.168.1.1	1,554	1,092	8.8.8.8	8.8.4.4		
WAN 1 Status						>> Dial PPPoE
Enable	Line	Name	Mode	Up Time		
Yes	VDSL2		PPPoE	00:00:00		
IP	GW IP	TX Bytes	TX Rate(bps)	RX Bytes	RX Rate(bps)	
---	---	0 (B)	0	0 (B)	0	
WAN 2 Status						>> Renew
Enable	Line	Name	Mode	Up Time		
Yes	Ethernet		DHCP Client	00:00:00		
IP	GW IP	TX Bytes	TX Rate(bps)	RX Bytes	RX Rate(bps)	
---	---	0 (B)	0	0 (B)	0	
WAN 3 Status						
Enable	Line	Name	Mode	Up Time	Signal	
Yes	USB		---	00:00:00	-	
IP	GW IP	TX Bytes	TX Rate(bps)	RX Bytes	RX Rate(bps)	
---	---	0 (B)	0	0 (B)	0	
WAN 4 Status						
Enable	Line	Name	Mode	Up Time	Signal	
Yes	USB		---	00:00:00	-	
IP	GW IP	TX Bytes	TX Rate(bps)	RX Bytes	RX Rate(bps)	
---	---	0	0	0	0	
Line 1 Information (VDSL2 Firmware Version: 776D07_A/B/C)						
Profile	State	UP Speed	Down Speed	SNR Upstream	SNR Downstream	
	TRAINING	0 (Kbps)	0 (Kbps)	0 (dB)	0 (dB)	

Physical Connection for IPv6 Protocol

Physical Connection		System Uptime: 0day 20:58:19	
IPv4	IPv6		
LAN Status			
IP Address FE80::21D:AFF:FEF7:COF0/64 (Link)			
TX Packets 332	RX Packets 0	TX Bytes 25,904	RX Bytes 0
WAN1 IPv6 Status			
Enable No	Mode Offline	Up Time ---	Gateway IP ---
WAN2 IPv6 Status			
Enable No	Mode Offline	Up Time ---	Gateway IP ---
WAN3 IPv6 Status			
Enable No	Mode Offline	Up Time ---	Gateway IP ---
WAN4 IPv6 Status			
Enable No	Mode Offline	Up Time ---	Gateway IP ---

Detailed explanation (for IPv4) is shown below:

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

Item	Description
	interface.

Detailed explanation (for IPv6) is shown below:

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



Info

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

I-5-8-2 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**.

Quick Start Wizard

Enter login password

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

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

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. Then click **Next** for next step.

Quick Start Wizard

WAN Interface

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

WAN1, WAN2, WAN3 and WAN4 will bring up different configuration page. Refer to the following for detailed information.

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

WAN1 is specified for ADSL or VDSL2 connection.

Quick Start Wizard

WAN Interface

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

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
Display Name	Type a name to identify such WAN.
VLAN Tag insertion (VDSL2)/(ADSL)	<p>The settings configured in this field are available for WAN1 and WAN2.</p> <p>Enable - Enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the WAN while sending them out. Please type the tag value and specify the priority for the packets sending by WAN1.</p> <p>Disable - Disable the function of VLAN with tag.</p> <p>Tag value - Type the value as the VLAN ID number. The range is from 0 to 4095.</p> <p>Priority - Type the packet priority number for such VLAN. The range is from 0 to 7.</p>

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

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

Quick Start Wizard

Connect to Internet

WAN 1

Protocol PPPoE / PPPoA ▼

For ADSL Only:

Encapsulation PPPoE LLC/SNAP ▼

VPI 8 Auto detect

VCI 35

Fixed IP Yes No(Dynamic IP)

IP Address

Subnet Mask

Default Gateway

Primary DNS 8.8.8.8

Second DNS 8.8.4.4

< Back
Next >
Finish
Cancel

Available settings are explained as follows:

Item	Description
Protocol	<p>There are two modes offered for you to choose for WAN1 interface.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> PPPoE / PPPoA ▼ PPPoE / PPPoA MPoA / Static or Dynamic IP </div> <p>Choose PPPoE/PPPoA as the protocol.</p>
For ADSL Only	<p>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.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> PPPoE LLC/SNAP ▼ PPPoE LLC/SNAP PPPoE VC MUX PPPoA LLC/SNAP PPPoA VC MUX </div>
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

Set PPPoE / PPPoA

WAN 1	
Service Name (Optional)	<input type="text" value="CHT"/>
Username	<input type="text" value="84005755@hinet.net"/>
Password	<input type="password" value="*****"/>
Confirm Password	<input type="password" value="*****"/>

Available settings are explained as follows:

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

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN1
Physical Mode:	ADSL
VPI:	8
VCI:	35
Protocol / Encapsulation:	PPPoE / LLC
Fixed IP:	No
Primary DNS:	8.8.8.8
Secondary DNS:	8.8.4.4

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

Quick Start Wizard Setup OK!

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

MPoA / Static or Dynamic IP

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

Quick Start Wizard

Connect to Internet

WAN 1
Protocol: MPoA / Static or Dynamic IP

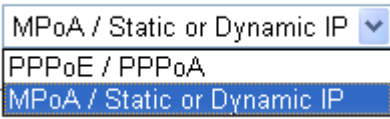
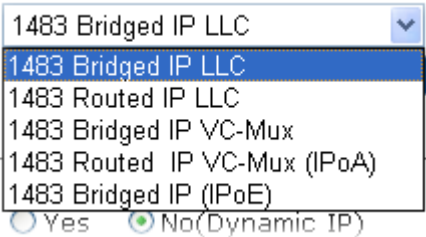
For ADSL Only:
Encapsulation: 1483 Bridged IP LLC
VPI: 0 (Auto detect)
VCI: 88

Fixed IP: Yes No(Dynamic IP)

IP Address:
Subnet Mask:
Default Gateway:
Primary DNS:
Second DNS:

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
Protocol	<p>There are two modes offered for you to choose for WAN1 interface.</p>  <p>Choose MPoA / Static or Dynamic IP as the protocol.</p>
For ADSL Only	<p>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.</p> 
Fixed IP	Click Yes to enable Fixed IP feature.
IP Address	Type the IP address if Fixed IP is enabled.
Subnet Mask	Type the subnet mask.
Default Gateway	Type the IP address as the default gateway.
Primary DNS	Type in the primary IP address for the router.

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

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

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN1
Physical Mode:	ADSL
VPI:	8
VCI:	35
Protocol / Encapsulation:	1483 Bridge LLC
Fixed IP:	No
Primary DNS:	8.8.8.8
Secondary DNS:	8.8.4.4

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.

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**.

Quick Start Wizard

WAN Interface

WAN Interface:	WAN2 ▼
Display Name:	<input type="text"/>
Physical Mode:	Ethernet ▼
Physical Type:	Auto negotiation ▼
VLAN Tag insertion	Disable ▼

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

1. 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.

Quick Start Wizard

Connect to Internet

WAN 2
Select one of the following Internet Access types provided by your ISP.

- PPPoE
- PPTP
- L2TP
- Static IP
- DHCP

2. Click **PPPoE** as the Internet Access Type. Then click **Next** to continue.

Quick Start Wizard

PPPoE Client Mode

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

Service Name (Optional)

Username

Password

Confirm Password

Available settings are explained as follows:

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

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.

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

Quick Start Wizard

Please confirm your settings:

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

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

- 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.

Ethernet WAN2 - PPTP/L2TP

1. 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.

Quick Start Wizard

Connect to Internet

WAN 2
Select one of the following Internet Access types provided by your ISP.

PPPoE
 PPTP
 L2TP
 Static IP
 DHCP

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

Quick Start Wizard

PPTP Client Mode

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

User Name

Password

Confirm Password

WAN IP Configuration

Obtain an IP address automatically
 Specify an IP address

IP Address

Subnet Mask

Gateway

Primary DNS

Second DNS

PPTP Server

Available settings are explained as follows:

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

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.

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

1. 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.

Quick Start Wizard

Connect to Internet

WAN 2
Select one of the following Internet Access types provided by your ISP.

PPPoE
 PPTP
 L2TP
 Static IP
 DHCP

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

Quick Start Wizard

Static IP Client Mode

WAN 2
Enter the Static IP configuration provided by your ISP.

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

Available settings are explained as follows:

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

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

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

Quick Start Wizard

Please confirm your settings:

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

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

- 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.

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.

Quick Start Wizard

Connect to Internet

WAN 2
Select one of the following Internet Access types provided by your ISP.

- PPPoE
- PPTP
- L2TP
- Static IP
- DHCP

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

Quick Start Wizard

DHCP Client Mode

WAN 2

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

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

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.

- 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.

Wireless (2.4G) WAN2 - Static IP

- 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.

Quick Start Wizard

Connect to Internet

WAN 2
Select one of the following Internet Access types.

Static IP
 DHCP

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

Quick Start Wizard

Static IP Client Mode

WAN 2
Enter the Static IP configuration.

WAN IP
 Subnet Mask
 Gateway

Available settings are explained as follows:

Item	Description
WAN IP	Type the IP address.

Subnet Mask	Type the subnet mask.
Gateway	Type the IP address of gateway.
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

Connect to Internet

WAN 2

Enter the AP configuration that router wants to connect.

SSID

MAC Address (Optional)

Channel :

Security Mode

Available settings are explained as follows:

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

- 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

Access Point List

Index	BSSID	Channel	RSSI	SSID	Authentication
<div style="text-align: center; margin-top: 50px;"> <input type="button" value="Scan"/> </div>					

AP's MAC address : : : : :

Universal Repeater

Note:

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

- Click the **Scan** button of the popup window and wait for a few seconds.

Wireless LAN >> Access Point Discovery

Access Point List

Index	BSSID	Channel	RSSI	SSID	Authentication
7	00:50:7F:19:38:80	11	47%	DrayTek-LAN-A	Mixed(WPA+WPA2)/PSK
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
10	00:1D:AA:BE:93:00	6	47%	DrayTek	Mixed(WPA+WPA2)/PSK
11	00:50:7F:62:98:E8	6	31%	DrayTek	NONE
12	02:1D:AA:7E:41:7C	3	7%	ap900_AT_2	Mixed(WPA+WPA2)/PSK
13	00:1D:AA:7E:41:7C	3	7%	ap900_AT_1	WPA2/PSK
14	02:1D:AA:7C:84:38	1	52%	AP810_111_2.4G-2	Mixed(WPA+WPA2)/PSK
15	00:1D:AA:7E:84:38	1	63%	AP810_111_2.4G-1	Mixed(WPA+WPA2)/PSK

AP's MAC address : : : : :

Universal Repeater

Note:

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

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

Quick Start Wizard

Connect to Internet

WAN 2

Enter the AP configuration that router wants to connect.

SSID	<input type="text" value="DrayTek"/>	<input type="button" value="AP Discovery"/>
MAC Address (Optional)	<input type="text" value="00 :1D :AA :BE :93 :00"/>	
Channel :	<input type="text" value="Channel 6, 2437MHz"/>	
Security Mode	<input type="text" value="WPA2/PSK"/>	
Encryption Mode	<input type="text" value="AES"/>	
Pass Phrase	<input type="text" value="12345678"/>	

< Back Next > Finish Cancel

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.

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN2
Physical Mode:	Wireless
Internet Access:	Static IP

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

< Back Next > Finish Cancel

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.

Quick Start Wizard

Connect to Internet

WAN 2
Select one of the following Internet Access types.

Static IP
 DHCP

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

Quick Start Wizard

Connect to Internet

WAN 2
Enter the AP configuration that router wants to connect.

SSID

MAC Address (Optional)

Channel :

Security Mode

Available settings are explained as follows:

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. <ul style="list-style-type: none"> ● Disable - The Router connects to the wireless AP

	<p>without any encryption mechanism.</p> <ul style="list-style-type: none"> ● 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.

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

Access Point List

Index	BSSID	Channel	RSSI	SSID	Authentication
<div style="border: 1px solid gray; width: 100%; height: 100%;"></div>					

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.

4. Click the Scan button of the popup window and wait for a few seconds.

Wireless LAN >> Access Point Discovery

Access Point List

Index	BSSID	Channel	RSSI	SSID	Authentication
11	00:50:7F:19:38:80	11	26%	900_ntp	NONE
12	06:1D:AA:9F:E9:48	11	78%	DrayTek-LAN-3	WPA2/PSK
13	00:50:7F:62:98:E8	6	23%	DrayTek	NONE
14	00:1D:AA:B9:66:70	6	68%	DrayTek	Mixed (WPA+WPA2) / PSK
15	00:1D:AA:BE:93:00	6	57%	DrayTek	Mixed (WPA+WPA2) / PSK
16	02:1D:AA:7E:41:7C	3	23%	ap900_AT_2	Mixed (WPA+WPA2) / PSK
17	00:1D:AA:7E:41:7C	3	18%	ap900_AT_1	WPA2/PSK
18	00:1D:AA:7E:84:38	1	57%	AP810_111_2.4G-1	Mixed (WPA+WPA2) / PSK
19	02:1D:AA:7C:84:38	1	68%	AP810_111_2.4G-2	Mixed (WPA+WPA2) / PSK

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.

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

Quick Start Wizard

Connect to Internet

WAN 2

Enter the AP configuration that router wants to connect.

SSID	<input type="text" value="DrayTek"/>	<input type="button" value="AP Discovery"/>
MAC Address (Optional)	<input type="text" value="00 :50 :7F :62 :98 :E8"/>	
Channel :	<input type="text" value="Channel 6, 2437MHz"/>	
Security Mode	<input type="text" value="Disable"/>	

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.

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN2
Physical Mode:	Wireless 2.4G
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)

WAN3/WAN4 is dedicated to physical mode in USB.

1. Choose WAN3/WAN4 as WAN Interface.

Quick Start Wizard

WAN Interface

WAN Interface:	WAN4 ▼
Display Name:	<input type="text"/>
Physical Mode:	USB

< Back Next > Finish Cancel

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

Quick Start Wizard

Connect to Internet

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

< Back Next > Finish Cancel

Available settings are explained as follows:

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

	<p>the string you can set is 47 characters.</p> <p>APN Name - APN means Access Point Name which is provided and required by some ISPs. Type the name and click Apply.</p>
3G/4G USB Modem (DHCP mode)	<p>SIM Pin code - Type PIN code of the SIM card that will be used to access Internet.</p> <p>Network Mode - Force Vigor router to connect Internet with the mode specified here. If you choose 4G/3G/2G as network mode, the router will choose a suitable one according to the actual wireless signal automatically.</p> <p>APN Name - APN means Access Point Name which is provided and required by some ISPs.</p>

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

Quick Start Wizard

Please confirm your settings:

WAN Interface:	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.

- 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-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.

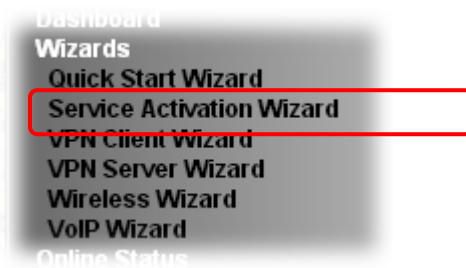
Now, follow the steps listed below to activate WCF feature for your router.



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. You can activate the Web content filter services and/or APPE enforcement service and / or DDNS service at the same time or individually. When you finish the selection, please click Next.

Service Activation Wizard

Select the service type that you want to activate

Activation Date : 2017-10-12

Web Content Filter(WCF) Service :

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

APP Enforcement(APPE) Service :

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

Dynamic DNS(DDNS) Service :

DT-DDNS [License Agreement](#)
This is a Dynamic Domain Name Service that is provided by DrayTek company. It is a free service will expire 1 year after activation. You may re-active the service after expiry.
Domain Name : .drayddns.com

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

Next >

Cancel



Info

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

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

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

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

Service Activation Wizard

Please confirm your settings

Service Type : Trial version

Service Activated : Web Content Filter (BPjM)
APP Enforcement (DT-APPE)
Dynamic DNS (2017101210301001.drayddns.com)

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

< Back **Activate** Cancel



Info

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

4. Now, the web page will display the service that you have activated according to your selection(s).

DrayTek Service Activation

Service Name	Start Date	Expire Date	Status
Web Content filter	2017-10-12	2018-10-12	BPjM
APP Enforcement	2017-10-12	2018-10-12	DT-APPE
DDNS	2017-10-12	2018-10-12	DT-DDNS

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

Copyright © DrayTek Corp. All Rights Reserved.

I-8 Registering Vigor Router

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

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

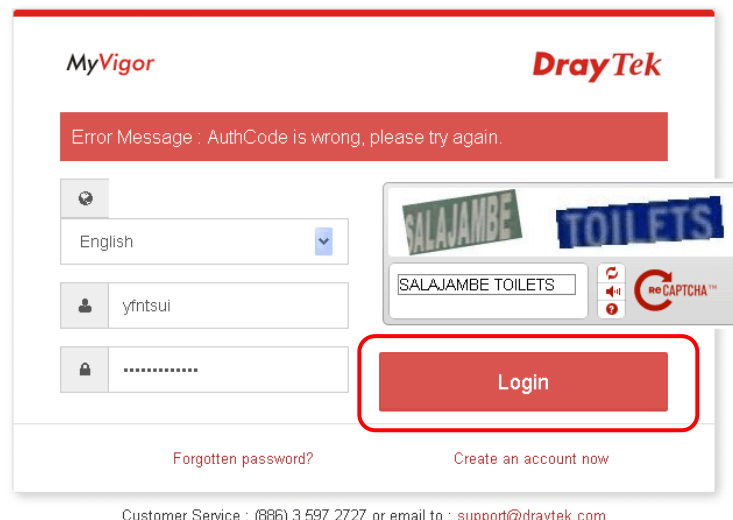


- 2 Click Support Area>>Production Registration from the home page.



Support Area
Product Registration

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



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. 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). Click Add.

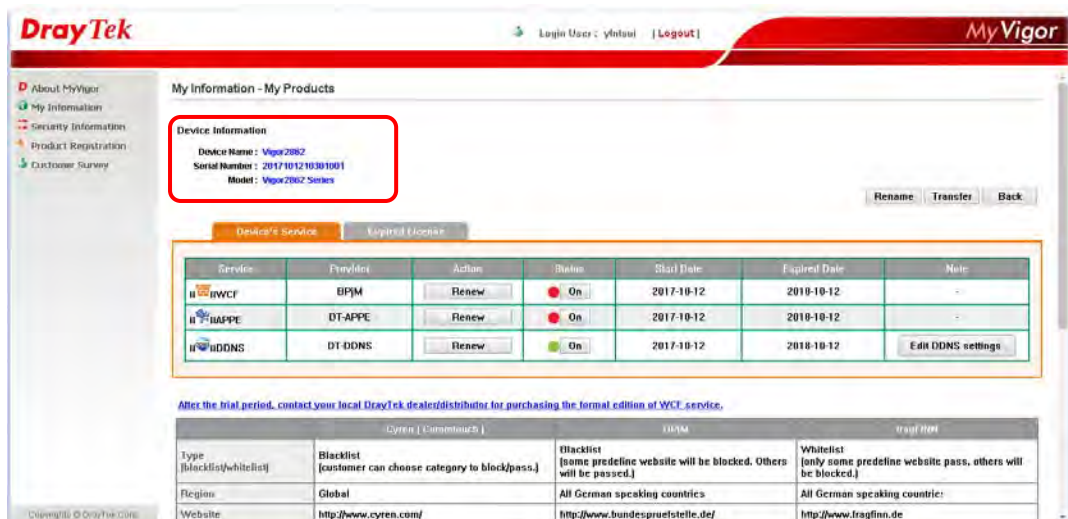


- When the following page appears, your router information has been added to the database.

Your device has been successfully added to the database.



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



Part II Connectivity



WAN

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



LAN

It means local area network. Private IP will be used in LAN. Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.



NAT

When the data flow passing through, the Network Address Translation (NAT) function of the router will dedicate to translate public/private addresses, and the packets will be delivered to the correct host PC in the local area network.



Applications

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



Routing

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, Vigor2862 adds the function of 3G/4G network connection for such purpose. By connecting 3G/4G USB Modem to the USB port of Vigor2862, it can support LTE/HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G/4G standard (HSUPA, etc). Vigor2862n 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 Vigor2862n series.



After connecting into the router, 3G/4G USB Modem will be regarded as the WAN3/WAN4 port. However, the original WAN1 and WAN2 still can be used and Load-Balance can be done in the router. Besides, 3G/4G USB Modem in WAN3/WAN4 also can be used as backup device. Therefore, when WAN1 and WAN2 are not available, the router will use 3.5G for supporting automatically. The supported 3G/4G USB Modem will be listed on DrayTek web site. Please visit www.draytek.com for more detailed information.

Web User Interface

II-1-1 General Setup

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

WAN >> General Setup

Load Balance Mode:

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

Note:

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

OK

Available settings are explained as follows:

Item	Description
Load Balance Mode	<p>This option is available for multiple-WAN for getting enough bandwidth for each WAN port. If you know the practical bandwidth for your WAN interface, please choose the setting of According to Line Speed. Otherwise, please choose Auto Weight to let the router reach the best load balance.</p> <p>IP Based - The same source / destination IP pair will select the same WAN interface as policy. It is the default setting.</p> <p>Sesseion Based- All of the WAN interfaces will be used (as out-going WAN) for passing through new sessions to get better transmission speed. Though good speed test result for throughput might be reached; however, some web site may not open smoothly, especially the site need authentication, e.g., FTP.</p> <p>If you have no strong demand about speed test result, keep default settings as IP based.</p>
Index	Click the WAN interface link under Index to access into the WAN configuration page.

Enable	V means such WAN interface is enabled and ready to be used.
Physical Mode / Type	Display the physical mode and physical type of such WAN interface.
Line Speed(Kbps) DownLink/UpLink	Display the downstream and upstream rate of such WAN interface.
Active Mode	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 >> General Setup

WAN 1

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

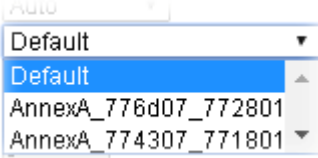

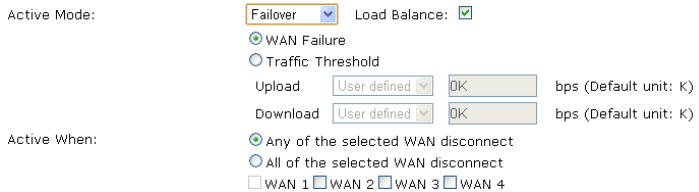
Note:

1. The line speed setting of WAN interface is available only when According to Line Speed is selected as the Load Balance Mode.
2. Service and customer tag settings are depending on network environment.

OK Cancel

Available settings are explained as follows:

Item	Description
Enable	Choose Yes to invoke the settings for this WAN interface. Choose No to disable the settings for this WAN interface.
Display Name	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.
DSL Modem Code	<p>Choose the correct DSL modem code for ensuring the network connection.</p>  <p>If you have no idea about the selection, simply choose Default or contact the dealer for assistance.</p>
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.
Active Mode	<p>Choose Always On to make the WAN1 connection being activated always.</p>  <p>Load Balance: Check this box to enable auto load balance function for such WAN interface.</p> <p>When the data traffic is large, the WAN interface with the function enabled will balance the data transmission automatically among all of the WAN interfaces in connection status.</p> <p>Failover - Choose it to make the WAN connection as a backup connection.</p> <ul style="list-style-type: none"> ● WAN Failure - When the active WAN failed, such WAN will be activated as the main network connection. ● Traffic Threshold - When the data traffic of active WAN reaches the traffic threshold (specified here), the failover WAN will be enabled automatically to share the overloaded data traffic.
Active When	<p>If you choose Failover as the Active Mode, Active When will appear. Please specify which WAN will be the Backup interface.</p>  <p>Any of the selected WAN disconnect - Such backup WAN will be activated when any master WAN interface disconnects.</p> <p>All of the selected WAN disconnect - Such backup WAN will be activated only when all master WAN interfaces disconnect.</p>

VLAN Tag insertion (ADSL/VDSL)	<p>Such feature is offered to the user with the environment supporting IEEE_802.1ad. In which, service is used for outer tag; customer is used for inner tag.</p> <p>Enable - Enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the WAN while sending them out. Please type the tag value and specify the priority for the packets sending by WAN1.</p> <p>Disable - Disable the function of VLAN with tag.</p> <p>Tag value - Type the value as the VLAN ID number. The range is form 0 to 4095.</p> <p>Priority - Type the packet priority number for such VLAN. The range is from 0 to 7.</p>
---------------------------------------	---

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

II-1-1-2 WAN2 (Ethernet)/(Wireless 2.4G/5G)

WAN2 can be configured for physical mode of Ethernet or Wireless 2.4/5G.

WAN >> General Setup

WAN 2

Enable:	Yes ▾	
Display Name:	<input type="text"/>	
Physical Mode:	Ethernet ▾	
Physical Type:	Auto negotiation ▾	
Line Speed(Kbps):	<input type="text"/>	
DownLink	<input type="text"/>	
UpLink	<input type="text"/>	
Active Mode:	Failover ▾	Load Balance: <input checked="" type="checkbox"/>
	<input type="radio"/> WAN Failure	
	<input type="radio"/> Traffic Threshold	
	Upload	User defined ▾ <input type="text"/> 0K bps (Default unit: K)
	Download	User defined ▾ <input type="text"/> 0K bps (Default unit: K)
Active When:	<input type="radio"/> Any of the selected WAN disconnect	
	<input type="radio"/> All of the selected WAN disconnect	
	<input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input type="checkbox"/> WAN 4	
VLAN Tag insertion	Service	Customer
	Disable ▾	Disable ▾
	Tag value	Tag value
	<input type="text"/>	<input type="text"/>
	(0~4095)	(0~4095)
	Priority	Priority
	<input type="text"/>	<input type="text"/>
	(0~7)	(0~7)

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.Service and customer tag settings are depending on network environment.

OK Cancel

Or,

WAN >> General Setup

WAN 2

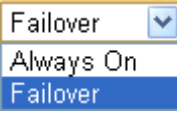
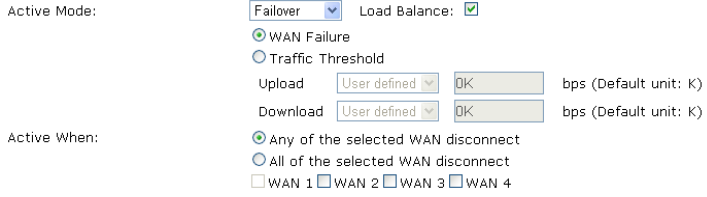
Enable:	Yes ▾	
Display Name:	<input type="text"/>	
Physical Mode:	Wireless 2.4G ▾	
Line Speed(Kbps):	<input type="text"/>	
DownLink	<input type="text"/>	
UpLink	<input type="text"/>	
Active Mode:	Failover ▾	Load Balance: <input checked="" type="checkbox"/>
	<input type="radio"/> WAN Failure	
	<input type="radio"/> Traffic Threshold	
	Upload	User defined ▾ <input type="text"/> 0K bps (Default unit: K)
	Download	User defined ▾ <input type="text"/> 0K bps (Default unit: K)
Active When:	<input type="radio"/> Any of the selected WAN disconnect	
	<input type="radio"/> All of the selected WAN disconnect	
	<input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input type="checkbox"/> 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.

OK Cancel

Available settings are explained as follows:

Item	Description
Enable	Choose Yes to invoke the settings for this WAN interface. Choose No to disable the settings for this WAN interface.
Display Name	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.
Line Speed (Kbps)	If you choose According to Line Speed as the Load Balance Mode , please type the line speed for downloading and uploading for such WAN interface. The unit is kbps.
Active Mode	<p>Choose Always On to make the WAN2 connection being activated always.</p>  <p>Load Balance: Check this box to enable auto load balance function for such WAN interface.</p> <p>When the data traffic is large, the WAN interface with the function enabled will balance the data transmission automatically among all of the WAN interfaces in connection status.</p> <p>Failover - Choose it to make the WAN connection as a backup connection.</p> <ul style="list-style-type: none"> ● WAN Failure - When the active WAN failed, such WAN will be activated as the main network connection. ● Traffic Threshold - When the data traffic of active WAN reaches the traffic threshold (specified here), the failover WAN will be enabled automatically to share the overloaded data traffic.
Active When	<p>If you choose Failover as the Active Mode, Active When will appear. Please specify which WAN will be the Backup interface.</p>  <p>Any of the selected WAN disconnect - Such backup WAN will be activated when any master WAN interface disconnects.</p> <p>All of the selected WAN disconnect - Such backup WAN will be activated only when all master WAN interfaces disconnect.</p> <p>Check boxes for WAN1 to WAN4 - Specify the WAN interface by checking the WAN box.</p>
VLAN Tag insertion	<p>Such feature is offered to the user with the environment supporting IEEE_802.1ad. In which, service is used for outer tag; customer is used for inner tag.</p> <p>It is available only when Ethernet is selected as Physical Mode.</p>

	<p>Enable - Enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the WAN while sending them out. Please type the tag value and specify the priority for the packets sending by WAN1.</p> <p>Disable - Disable the function of VLAN with tag.</p> <p>Tag value - Type the value as the VLAN ID number. The range is form 0 to 4095.</p> <p>Priority - Type the packet priority number for such VLAN. The range is from 0 to 7.</p>
--	---

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

WAN 3


Enable:	Yes ▾
Display Name:	<input type="text"/>
Physical Mode:	USB
Line Speed(Kbps):	
DownLink	<input type="text" value="0"/>
UpLink	<input type="text" value="0"/>
Active Mode:	Failover ▾ Load Balance: <input checked="" type="checkbox"/>
	<input checked="" type="radio"/> WAN Failure <input type="radio"/> Traffic Threshold
	Upload <input type="text" value="User defined"/> <input type="text" value="0K"/> bps (Default unit: K)
	Download <input type="text" value="User defined"/> <input type="text" value="0K"/> bps (Default unit: K)
Active When:	<input checked="" type="radio"/> Any of the selected WAN disconnect <input type="radio"/> All of the selected WAN disconnect <input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input type="checkbox"/> 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.

OK Cancel

Available settings are explained as follows:

Item	Description
Enable	Choose Yes to invoke the settings for this WAN interface. Choose No to disable the settings for this WAN interface.
Display Name	Type the description for such WAN interface.
Physical Mode	Display the physical mode of such WAN interface.
Line Speed (Kbps)	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 WAN2 connection being activated always.  Load Balance: Check this box to enable auto load balance function for such WAN interface.

	<p>When the data traffic is large, the WAN interface with the function enabled will balance the data transmission automatically among all of the WAN interfaces in connection status.</p> <p>Failover - Choose it to make the WAN connection as a backup connection.</p> <ul style="list-style-type: none"> ● WAN Failure - When the active WAN failed, such WAN will be activated as the main network connection. ● Traffic Threshold - When the data traffic of active WAN reaches the traffic threshold (specified here), the failover WAN will be enabled automatically to share the overloaded data traffic.
<p>Active When</p>	<p>If you choose Failover as the Active Mode, Active When will appear. Please specify which WAN will be the Backup interface.</p> <p>Active Mode: Failover Load Balance: <input checked="" type="checkbox"/></p> <p><input checked="" type="radio"/> WAN Failure <input type="radio"/> Traffic Threshold</p> <p>Upload User defined OK bps (Default unit: K) Download User defined OK bps (Default unit: K)</p> <p>Active When:</p> <p><input checked="" type="radio"/> Any of the selected WAN disconnect <input type="radio"/> All of the selected WAN disconnect</p> <p><input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input type="checkbox"/> WAN 4</p> <p>Any of the selected WAN disconnect - Such backup WAN will be activated when any master WAN interface disconnects.</p> <p>All of the selected WAN disconnect - Such backup WAN will be activated only when all master WAN interfaces disconnect.</p>

After 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 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	Details Page	IPv6
WAN1		ADSL / VDSL2	None	Details Page	IPv6
WAN2		Ethernet	None	Details Page	IPv6
WAN3		USB	PPPoE / PPPoA	Details Page	IPv6
WAN4		USB	MPoA / Static or Dynamic IP	Details Page	IPv6

Note:

- 1.Device on USB port 1 applies WAN3 configuration.
- 2.Device on USB port 2 applies WAN4 configuration.

Advanced You can configure DHCP client options here.

Access Mode for Ethernet / USB,

Ethernet	None	USB	None
USB	None	USB	None
USB	PPPoE	1 applies WAN3 c	3G/4G USB Modem(PPP mode)
	Static or Dynamic IP	2 applies WAN4 c	3G/4G USB Modem(DHCP mode)
	PPTP/L2TP		

Available settings are explained as follows:

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 /WAN4 (3G/4G USB Modem) accrodging 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.

WAN >> Internet Access

DHCP Client Options Status

Enable	Interface	Option	Type	Data
Options List				
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Enable:

Interface: All WAN1 WAN2 WAN3 WAN4 WAN5 WAN6 WAN7

Option Number:

Data Type: ASCII Character (EX: Option:18, Data:/path)
 Hexadecimal Digit (EX: Option:18, Data:2f70617468)
 Address List (EX: Option:44, Data:172.16.2.10,172.16.2.20...)

Data:

Note:

1. Option 12 is reserved. You cannot configure it here, but you can configure it in "Router Name" field of "WAN >> Internet Access >> Details Page".
2. Option 55 is reserved and configured with value 1, 3, 6, 15 and 212, also 33 and 121 for some models.
3. Configuring option 61 here will override the setting in "WAN >> Internet Access" page's DHCP Client Identifier field.

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.

Data Type - 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

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.

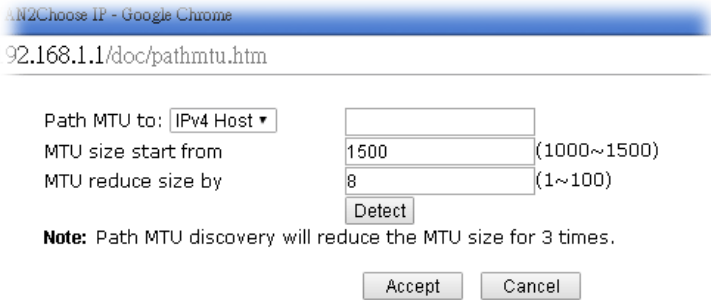
WAN >> Internet Access

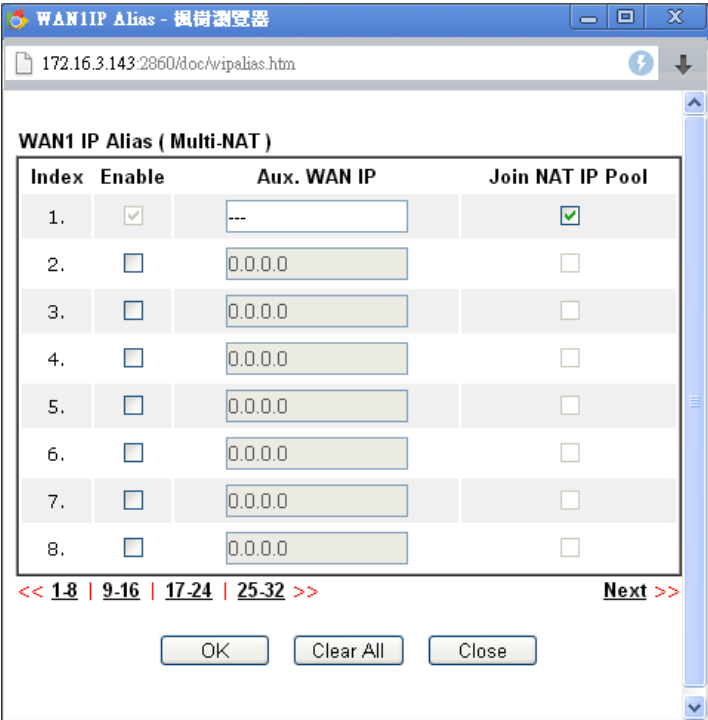
WAN 1

PPPoE / PPPoA	MPoA / Static or Dynamic IP	IPv6
<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Modem Settings (for ADSL only) Multi-PVC channel: Channel 1 VPI: 0 VCI: 33 Encapsulating Type: LLC/SNAP Protocol: PPPoE Modulation: Multimode		
PPPoE Pass-through <input type="checkbox"/> For Wired LAN ² <input type="checkbox"/> For Wireless LAN		
WAN Connection Detection Mode: ARP Detect		
MTU Path MTU Discovery: 1492 (Max:1500) Detect		
ISP Access Setup Service Name ¹ : Username: Password: <input type="checkbox"/> Separate Account for ADSL PPP Authentication: PAP or CHAP IP Address From ISP WAN IP Alias Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address:		
<input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: 00 · 1D · AA · BC · 4D · C1		
Index(1-15) in Schedule Setup: => , , ,		

Available settings are explained as follows:

Item	Description
Enable/Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
Modem Setting (for ADSL only)	It is not necessary to configure settings in these fields for modem settings are prepared for ADSL only.
PPPoE Pass-through	<p>The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction.</p> <p>For Wired LAN - If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet.</p> <p>For Wireless LAN - 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 into Internet.</p> <p>Note: To have PPPoA Pass-through, please choose PPPoA protocol and check the box(es) here. The router will behave like a modem which only serves the PPPoE client on the LAN. That's, the router will offer PPPoA dial-up connection.</p>
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.

	<p>Mode - Choose ARP Detect or Ping Detect for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items.</p> <ul style="list-style-type: none"> ● Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation. ● Ping Interval - 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.
<p>MTU</p>	<p>It means Max Transmit Unit for packet.</p> <p>Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path.</p> <p>Click Detect to open the following dialog.</p>  <ul style="list-style-type: none"> ● Path MTU to - Type the IP address as the specific transmit path. ● MTU size start from - Determine the starting point value of the packet. ● MTU reduce size by- It determines the decreasing size of MTU value. For example, the number specified in this field is "8". The maximum MTU size is "1500". After clicking the "detect" button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically. ● Detect - Click it to detect a suitable MTU value ● Accept- After clicking it, the detected value will be displayed in the field of MTU.
<p>ISP Access Setup</p>	<p>Enter your allocated username, password and authentication parameters according to the information provided by your ISP.</p> <p>Username - Type in the username provided by ISP in this field.</p> <p>Password - Type in the password provided by ISP in this field.</p> <p>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</p>

	<p>account and password for ADSL connection by checking this box. If it is checked, the system will ask you to type another group of account and password additionally.</p> <p>PPP Authentication - Select PAP only or PAP or CHAP for PPP.</p>
<p>IP Address From ISP</p>	<p>Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function.</p> <p>WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.</p>  <p>Fixed IP - Click Yes to use this function and type in a fixed IP address in the box of Fixed IP Address.</p> <p>Default MAC Address - You can use Default MAC Address or specify another MAC address by typing on the boxes of MAC Address for the router.</p> <p>Specify a MAC Address - Type the MAC address for the router manually.</p> <p>Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Applications >> Schedule web page and you can use the number that you have set in that web page.</p>

After 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 >> Internet Access

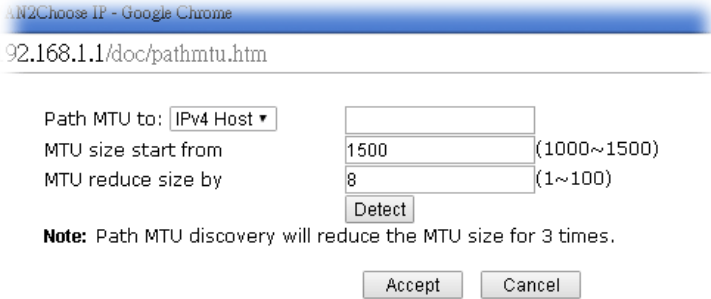
WAN 1

PPPoE / PPPoA	MPoA / Static or Dynamic IP	IPv6
<input type="radio"/> Enable <input checked="" type="radio"/> Disable		WAN IP Network Settings WAN IP Alias
Modem Settings (for ADSL only) Multi-PVC channel: Channel 2 Encapsulation: 1483 Bridged IP LLC VPI: 0 VCI: 88 Modulation: Multimode		<input type="radio"/> Obtain an IP address automatically Router Name: drayrouter * Domain Name: * <input type="checkbox"/> DHCP Client Identifier * Username: <input type="text"/> Password: <input type="text"/> <input checked="" type="radio"/> Specify an IP address IP Address: <input type="text"/> Subnet Mask: <input type="text"/> Gateway IP Address: <input type="text"/>
WAN Connection Detection Mode: ARP Detect		<input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: 00 1D AA BC 4D C1
MTU Path MTU Discovery: Detect (Max: 1500)		DNS Server IP Address Primary IP Address: 8.8.8.8 Secondary IP Address: 8.8.4.4
RIP Protocol <input type="checkbox"/> Enable RIP		
Bridge Mode <input type="checkbox"/> Enable Bridge Mode Bridge Subnet: LAN 1		

*: Required for some ISPs

Available settings are explained as follows:

Item	Description
Enable/Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
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. <ul style="list-style-type: none"> ● Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● Ping Gateway IP - If you choose Ping Detect as detection

	<p>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.</p> <ul style="list-style-type: none"> ● 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.
<p>MTU</p>	<p>It means Max Transmit Unit for packet.</p> <p>Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path.</p> <p>Click Detect to open the following dialog.</p>  <ul style="list-style-type: none"> ● Path MTU to - Type the IP address as the specific transmit path. ● MTU size start from - Determine the starting point value of the packet. Default setting is 1500. ● MTU reduce size by- It determines the decreasing size of MTU value. For example, the number specified in this field is "8". The maximum MTU size is "1500". After clicking the "detect" button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically. ● Detect - Click it to detect a suitable MTU value ● Accept- After clicking it, the detected value will be displayed in the field of MTU.
<p>RIP Protocol</p>	<p>Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.</p>
<p>Bridge Mode</p>	<p>Enable Bridge Mode - If the function is enabled, the router will work as a bridge modem.</p> <p>Enable Firewall - It is available when Bridge Mode is enabled. When both Bridge Mode and Firewall check boxes are enabled, the settings configured (user profiles) under User Management will be ignored. And all of the filter rules defined and enabled in Firewall menu will be activated.</p> <p>Bridge Subnet - Make a bridge between the selected LAN subnet and such WAN interface.</p>
<p>WAN IP Network Settings</p>	<p>This group allows you to obtain an IP address automatically and allows you type in IP address manually.</p> <p>WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use</p>

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*

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

WAN >> Internet Access

WAN 1

PPPoE / PPPoA	MPoA / Static or Dynamic IP	IPv6
<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Modem Settings (for ADSL only) Multi-PVC channel: Channel 1 VPI: 8 VCI: 35 Encapsulating Type: VC MUX Protocol: PPPoA Modulation: Multimode		
PPPoE Pass-through <input type="checkbox"/> For Wired LAN ² <input type="checkbox"/> For Wireless LAN		
WAN Connection Detection Mode: ARP Detect		
MTU Path MTU Discovery: 1500 (Max:1500) Detect		
		ISP Access Setup Service Name ¹ : Username: Password: <input type="checkbox"/> Separate Account for ADSL PPP Authentication: PAP or CHAP IP Address From ISP WAN IP Alias Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address:
		<input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: 00 · 1D · AA · F7 · C0 · F1
		Index(1-15) in Schedule Setup: => , , ,

Note:

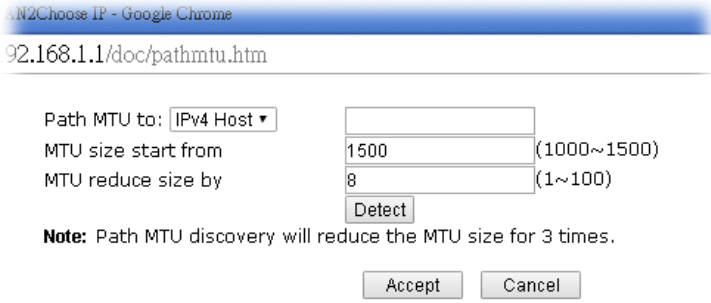
- 1: (Optional) Required for some ISPs. Leave blank if in doubt because the connection request might be denied if "Service Name" is incorrect.
- 2: If this box is checked while using the PPPoA protocol, the router will behave like a modem which only serves the PPPoE client on the LAN.

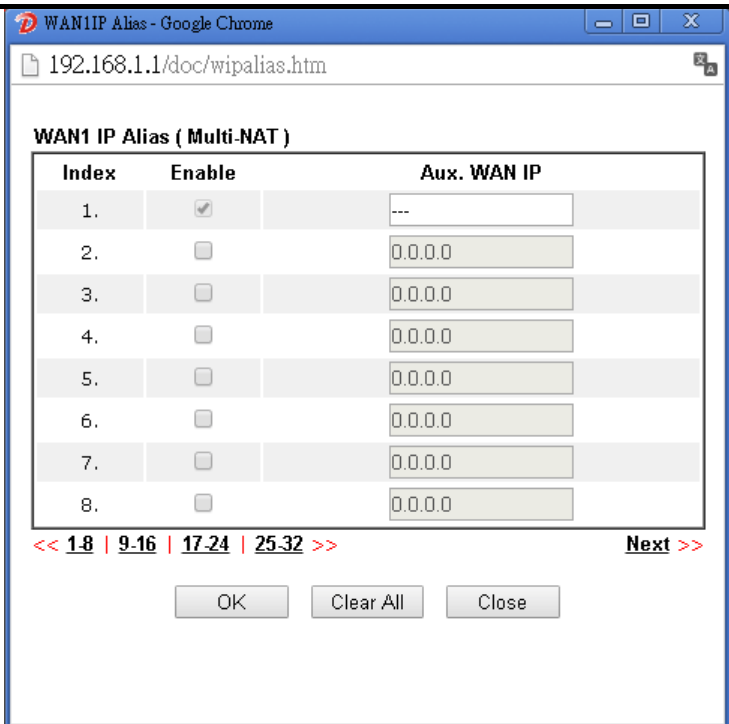
OK Cancel

Available settings are explained as follows:

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

	Modulation <div style="border: 1px solid black; padding: 2px; margin-left: 20px;"> Multimode ▼ T1.413 G.Lite G.DMT ADSL2(G.992.3) ADSL2 annex M ADSL2+(G.992.5) ADSL2+ annex M Multimode </div>
PPPoE Pass-through	<p>The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction.</p> <p>For Wired LAN - If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet.</p> <p>For Wireless LAN - 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 into Internet.</p> <p>Note: To have PPPoA Pass-through, please choose PPPoA protocol and check the box(es) here. The router will behave like a modem which only serves the PPPoE client on the LAN. That's, the router will offer PPPoA dial-up connection.</p>
WAN Connection Detection	<p>Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.</p> <p>Mode - Choose ARP Detect or Ping Detect for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items.</p> <ul style="list-style-type: none"> ● Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation. ● Ping Interval - Type the interval for the system to execute the PING operation. ● Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
MTU	<p>It means Max Transmit Unit for packet.</p> <p>Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path.</p> <p>Click Detect to open the following dialog.</p>

	 <ul style="list-style-type: none"> ● Path MTU to - Type the IP address as the specific transmit path. ● MTU size start from - Determine the starting point value of the packet. Default setting is 1500. ● MTU reduce size by- It determines the decreasing size of MTU value. For example, the number specified in this field is "8". The maximum MTU size is "1500". After clicking the "detect" button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically. ● Detect - Click it to detect a suitable MTU value ● Accept- After clicking it, the detected value will be displayed in the field of MTU.
<p>ISP Access Setup</p>	<p>Enter your allocated username, password and authentication parameters according to the information provided by your ISP.</p> <p>Username - Type in the username provided by ISP in this field.</p> <p>Password - Type in the password provided by ISP in this field.</p> <p>Separate Account for ADSL - In default, WAN1 supports VDSL2/ADSL and uses the same PPPoE account and password for connection. If required, you can configure another account and password for ADSL connection by checking this box. If it is checked, the system will ask you to type another group of account and password additionally.</p> <p>PPP Authentication - Select PAP only or PAP or CHAP for PPP.</p> <p>Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action.</p>
<p>IP Address From ISP</p>	<p>Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function.</p> <p>WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.</p>



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.

WAN 1

Enable Disable

Modem Settings (for ADSL only)

Multi-PVC channel: Channel 2

Encapsulation: 1483 Bridged IP LLC

VPI: 0

VCI: 88

Modulation: Multimode

WAN Connection Detection

Mode: ARP Detect

MTU 1492 (Max: 1500)

Path MTU Discovery: Detect

RIP Protocol

Enable RIP

Bridge Mode

Enable Bridge Mode

Enable Full Bridge Mode

Bridge Subnet: LAN 1

WAN IP Network Settings WAN IP Alias

Obtain an IP address automatically

Router Name: Vigor*

Domain Name: *

DHCP Client Identifier *

Username: []

Password: []

Specify an IP address

IP Address: []

Subnet Mask: []

Gateway IP Address: []

Default MAC Address

Specify a MAC Address

MAC Address: 00 . 1D . AA : 5D . C9 . E1

DNS Server IP Address

Primary IP Address: 8.8.8.8

Secondary IP Address: 8.8.4.4

*: Required for some ISPs

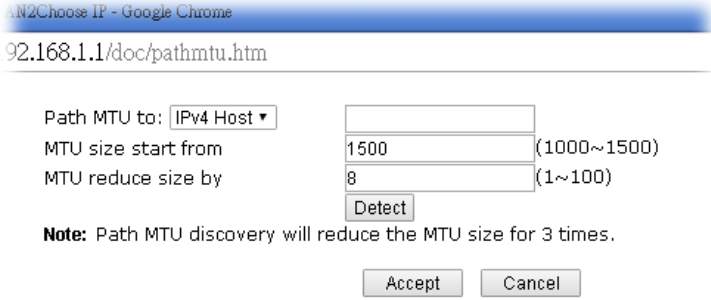
Note:

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.
3. If both Bridge Mode and Firewall are enabled, the settings under User Management will be ignored.
4. Full Bridge Mode supports forwarding packets with VLAN tags.
5. Full Bridge Mode doesn't support wireless LAN.

OK Cancel

Available settings are explained as follows:

Item	Description
Enable/Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
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. Encapsulation - 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 Always on , 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

	<p>settings for the following items.</p> <ul style="list-style-type: none"> ● Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation. ● Ping Interval - Type the interval for the system to execute the PING operation. ● Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
<p>MTU</p>	<p>It means Max Transmit Unit for packet.</p> <p>Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path.</p> <p>Click Detect to open the following dialog.</p>  <ul style="list-style-type: none"> ● Path MTU to - Type the IP address as the specific transmit path. ● MTU size start from - Determine the starting point value of the packet. Default setting is 1500. ● MTU reduce size by - It determines the decreasing size of MTU value. For example, the number specified in this field is "8". The maximum MTU size is "1500". After clicking the "detect" button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically. ● Detect - Click it to detect a suitable MTU value ● Accept - After clicking it, the detected value will be displayed in the field of MTU.
<p>RIP Protocol</p>	<p>Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.</p>
<p>Bridge Mode</p>	<p>Enable Bridge Mode - If the function is enabled, the router will work as a bridge modem. Yet, the incoming packets with VLAN tags will be discarded.</p> <p>Enable Full Bridge Mode - If the function is enabled, the router will work as a bridge modem which is able to forward incoming packets with VLAN tags.</p> <p>Enable Firewall - It is available when Bridge Mode is enabled. When both Bridge Mode and Firewall check boxes</p>

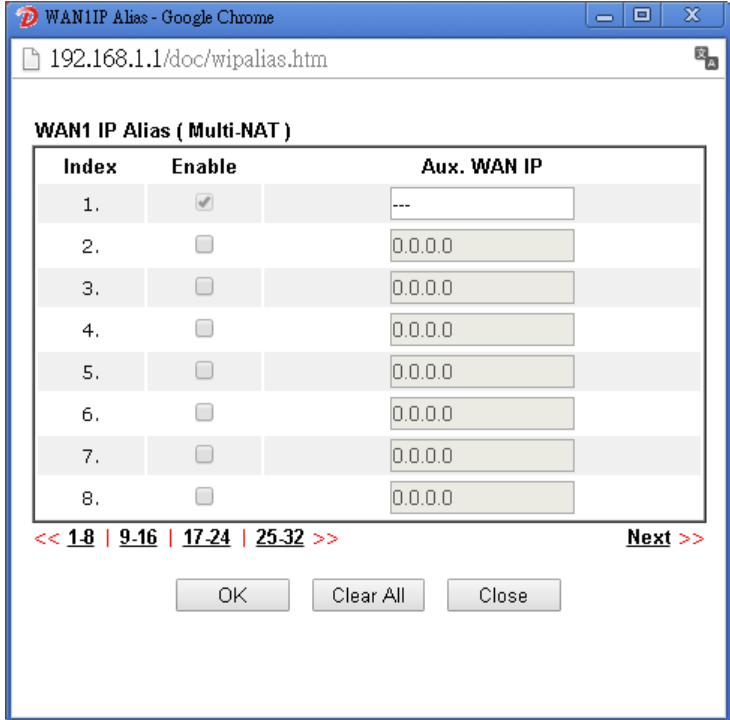
are enabled, the settings configured (user profiles) under User Management will be ignored. And all of the filter rules defined and enabled in Firewall menu will be activated.

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 -

- **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.

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

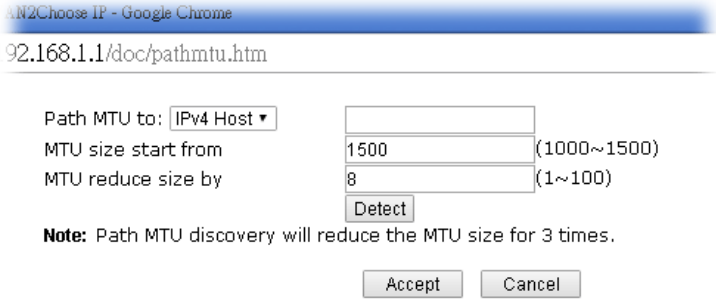
WAN 2

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
ISP Access Setup Service Name (Optional) <input type="text"/> Username <input type="text"/> Password <input type="text"/> Index(1-15) in Schedule Setup: => <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>		PPP/MP Setup PPP Authentication <input type="text" value="PAP or CHAP"/> <input type="text" value="PAP or CHAP"/> Idle Timeout <input type="text" value="-1"/> second(s)	
WAN Connection Detection Mode <input type="text" value="ARP Detect"/>		IP Address Assignment Method (IPCP) <input type="text" value="WAN IP Alias"/> Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address <input type="text"/>	
MTU <input type="text" value="1500"/> (Max:1500) Path MTU Discovery <input type="text" value="Detect"/>		<input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: <input type="text" value="00"/> <input type="text" value="1D"/> <input type="text" value="AA"/> <input type="text" value:f7"=""/> <input type="text" value:c0"=""/> <input type="text" value:f2"=""/>	
TTL Change the TTL value <input type="text" value="Enable"/>			

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

Available settings are explained as follows:

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

	<p>characters.</p> <p>Password - Type in the password provided by ISP in this field. The maximum length of the password you can set is 62 characters.</p> <p>Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page.</p>
<p>WAN Connection Detection</p>	<p>Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.</p> <p>Mode - Choose ARP Detect or Ping Detect for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items.</p> <ul style="list-style-type: none"> ● Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation. ● Ping Interval - 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.
<p>MTU</p>	<p>It means Max Transmit Unit for packet.</p> <p>Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path.</p> <p>Click Detect to open the following dialog.</p>  <ul style="list-style-type: none"> ● Path MTU to - Type the IP address as the specific transmit path. ● MTU size start from - Determine the starting point value of the packet. Default setting is 1500. ● MTU reduce size by - It determines the decreasing size of MTU value. For example, the number specified in this field is "8". The maximum MTU size is "1500". After clicking the "detect" button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically. ● Detect - Click it to detect a suitable MTU value ● Accept - After clicking it, the detected value will be

	displayed in the field of MTU.
TTL	<p>Change the TTL value - Enable or disable the TTL (Time to Live) for a packet transmitted through Vigor router.</p> <p>Enable - TTL value will be reduced (-1) when it passes through Vigor router. It will cause the client, accessing Internet through Vigor router, be blocked by certain ISP when TTL value becomes "0".</p> <p>Disable - TTL value will not be reduced. Then, when a packet passes through Vigor router, it will not be cancelled. That is, the client who sends out the packet will not be blocked by ISP.</p>
PPP/MP Setup	<p>PPP Authentication - Select PAP only or PAP or CHAP for PPP.</p> <p>Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action.</p>
IP Address Assignment Method (IPCP)	<p>Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function.</p> <p>WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 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.</p> <p>Fixed IP - Click Yes to use this function and type in a fixed IP address in the box of Fixed IP Address.</p> <p>Default MAC Address - You can use Default MAC Address or specify another MAC address by typing on the boxes of MAC Address for the router.</p> <p>Specify a MAC Address - Type the MAC address for the router manually.</p>

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

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

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Keep WAN Connection <input type="checkbox"/> Enable PING to keep alive PING to the IP: <input type="text"/> PING Interval: <input type="text"/> minute(s)		WAN IP Network Settings <input type="button" value="WAN IP Alias"/>	
WAN Connection Detection Mode: <input type="text" value="ARP Detect"/>		<input type="radio"/> Obtain an IP address automatically Router Name: <input type="text"/> * Domain Name: <input type="text"/> * <input type="checkbox"/> DHCP Client Identifier * Username: <input type="text"/> Password: <input type="text"/>	
MTU <input type="text" value="1500"/> (Max: 1500) Path MTU Discovery: <input type="button" value="Detect"/>		<input checked="" type="radio"/> Specify an IP address IP Address: <input type="text" value="172.16.3.130"/> Subnet Mask: <input type="text" value="255.255.255.0"/> Gateway IP Address: <input type="text" value="172.16.3.1"/>	
RIP Protocol <input type="checkbox"/> Enable RIP		<input type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: <input type="text" value="00"/> <input type="text" value="1D"/> <input type="text" value="AA"/> <input type="text" value="5D"/> <input type="text" value="C9"/> <input type="text" value="E2"/>	
Bridge Mode <input type="checkbox"/> Enable Bridge Mode <input type="checkbox"/> Enable Full Bridge Mode Bridge Subnet: <input type="text" value="LAN 1"/>		DNS Server IP Address Primary IP Address: <input type="text" value="8.8.8.8"/> Secondary IP Address: <input type="text" value="8.8.4.4"/>	
TTL Change the TTL value: <input type="text" value="Enable"/>			

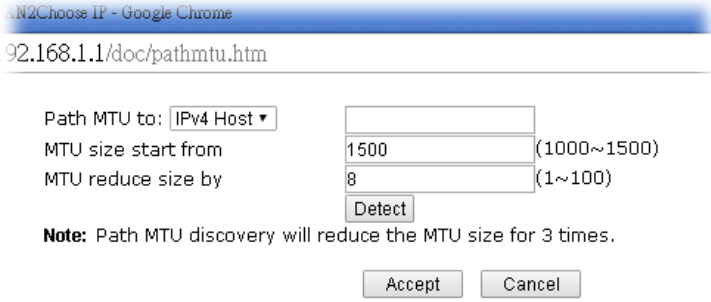
*: Required for some ISPs

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.
3. If both Bridge Mode and Firewall are enabled, the settings under User Management will be ignored.
4. Full Bridge Mode supports forwarding packets with VLAN tags.
5. Full Bridge Mode doesn't support wireless LAN.

Available settings are explained as follows:

Item	Description
Enable / Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
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

	<p>settings for the following items.</p> <ul style="list-style-type: none"> ● Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation. ● Ping Interval - Type the interval for the system to execute the PING operation. ● Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
<p>MTU</p>	<p>It means Max Transmit Unit for packet.</p> <p>Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path.</p> <p>Click Detect to open the following dialog.</p>  <ul style="list-style-type: none"> ● Path MTU to - Type the IP address as the specific transmit path. ● MTU size start from - Determine the starting point value of the packet. Default setting is 1500. ● MTU reduce size by - It determines the decreasing size of MTU value. For example, the number specified in this field is "8". The maximum MTU size is "1500". After clicking the "detect" button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically. ● Detect - Click it to detect a suitable MTU value ● Accept - After clicking it, the detected value will be displayed in the field of MTU.
<p>RIP Protocol</p>	<p>Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.</p>
<p>Bridge Mode</p>	<p>Enable Bridge Mode - If the function is enabled, the router will work as a bridge modem. Yet, the incoming packets with VLAN tags will be discarded.</p> <p>Enable Full Bridge Mode - If the function is enabled, the router will work as a bridge modem which is able to forward incoming packets with VLAN tags.</p> <p>Enable Firewall - It is available when Bridge Mode is enabled. When both Bridge Mode and Firewall check boxes</p>

	<p>are enabled, the settings configured (user profiles) under User Management will be ignored. And all of the filter rules defined and enabled in Firewall menu will be activated.</p> <p>Bridge Subnet - Make a bridge between the selected LAN subnet and such WAN interface.</p>
TTL	<p>Change the TTL value - Enable or disable the TTL (Time to Live) for a packet transmitted through Vigor router.</p> <p>Enable - TTL value will be reduced (-1) when it passes through Vigor router. It will cause the client, accessing Internet through Vigor router, to be blocked by certain ISP when TTL value becomes "0".</p> <p>Disable - TTL value will not be reduced. Then, when a packet passes through Vigor router, it will not be cancelled. That is, the client who sends out the packet will not be blocked by ISP.</p>
WAN IP Network Settings	<p>This group allows you to obtain an IP address automatically and allows you to type in IP address manually.</p> <p>WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 32 public IP addresses other than the current one you are using.</p> <p>Obtain an IP address automatically - Click this button to obtain the IP address automatically if you want to use Dynamic IP mode.</p> <ul style="list-style-type: none"> ● Router Name: Type in the router name provided by ISP. ● Domain Name: Type in the domain name that you have assigned. <p>DHCP Client Identifier for some ISP</p> <ul style="list-style-type: none"> ● Enable: Check the box to specify username and password as the DHCP client identifier for some ISP. ● Username: Type a name as username. The maximum length of the user name you can set is 63 characters. ● Password: Type a password. The maximum length of the password you can set is 62 characters. <p>Specify an IP address - Click this radio button to specify some data if you want to use Static IP mode.</p> <ul style="list-style-type: none"> ● IP Address: Type the IP address. ● Subnet Mask: Type the subnet mask. ● Gateway IP Address: Type the gateway IP address. <p>Default MAC Address: Click this radio button to use default MAC address for the router.</p> <p>Specify a MAC Address: Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the Specify a MAC Address and enter the MAC address in the MAC Address field.</p>
DNS Server IP Address	<p>Type in the primary IP address for the router if you want to use Static IP mode. If necessary, type in secondary IP address for necessity in the future.</p>

After 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.

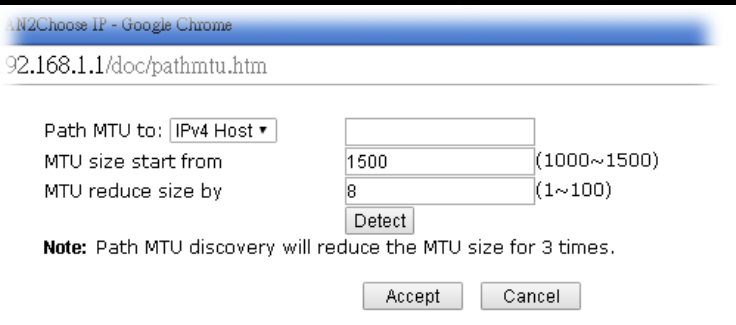
WAN >> Internet Access

WAN 2

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
<input type="radio"/> Enable PPTP <input type="radio"/> Enable L2TP <input checked="" type="radio"/> Disable Server Address <input type="text"/> Specify Gateway IP Address <input type="text"/>		PPP Setup PPP Authentication <input type="text" value="PAP or CHAP"/> Idle Timeout <input type="text" value="-1"/> second(s)	
ISP Access Setup Username <input type="text"/> Password <input type="text"/> Index(1-15) in Schedule Setup: => <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>		IP Address Assignment Method (IPCP) <input type="button" value="WAN IP Alias"/> Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address <input type="text"/>	
MTU <input type="text" value="1460"/> (Max:1460) Path MTU Discovery <input type="button" value="Detect"/>		WAN IP Network Settings <input type="radio"/> Obtain an IP address automatically <input checked="" type="radio"/> Specify an IP address IP Address <input type="text"/> Subnet Mask <input type="text"/>	

Available settings are explained as follows:

Item	Description
PPTP/L2TP	<p>Enable PPTP - Click this radio button to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface.</p> <p>Enable L2TP - Click this radio button to enable a L2TP client to establish a tunnel to a DSL modem on the WAN interface.</p> <p>Disable - Click this radio button to close the connection through PPTP or L2TP.</p> <p>Server Address - Specify the IP address of the PPTP/L2TP server if you enable PPTP/L2TP client mode.</p> <p>Specify Gateway IP Address - Specify the gateway IP address for DHCP server.</p>
ISP Access Setup	<p>Username -Type in the username provided by ISP in this field. The maximum length of the user name you can set is 63 characters.</p> <p>Password -Type in the password provided by ISP in this field. The maximum length of the password you can set is 62 characters.</p> <p>Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page.</p>
MTU	<p>It means Max Transmit Unit for packet.</p> <p>Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path.</p> <p>Click Detect to open the following dialog.</p>

	 <ul style="list-style-type: none"> ● Path MTU to - Type the IP address as the specific transmit path. ● MTU size start from - Determine the starting point value of the packet. Default setting is 1500. ● MTU reduce size by- It determines the decreasing size of MTU value. For example, the number specified in this field is "8". The maximum MTU size is "1500". After clicking the "detect" button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically. ● Detect - Click it to detect a suitable MTU value ● Accept - After clicking it, the detected value will be displayed in the field of MTU.
<p>PPP Setup</p>	<p>PPP Authentication - Select PAP only or PAP or CHAP for PPP.</p> <p>Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action.</p>
<p>IP Address Assignment Method(IPCP)</p>	<p>WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 32 public IP addresses other than the current one you are using.</p> <p>Fixed IP - Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Click Yes to use this function and type in a fixed IP address in the box.</p> <p>Fixed IP Address -Type a fixed IP address.</p>
<p>WAN IP Network Settings</p>	<p>Obtain an IP address automatically - Click this button to obtain the IP address automatically.</p> <p>Specify an IP address - Click this radio button to specify some data.</p> <ul style="list-style-type: none"> ● IP Address - Type the IP address. ● Subnet Mask - Type the subnet mask.

After finishing all the settings here, please click **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 >> Internet Access

WAN 2

Static or Dynamic IP	
<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
<input checked="" type="radio"/> Obtain an IP address automatically <input type="radio"/> 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 ▼
MTU	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 ▼

Note: If Channel is modified, the **Channel setting of wireless 2.4G** would be also modified.

Available settings are explained as follows:

Item	Description
Enable/Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
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 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.
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

	<p>Detect as the detection mode, you have to type required settings for the following items.</p> <ul style="list-style-type: none"> ● Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation. ● Ping Interval - Type the interval for the system to execute the PING operation. ● Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged. 																																																												
<p>MTU</p>	<p>It means Max Transmit Unit for packet.</p>																																																												
<p>AP Discovery</p>	<p>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.</p> <p>Wireless LAN >> Access Point Discovery</p> <hr/> <p>Access Point List</p> <table border="1"> <thead> <tr> <th>Index</th> <th>BSSID</th> <th>Channel</th> <th>RSSI</th> <th>SSID</th> <th>Authentication</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>02:1D:AA:9F:E9:48</td> <td>11</td> <td>78%</td> <td>DrayTek-LAN-B</td> <td>Mixed(WPA+WPA2)/PSK</td> </tr> <tr> <td>2</td> <td>00:1D:AA:9F:E9:48</td> <td>11</td> <td>78%</td> <td>AP900-airtime</td> <td>WPA2/PSK</td> </tr> <tr> <td>3</td> <td>02:1D:AA:90:20:80</td> <td>11</td> <td>26%</td> <td>ap902_2.4G_114_2</td> <td>WPA2/PSK</td> </tr> <tr> <td>4</td> <td>00:1D:AA:90:20:80</td> <td>11</td> <td>26%</td> <td>ap902_Wifi_114_1</td> <td>WPA2/PSK</td> </tr> <tr> <td>5</td> <td>02:50:7F:22:33:88</td> <td>11</td> <td>23%</td> <td>AP900_110_Bandstee...</td> <td>WPA2/PSK</td> </tr> <tr> <td>6</td> <td>00:50:7F:22:33:88</td> <td>11</td> <td>23%</td> <td>AP900_110_2.4G-1</td> <td>WPA2/PSK</td> </tr> <tr> <td>7</td> <td>02:1D:AA:7E:41:80</td> <td>11</td> <td>13%</td> <td>TestRoaming2.4G-B</td> <td>Mixed(WPA+WPA2)/PSK</td> </tr> <tr> <td>8</td> <td>00:1D:AA:7E:41:80</td> <td>11</td> <td>18%</td> <td>TestRoaming2.4G-A</td> <td>Mixed(WPA+WPA2)/PSK</td> </tr> <tr> <td>9</td> <td>00:1D:AA:DD:75:00</td> <td>11</td> <td>63%</td> <td>v2860_lte_1</td> <td>Mixed(WPA+WPA2)/PSK</td> </tr> </tbody> </table> <p style="text-align: center;">Scan</p> <p>AP's MAC address <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/></p> <p style="text-align: center;">Add to <input checked="" type="radio"/> Universal Repeater</p> <p>Note:</p> <ol style="list-style-type: none"> 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. 	Index	BSSID	Channel	RSSI	SSID	Authentication	1	02:1D:AA:9F:E9:48	11	78%	DrayTek-LAN-B	Mixed(WPA+WPA2)/PSK	2	00:1D:AA:9F:E9:48	11	78%	AP900-airtime	WPA2/PSK	3	02:1D:AA:90:20:80	11	26%	ap902_2.4G_114_2	WPA2/PSK	4	00:1D:AA:90:20:80	11	26%	ap902_Wifi_114_1	WPA2/PSK	5	02:50:7F:22:33:88	11	23%	AP900_110_Bandstee...	WPA2/PSK	6	00:50:7F:22:33:88	11	23%	AP900_110_2.4G-1	WPA2/PSK	7	02:1D:AA:7E:41:80	11	13%	TestRoaming2.4G-B	Mixed(WPA+WPA2)/PSK	8	00:1D:AA:7E:41:80	11	18%	TestRoaming2.4G-A	Mixed(WPA+WPA2)/PSK	9	00:1D:AA:DD:75:00	11	63%	v2860_lte_1	Mixed(WPA+WPA2)/PSK
Index	BSSID	Channel	RSSI	SSID	Authentication																																																								
1	02:1D:AA:9F:E9:48	11	78%	DrayTek-LAN-B	Mixed(WPA+WPA2)/PSK																																																								
2	00:1D:AA:9F:E9:48	11	78%	AP900-airtime	WPA2/PSK																																																								
3	02:1D:AA:90:20:80	11	26%	ap902_2.4G_114_2	WPA2/PSK																																																								
4	00:1D:AA:90:20:80	11	26%	ap902_Wifi_114_1	WPA2/PSK																																																								
5	02:50:7F:22:33:88	11	23%	AP900_110_Bandstee...	WPA2/PSK																																																								
6	00:50:7F:22:33:88	11	23%	AP900_110_2.4G-1	WPA2/PSK																																																								
7	02:1D:AA:7E:41:80	11	13%	TestRoaming2.4G-B	Mixed(WPA+WPA2)/PSK																																																								
8	00:1D:AA:7E:41:80	11	18%	TestRoaming2.4G-A	Mixed(WPA+WPA2)/PSK																																																								
9	00:1D:AA:DD:75:00	11	63%	v2860_lte_1	Mixed(WPA+WPA2)/PSK																																																								
<p>SSID</p>	<p>The identification of the Wireless AP.</p>																																																												
<p>MAC Address (Optional)</p>	<p>The MAC Address of the Wireless AP.</p>																																																												
<p>Channel</p>	<p>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.</p>																																																												
<p>Security Mode</p>	<p>The mode to connect to the Wireless AP.</p> <p>Disable - The Router connects to the wireless AP without any encryption mechanism.</p> <p>WEP - The Router connects to the wireless AP as a WEP client and the encryption key should be entered in WEP Key.</p> <ul style="list-style-type: none"> ● 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 																																																												

	<p>in ASCII or Hexadecimal. Check the key you wish to use.</p> <p>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.</p> <p>WPA2/PSK - The Router connects to the wireless AP as a WPA2 client and the encryption key should be entered in PSK.</p> <p>Pass Phrase - The PSK. Either 8-63 ASCII characters, such as 012345678. (or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").</p>
--	--

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) IPv6

[Modem Support List](#)

3G/4G USB Modem(PPP mode) Enable Disable

SIM PIN code

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

APN Name

Modem Initial String2

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

Service Name (Optional)

PPP Username (Optional)

PPP Password (Optional)

PPP Authentication

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

WAN Connection Detection

Mode

Available settings are explained as follows:

Item	Description																																																								
Modem Support List	<p>It lists all of the modems supported by such router.</p> <p>@8.1.1/@oc/pppsuplist.htm</p> <p>3G/4G Modem Support List(PPP mode)</p> <p>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.</p> <table border="1"> <thead> <tr> <th>Brand</th> <th>Model</th> <th>LTE</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>Aiko</td> <td>Aiko 83D</td> <td></td> <td>Y</td> </tr> <tr> <td>Alcatel</td> <td>Alcatel L100V</td> <td>✔</td> <td>Y</td> </tr> <tr> <td>Alcatel</td> <td>Alcatel W100</td> <td>✔</td> <td>Y</td> </tr> <tr> <td>BandRich</td> <td>Bandlux C170</td> <td></td> <td>Y</td> </tr> <tr> <td>BandRich</td> <td>Bandlux C270</td> <td></td> <td>Y</td> </tr> <tr> <td>BandRich</td> <td>Bandlux C321</td> <td></td> <td>Y</td> </tr> <tr> <td>BandRich</td> <td>Bandlux C330</td> <td></td> <td>Y</td> </tr> <tr> <td>BandRich</td> <td>Bandlux C331</td> <td></td> <td>Y</td> </tr> <tr> <td>BandRich</td> <td>Bandlux C502</td> <td></td> <td>Y</td> </tr> <tr> <td>D-Link</td> <td>D_LINK DWM221 B1</td> <td>✔</td> <td>Y</td> </tr> <tr> <td>Huawei</td> <td>Huawei E169u</td> <td></td> <td>Y</td> </tr> <tr> <td>Huawei</td> <td>Huawei E220</td> <td></td> <td>Y</td> </tr> <tr> <td>Huawei</td> <td>Huawei E303D</td> <td></td> <td>Y</td> </tr> </tbody> </table>	Brand	Model	LTE	Status	Aiko	Aiko 83D		Y	Alcatel	Alcatel L100V	✔	Y	Alcatel	Alcatel W100	✔	Y	BandRich	Bandlux C170		Y	BandRich	Bandlux C270		Y	BandRich	Bandlux C321		Y	BandRich	Bandlux C330		Y	BandRich	Bandlux C331		Y	BandRich	Bandlux C502		Y	D-Link	D_LINK DWM221 B1	✔	Y	Huawei	Huawei E169u		Y	Huawei	Huawei E220		Y	Huawei	Huawei E303D		Y
Brand	Model	LTE	Status																																																						
Aiko	Aiko 83D		Y																																																						
Alcatel	Alcatel L100V	✔	Y																																																						
Alcatel	Alcatel W100	✔	Y																																																						
BandRich	Bandlux C170		Y																																																						
BandRich	Bandlux C270		Y																																																						
BandRich	Bandlux C321		Y																																																						
BandRich	Bandlux C330		Y																																																						
BandRich	Bandlux C331		Y																																																						
BandRich	Bandlux C502		Y																																																						
D-Link	D_LINK DWM221 B1	✔	Y																																																						
Huawei	Huawei E169u		Y																																																						
Huawei	Huawei E220		Y																																																						
Huawei	Huawei E303D		Y																																																						
3G /4G USB Modem (PPP mode)	Click Enable for activating this function. If you click Disable, this function will be closed and all the settings that you																																																								

	adjusted in this page will be invalid.
SIM PIN code	Type PIN code of the SIM card that will be used to access Internet. 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. <ul style="list-style-type: none"> ● Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation. ● Ping Interval - Type the interval for the system to

execute the PING operation.

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

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) IPv6 [Modem Support List](#)

<input checked="" type="radio"/> Enable <input type="radio"/> Disable SIM PIN code <input type="text"/> Network Mode <input type="text" value="4G/3G/2G"/> (Default:4G/3G/2G) APN Name <input type="text"/> LTE hardware version ---	Authentication <input type="text" value="PAP or CHAP"/> Username <input type="text"/> (Optional) Password <input type="text"/> (Optional)
WAN Connection Detection Mode <input type="text" value="ARP Detect"/>	
MTU <input type="text" value="1500"/> (Default:1500) Path MTU Discovery <input type="text" value="Choose IP"/>	

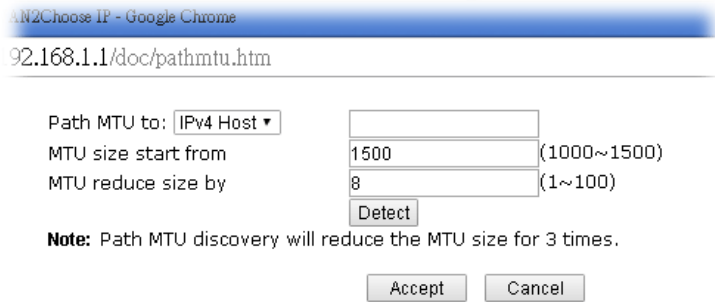
Note:

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

OK Cancel

Available settings are explained as follows:

Item	Description																																																				
Modem Support List	<p>It lists all of the modems supported by such router.</p> <p>3G/4G Modem Support List(DHCP mode)</p> <p>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.</p> <table border="1"> <thead> <tr> <th>Brand</th> <th>Model</th> <th>LTE</th> <th>Status</th> </tr> </thead> <tbody> <tr><td>Alcatel</td><td>Alcatel L100V</td><td>✓</td><td>Y</td></tr> <tr><td>Alcatel</td><td>Alcatel L800</td><td>✓</td><td>Y</td></tr> <tr><td>Alcatel</td><td>Alcatel W100</td><td>✓</td><td>Y</td></tr> <tr><td>Alcatel</td><td>Alcatel W800</td><td>✓</td><td>M</td></tr> <tr><td>Alcatel</td><td>Alcatel Y855</td><td>✓</td><td>Y</td></tr> <tr><td>D-Link</td><td>D_LINK DWM156 A8</td><td></td><td>M</td></tr> <tr><td>Huawei</td><td>Huawei E303</td><td></td><td>Y</td></tr> <tr><td>Huawei</td><td>Huawei E3131</td><td></td><td>Y</td></tr> <tr><td>Huawei</td><td>Huawei E3272</td><td>✓</td><td>Y</td></tr> <tr><td>Huawei</td><td>Huawei E3276</td><td>✓</td><td>Y</td></tr> <tr><td>Huawei</td><td>Huawei E3372h-607</td><td>✓</td><td>Y</td></tr> <tr><td>Huawei</td><td>Huawei E3531</td><td></td><td>Y</td></tr> </tbody> </table>	Brand	Model	LTE	Status	Alcatel	Alcatel L100V	✓	Y	Alcatel	Alcatel L800	✓	Y	Alcatel	Alcatel W100	✓	Y	Alcatel	Alcatel W800	✓	M	Alcatel	Alcatel Y855	✓	Y	D-Link	D_LINK DWM156 A8		M	Huawei	Huawei E303		Y	Huawei	Huawei E3131		Y	Huawei	Huawei E3272	✓	Y	Huawei	Huawei E3276	✓	Y	Huawei	Huawei E3372h-607	✓	Y	Huawei	Huawei E3531		Y
Brand	Model	LTE	Status																																																		
Alcatel	Alcatel L100V	✓	Y																																																		
Alcatel	Alcatel L800	✓	Y																																																		
Alcatel	Alcatel W100	✓	Y																																																		
Alcatel	Alcatel W800	✓	M																																																		
Alcatel	Alcatel Y855	✓	Y																																																		
D-Link	D_LINK DWM156 A8		M																																																		
Huawei	Huawei E303		Y																																																		
Huawei	Huawei E3131		Y																																																		
Huawei	Huawei E3272	✓	Y																																																		
Huawei	Huawei E3276	✓	Y																																																		
Huawei	Huawei E3372h-607	✓	Y																																																		
Huawei	Huawei E3531		Y																																																		
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.																																																				
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.
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. <ul style="list-style-type: none"> ● Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation. ● Ping Interval - Type the interval for the system to execute the PING operation. ● Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
MTU	It means Max Transmit Unit for packet. 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.  <ul style="list-style-type: none"> ● Path MTU to - Type the IP address as the specific transmit path. ● MTU size start from - Determine the starting point value of the packet. Default setting is 1500. ● MTU reduce size by - It determines the decreasing size of MTU value. For example, the number specified in this field is "8". The maximum MTU size is "1500". After clicking the "detect" button, the system will

	<p>calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically.</p> <ul style="list-style-type: none"> ● Detect - Click it to detect a suitable MTU value ● Accept - After clicking it, the detected value will be displayed in the field of MTU.
Authentication	<p>Select PAP only or PAP or CHAP for PPP authentication.</p> <p>Username - Type the username for authentication (optional).</p> <p>Password - Type the password for authentication (optional).</p>

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

II-1-2-11 Details Page for IPv6 – Offline in WAN1/WAN2/WAN3/WAN4

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

WAN >> Internet Access

WAN 1

PPPoE	Static or Dynamic IP	PPTP	IPv6
Internet Access Mode			
Connection Type		Offline ▼	

II-1-2-12 Details Page for IPv6 – PPP in WAN1/WAN2

WAN >> Internet Access



WAN 1

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

Note:

IPv4 WAN setting should be **PPPoE / PPPoA** client.

Available settings are explained as follows:

Item	Description
WAN Connection Detection	<p>Such function allows you to verify whether network connection is alive or not through Ping Detect.</p> <p>Mode - Choose Always On or Ping Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always.</p>

	<ul style="list-style-type: none"> ● Ping IP/Hostname - If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. ● TTL (Time to Live) -If you choose Ping Detect as detection mode, you have to type TTL value.
RIPng Protocol	RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.

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

Online Status

Physical Connection		System Uptime: 0:2:32	
IPv4	IPv6		
LAN Status			
IP Address			
2001:B010:7300:201:21D:AFF:FEA6:2568/64 (Global)			
FE80::21D:AFF:FEA6:2568/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
7	4	690	328
WAN2 IPv6 Status >> Drop PPP			
Enable	Mode	Up Time	
Yes	PPP	0:02:08	
IP		Gateway IP	
2001:B010:7300:201:21D:AFF:FEA6:256A/128 (Global)		FE80::90:1A00:242:AD52	
FE80::1D:AFF:FEA6:256A/128 (Link)			
DNS IP			
2001:B000:168::1			
2001:B000:168::2			
TX Packets	RX Packets	TX Bytes	RX Bytes
7	9	544	1126



Info

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

II-1-2-13 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.



WAN 1

PPPoE / PPPoA	MPoA / Static or Dynamic IP	IPv6
Internet Access Mode		
Connection Type		TSPC ▼
TSPC Configuration		
Username		<input type="text"/>
Password		<input type="text"/>
Tunnel Broker		<input type="text"/>
WAN Connection Detection		
Mode		Ping Detect ▼
Ping IP/Hostname		<input type="text"/>
TTL(1-255,0:Auto)		<input type="text" value="0"/>
OK		Cancel

Available settings are explained as follows:

Item	Description
Username	Type the name obtained from the broker. It is suggested for you to apply another username and password for http://gogonet.gogo6.com/page/freenet6-account . 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. <ul style="list-style-type: none"> ● Ping IP/Hostname - If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. ● TTL (Time to Live) -If you choose Ping Detect as detection mode, you have to type TTL value.

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

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

WAN >> Internet Access



WAN 1

PPPoE / PPPoA	MPoA / Static or Dynamic IP	IPv6
Internet Access Mode		
Connection Type		AICCU
AICCU Configuration		
<input type="checkbox"/> Always On		
Username	<input type="text"/>	
Password	<input type="text"/>	
Tunnel Broker	tic.sixxs.net	
Tunnel ID	<input type="text"/>	
Subnet Prefix	<input type="text"/>	/ <input type="text"/>
WAN Connection Detection		
Mode		Always On

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

OK Cancel

Available settings are explained as follows:

Item	Description
Always On	Check this box to keep the network connection always.
Username	Type the name obtained from the broker. Please apply new account at http://www.sixxs.net/ . It is suggested for you to apply another username and password. 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-1-2-15 Details Page for IPv6 – DHCPv6 Client in WAN1/WAN2

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

WAN >> Internet Access



WAN 1

PPPoE / PPPoA	MPOA / Static or Dynamic IP	IPv6
Internet Access Mode		
Connection Type		DHCPv6 Client
DHCPv6 Client Configuration		
IAID (Identity Association ID)	44180515	
DUID (DHCP Unique ID)	00030001001daaf7c0f1	
Authentication Protocol	None	
WAN Connection Detection		
Mode	Ping Detect	
Ping IP/Hostname		
TTL(1-255,0:Auto)	0	
RIPng Protocol		
<input type="checkbox"/> Enable		
Bridge Mode		
<input type="checkbox"/> Enable Bridge Mode		
Bridge Subnet	LAN 1	

OK

Cancel

Available settings are explained as follows:

Item	Description
DHCPv6 Client Configuration	<p>IAID - Type a number as IAID.</p> <p>DUID - Display the DHCP unique ID used by such WAN interface.</p> <p>Authentication Protocol - Such protocol will be used for the client to be authenticated by DHCPv6 server before accessing into Internet. There are three types can be specified, Reconfigure Key, Delayed and None. In general, the default setting is None.</p> <ul style="list-style-type: none"> ● Reconfigure Key - During the connection process, DHCPv6 server will authenticate the client automatically. ● Delayed - During the connection process, DHCPv6 server will authenticate and identify the client based on the key ID, realm and secret information specified in these fields. <p>Key ID - Type a value (range from 1 to 65535) which will be used to generate HMAC-MD5 value.</p> <p>Realm - The name (1 to 31 characters) typed here will identify the key which generates HMAC-MD5 value.</p> <p>Secret - Type a text (1 to 31 characters) as a unique identifier for each client on each DHCP server.</p>
WAN Connection Detection	<p>Such function allows you to verify whether network connection is alive or not through NS Detect or Ping Detect.</p> <p>Mode - Choose Always On, Ping Detect or NS Detect for the system to execute for WAN detection. With NS Detect mode, the system will check if network connection is</p>

	<p>established or not, like IPv4 ARP Detect. Always On means no detection will be executed. The network connection will be on always.</p> <ul style="list-style-type: none"> ● Ping IP/Hostname - If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. ● TTL (Time to Live) -If you choose Ping Detect as detection mode, you have to type TTL value.
RIPng Protocol	RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.
Bridge Mode	<p>Enable Bridge Mode - If the function is enabled, the router will work as a bridge modem.</p> <p>Enable Firewall - It is available when Bridge Mode is enabled. When both Bridge Mode and Firewall check boxes are enabled, the settings configured (user profiles) under User Management will be ignored. And all of the filter rules defined and enabled in Firewall menu will be activated.</p> <p>Bridge Subnet - Make a bridge between the selected LAN subnet and such WAN interface.</p>

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

II-1-2-16 Details Page for IPv6 – Static IPv6 in WAN1/WAN2

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

WAN >> Internet Access



WAN 1

PPPoE / PPPoA MPoA / Static or Dynamic IP **IPv6**

Internet Access Mode
 Connection Type: Static IPv6

Static IPv6 Address Configuration
 IPv6 Address / Prefix Length
 / Add Update Delete

Current IPv6 Address Table

Index	IPv6 Address/Prefix Length	Scope

Static IPv6 Gateway configuration
 IPv6 Gateway Address

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

RIPng Protocol
 Enable

Bridge Mode
 Enable Bridge Mode
 Bridge Subnet: LAN 1

OK Cancel

Available settings are explained as follows:

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

Detection	<p>connection is alive or not through Ping Detect.</p> <p>Mode - Choose Always On or Ping Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always.</p> <ul style="list-style-type: none"> ● Ping IP/Hostname - If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. ● TTL (Time to Live) -If you choose Ping Detect as detection mode, you have to type TTL value.
RIPng Protocol	<p>RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.</p>
Bridge Mode	<p>Enable Bridge Mode - If the function is enabled, the router will work as a bridge modem.</p> <p>Enable Firewall - It is available when Bridge Mode is enabled. When both Bridge Mode and Firewall check boxes are enabled, the settings configured (user profiles) under User Management will be ignored. And all of the filter rules defined and enabled in Firewall menu will be activated.</p> <p>Bridge Subnet - Make a bridge between the selected LAN subnet and such WAN interface.</p>

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

II-1-2-17 Details Page for IPv6 – 6in4 Static Tunnel in WAN1/WAN2

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

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

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

WAN >> Internet Access



WAN 1

PPPoE / PPPoA MPoA / Static or Dynamic IP IPv6

Internet Access Mode

Connection Type: 6in4 Static Tunnel

6in4 Static Tunnel

Remote Endpoint IPv4 Address:

6in4 IPv6 Address: / (default:64)

LAN Routed Prefix: / (default:64)

Tunnel TTL: (default:255)

WAN Connection Detection

Mode: Ping Detect

Ping IP/Hostname:

TTL(1-255,0: Auto):

OK Cancel

Available settings are explained as follows:

Item	Description
Remote Endpoint IPv4 Address	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. <ul style="list-style-type: none"> ● Ping IP/Hostname - If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. ● TTL (Time to Live) -If you choose Ping Detect as detection mode, you have to type TTL value.

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

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

Online Status

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

II-1-2-18 Details Page for IPv6 – 6rd in WAN1/WAN2

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

WAN >> Internet Access



WAN 1

PPPoE / PPPoA	MPoA / Static or Dynamic IP	IPv6
Internet Access Mode		
Connection Type		6rd
6rd Settings		
6rd Mode		<input type="radio"/> Auto 6rd <input checked="" type="radio"/> Static 6rd
Static 6rd Settings		
IPv4 Border Relay:	<input type="text"/>	
IPv4 Mask Length:	<input type="text" value="0"/>	
6rd Prefix:	<input type="text"/>	
6rd Prefix Length:	<input type="text" value="0"/>	
WAN Connection Detection		
Mode	Ping Detect	
Ping IP/Hostname	<input type="text"/>	
TTL(1-255,0: Auto)	<input type="text" value="0"/>	

Available settings are explained as follows:

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

IPv4 Border Relay	Type the IPv4 addresses of the 6rd Border Relay for a given 6rd domain.
IPv4 Mask Length	Type a number of high-order bits that are identical across all CE IPv4 addresses within a given 6rd domain. It may be any value between 0 and 32.
6rd Prefix	Type the 6rd IPv6 address.
6rd Prefix Length	Type the IPv6 prefix length for the 6rd IPv6 prefix in number of bits.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. Mode - Choose Always On or Ping Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always. <ul style="list-style-type: none"> ● Ping IP/Hostname - If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. ● TTL (Time to Live) -If you choose Ping Detect as detection mode, you have to type TTL value.

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

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

Online Status

Physical Connection		System Uptime: 0day 0:9:15	
IPv4	IPv6		
LAN Status			
IP Address			
2001:E41:A865:1D00:21D:AAFF:FE83:11B4/64 (Global)			
FE80::21D:AAFF:FE83:11B4/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
15	113	1354	18040
WAN1 IPv6 Status			
Enable	Mode	Up Time	
Yes	6rd	0:09:06	
IP		Gateway IP	
2001:E41:A865:1D01:21D:AAFF:FE83:11B5/128 (Global)		---	
FE80::C0A8:651D/128 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
13	29	967	2620

II-1-3 Multi-PVC/VLAN

This router allows you to create multi-PVC for different data transferring for using. Simply go to WAN 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/VLAN

Multi-PVC/VLAN

General		Advanced			
Channel	Enable	WAN Type	VPI/VCI	VLAN Tag	Port-based Bridge
1	Yes	ADSL	8/35	None	
2	Yes	Ethernet(WAN2)		None	
5. WAN5	No	ADSL	1/45	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
6. WAN6	No	ADSL	1/46	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
7. WAN7	No	ADSL	1/47	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
8.	No	ADSL	1/48	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
9.	No	ADSL	1/49	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
10.	No	ADSL	1/50	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4

Note:

Channel 3 and channel 4 are reserved for USB WAN.

OK

Cancel

Available settings are explained as follows:

Item	Description
Channel	Display the number of each channel. Channels 1 and 2 are used by the Internet Access web user interface and can not be configured here. Channels 5 ~ 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 ~ P4 - 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

Multi-PVC/VLAN Channel 8: **Enable** **Disable**
 WAN Type : ADSL

General Settings	ATM QoS
VPI <input style="width: 50px;" type="text" value="1"/>	QoS Type UBR
VCI <input style="width: 50px;" type="text" value="48"/>	PCR <input style="width: 50px;" type="text" value="0"/>
Protocol PPPoA	SCR <input style="width: 50px;" type="text" value="0"/>
Encapsulation VC MUX	MBS <input style="width: 50px;" type="text" value="0"/>
<input type="checkbox"/> Add VLAN Header	
VLAN Tag <input style="width: 50px;" type="text" value="0"/>	
Priority <input style="width: 50px;" type="text" value="0"/>	

Bridge mode

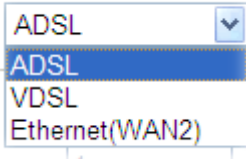

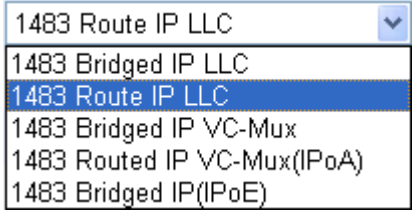
Enable

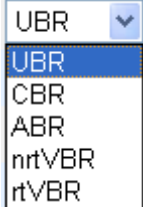
Physical Members

P1 P2 P3 P4

OK
Cancel

Available settings are explained as follows:

Item	Description
Multi-VLAN Channel 8/9/10	<p>Enable - Click it to enable the configuration of this channel.</p> <p>Disable - Click it to disable the configuration of this channel.</p>
WAN Type	<p>The connections and interfaces created in every channel may select a specific WAN type to be built upon. In the Multi-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.</p> 
General Settings	<p>VPI - Type in the value provided by your ISP.</p> <p>VCI - Type in the value provided by your ISP.</p> <p>Protocol - Select a proper protocol for this channel.</p> <p>Encapsulation - Choose a proper type for this channel. The types will be different according to the protocol setting that you choose.</p>   <p>Add VLAN Header - Check the box to enable the following two options.</p> <p>VLAN Tag - Type the value as the VLAN ID number. Valid settings are in the range from 1 to 4095. The network traffic</p>

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

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 Channel 5: Enable Disable

WAN Type :

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

Open Port-based Bridge Connection for this Channel

Physical Members

P1 P2 P3 P4

Open WAN Interface for this Channel

WAN Application: Management IPTV

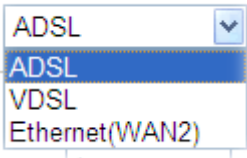
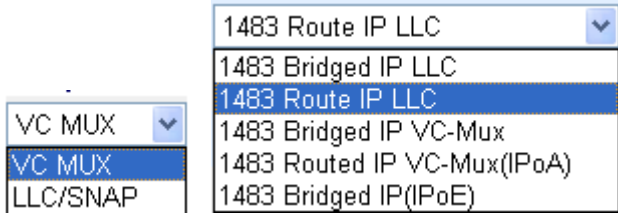
WAN Connection Detection

Mode

<p>PPPoE/PPPoA Client</p> <p>ISP Access Setup</p> <p>ISP Name <input type="text"/></p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>PPP Authentication <input type="text" value="PAP or CHAP"/></p> <p><input checked="" type="checkbox"/> Always On</p> <p>Idle Timeout <input type="text" value="-1"/> second(s)</p> <p>IP Address From ISP</p> <p>Fixed IP <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP)</p> <p>Fixed IP Address <input type="text"/></p>	<p>MPoA (RFC1483/2684)</p> <p><input checked="" type="radio"/> Obtain an IP address automatically</p> <p>Router Name <input type="text" value="Vigor"/>*</p> <p>Domain Name <input type="text"/>*</p> <p><small>*: Required for some ISPs</small></p> <p><input checked="" type="radio"/> Specify an IP address</p> <p>IP Address <input type="text"/></p> <p>Subnet Mask <input type="text"/></p> <p>Gateway IP Address <input type="text"/></p> <p>DNS Server IP Address</p> <p>Primary IP Address <input type="text" value="8.8.8.8"/></p> <p>Secondary IP Address <input type="text" value="8.8.4.4"/></p>
--	--

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.

	
<p>General Settings</p>	<p>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.</p>  <p>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.</p>
<p>ATM OoS</p>	<p>QoS Type - Select a proper QoS type for the channel. Type the values for PCR, SCR and MBS respectively.</p>
<p>Open Port-based Bridge Connection for this Channel</p>	<p>The settings here will create a bridge between the LAN ports selected and the WAN. The WAN interface of the bridge connection will be built upon the WAN type selected using the VLAN tag configured. Physical Members - Group the physical ports by checking the corresponding check box(es) for applying the port-based bridge connection.</p>
<p>Open WAN Interface for this Channel</p>	<p>Check the box to enable relating function. WAN Application -</p> <ul style="list-style-type: none"> ● Management - It can be specified for general management (Web configuration/telnet/TR069). If you choose Management, the configuration for this VLAN will be effective for Web configuration/telnet/TR069. ● IPTV - The IPTV configuration will allow the WAN interface to send IGMP packets to IPTV servers.
<p>ISP Access Setup</p>	<p>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</p>

	<p>characters.</p> <p>PPP Authentication - Select PAP only or PAP or CHAP for PPP.</p> <p>Always On - Check it to keep the network connection always.</p> <p>Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action.</p> <p>Fixed IP - Click Yes to use this function and type in a fixed IP address in the box of Fixed IP Address.</p>
MPoA (RFC...)	<p>Obtain an IP address automatically - Click this button to obtain the IP address automatically.</p> <ul style="list-style-type: none"> ● Router Name - Type in the router name provided by ISP. ● Domain Name - Type in the domain name that you have assigned. <p>Specify an IP address - Click this radio button to specify some data.</p> <ul style="list-style-type: none"> ● IP Address - Type in the private IP address. ● Subnet Mask - Type in the subnet mask. ● Gateway IP Address - Type in gateway IP address. <p>DNS Server IP Address - Type in the primary IP address for the router if you want to use Static IP mode. If necessary, type in secondary IP address for necessity in the future.</p>

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

Advanced

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

WAN >> Multi-PVC/VLAN

Multi-PVC/VLAN

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

Note:

1. If the parameters in the ATM QoS settings are set to zero, then their default settings will be used. Also, PCR(max)=ADSL Up Speed /53/8.
2. Multiple channels may use the same ADSL channel link through the PVC Binding configuration. The PVC Binding configuration is only supported for channels using ADSL, please make sure the channel that you are binding to is using ADSL as its WAN type. The binding will work only under PPPoE and MPoA 1483 Bridge mode.
3. Channel 3 and channel 4 are reserved for USB WAN.

OK Cancel

Available settings are explained as follows:

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

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

II-1-4 WAN Budget

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

II-1-4-1 General Setup

WAN >> WAN Budget

General Setup			Status		
Index	Enable	Quota	When quota exceeded	Time cycle	Duration
WAN1	<input type="checkbox"/>	0MB/0MB			0/00/00 00:00~0/00/00 00:00
WAN2	<input type="checkbox"/>	0MB/0MB			0/00/00 00:00~0/00/00 00:00
WAN3	<input type="checkbox"/>	0MB/0MB			0/00/00 00:00~0/00/00 00:00
WAN4	<input type="checkbox"/>	0MB/0MB			0/00/00 00:00~0/00/00 00:00

Note:

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

OK Cancel

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

WAN >> WAN Budget

WAN 1

Enable

Criterion and Action

Quota Limit: MB

When quota exceeded : Shutdown WAN interface
Using **Notification Object** 1-WAN_Notify

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

Monthly Custom

Select the day of a month when your (cellular) data resets.
Data quota resets on day at

Note:

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

OK Cancel

Available settings are explained as follows:

Item	Description
Enable	Check the box to enable such function.
Quota Limit	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. ● Using Notification Object - The system will send out a notification based on the content of the notification

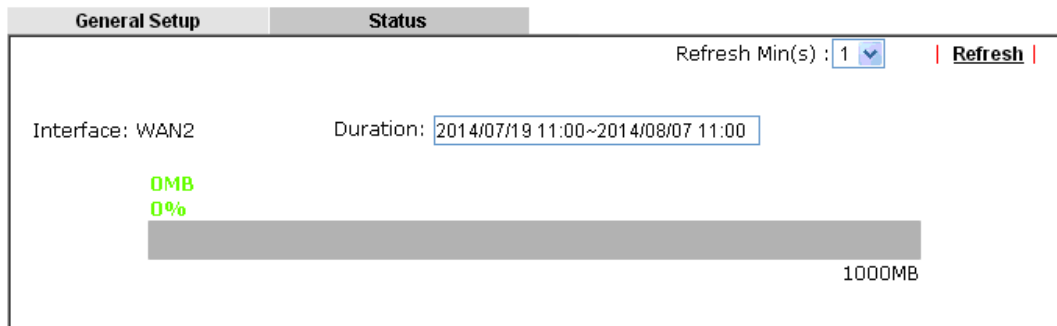
	<p>object.</p> <ul style="list-style-type: none"> ● Set Mail Alert - The system will send out a warning message to the administrator when the quota is running out. However, the connection charges will be calculated continuously. ● Set SMS message - The system will send out SMS message to the administrator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

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

II-1-4-2 Status

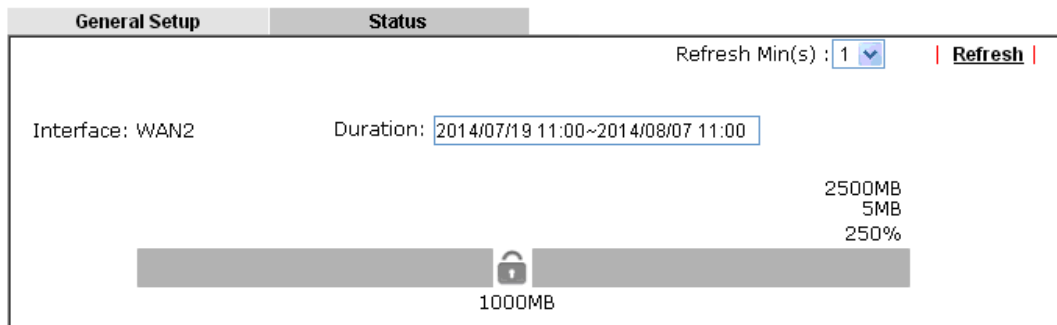
The status page displays the status WAN budget, including the duration and the usage.

WAN >> WAN Budget



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

WAN >> WAN Budget



Application Notes

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

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

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

IPv4 Internet Access				
	Line / Mode	IP Address	MAC Address	Up Time
WAN1	Fiber / ---	Disconnected	00-1D-AA-B3-85-B9	00:00:00
WAN2	Ethernet / PPPoE	118.200.200.200	00-1D-AA-B3-85-BA	2:56:04
WAN3	USB / ---	Disconnected	00-1D-AA-B3-85-BB	00:00:00
WAN4	USB / ---	Disconnected	00-1D-AA-B3-85-BC	00:00:00

IPv6 Internet Access				
	Mode	Address	Scope	Up Time
WAN2	AICCU	2401:0000:1000:70::2/128 FE80::E800:100:70:2/128	Global Link	2:56:01

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

LAN >> General Setup

General Setup

Index	Status	DHCP	DHCPv6	IP Address		
LAN 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.1.1	Details Page	IPv6
LAN 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.2.1	Details Page	IPv6
LAN 3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.3.1	Details Page	IPv6
LAN 4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.4.1	Details Page	IPv6
LAN 5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.5.1	Details Page	IPv6
LAN 6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.6.1	Details Page	IPv6
LAN 7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.7.1	Details Page	IPv6
LAN 8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.8.1	Details Page	IPv6
DMZ Port	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.17.1	Details Page	IPv6
IP Routed Subnet	<input type="checkbox"/>	<input checked="" type="checkbox"/>		192.168.0.1	Details Page	

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

LAN >> General Setup

LAN 1 Ethernet TCP / IP and DHCP Setup LAN 1 IPv6 Setup

Enable IPv6

WAN Primary interface: WAN2

Static IPv6 Address
 IPv6 Address: / Prefix Length
 / / Add Delete

Unique Local Address(ULA) configuration
 Off / 64

Current IPv6 Address Table

Index	IPv6 Address/Prefix Length	Scope
1	2401:1000:1000:0070::25 / 64	Global
2	FE80::21D:AFF:FE3:85B8 / 64	Link

DNS Server IPv6 Address Deploy when WAN is up

Primary DNS Server: 2001:4860:4860:8888
 Secondary DNS Server: 2001:4860:4860:8844

Management SLAAC(stateless) Other Option(O-bit)

DHCPv6 Server
 Enable Server Disable Server
 Auto IPv6 range
 Start IPv6 Address: ::
 End IPv6 Address: ::
 Advance setting: Edit

Advance setting Edit

OK

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

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

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . : 
    IP Address. . . . . : 192.168.1.11
    Subnet Mask . . . . . : 255.255.255.0
    IP Address. . . . . : 2401:e000:100:0070::25:100b:ce3d:e09b
    IP Address. . . . . : 2401:e000:100:0070:10da:e0ff:feb1:ee8d
    IP Address. . . . . : fe80::16da:e9ff:feb1:cad875
    Default Gateway . . . . . : 192.168.1.1
    fe80::21d:aaff:feb3:85b875
```

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

```
C:\WINDOWS>ping ipv6.google.com
Pinging ipv6.1.google.com [2404:6800:4008:c01::71] with 32 bytes of data:
Reply from 2404:6800:4008:c01::71: time=326ms
Reply from 2404:6800:4008:c01::71: time=172ms
Reply from 2404:6800:4008:c01::71: time=243ms
Reply from 2404:6800:4008:c01::71: time=246ms

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

A-2 How to configure IPv6 on WAN interface?

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

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

Online Status

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

IPv4		IPv6			
LAN Status	Primary DNS: 168.95.1.1		Secondary DNS: 168.95.192.1		
IP Address	TX Packets	RX Packets			
192.168.86.1	643	793			
WAN 1 Status >> Dial PPPoA					
Enable	Line	Name	Mode	Up Time	
Yes	ADSL		PPPoA	00:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
---	---	0	0	0	0
WAN 2 Status >> Drop PPPoE					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:03:20	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
118.106.103.103	168.95.192.1	79	3	81	9

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

WAN >> Internet Access

Internet Access

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

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

WAN >> Internet Access ?

WAN 2

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

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

Online Status

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

IPv4 IPv6

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

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

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

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

Diagnostics >> Ping Diagnosis

Ping Diagnosis

IPV4 IPV6

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

Ping through:

Ping IPv6 Address:

Result |

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

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

PPP (Point-to-Point Protocol)

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

WAN >> Internet Access



WAN 2

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

Note:

IPv4 WAN setting should be **PPPoE / PPPoA** client.

OK

Cancel

TSPC (Tunnel Setup Protocol Client)

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

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

WAN >> Internet Access



WAN 2

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

OK

Cancel

Static IPv6

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

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

WAN >> Internet Access ?

WAN 2

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

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

WAN >> Internet Access ?

WAN 2

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

Static IPv6 Gateway configuration

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

WAN Connection Detection

Mode: Always On

Bridge Mode

Enable Bridge Mode

Bridge Subnet: LAN 1

6in4 Static Tunnel

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

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

WAN >> Internet Access ?

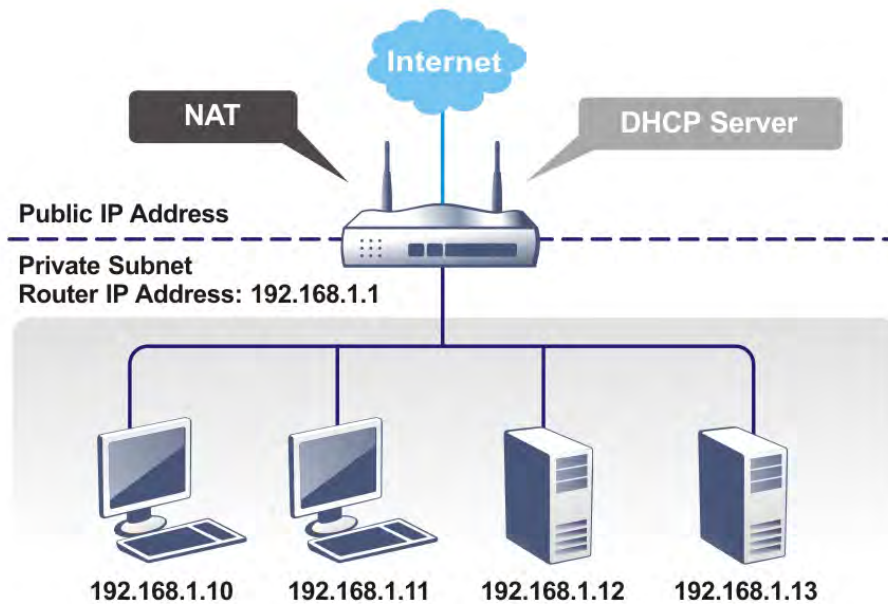
WAN 2

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
Internet Access Mode			
Connection Type		6in4 Static Tunnel	
6in4 Static Tunnel			
Remote Endpoint IPv4 Address		216.211.221.16	
6in4 IPv6 Address		2001:47c:1b:836::2 / 64 (default:64)	
LAN Routed Prefix		2001:47c:1b:836:: / 64 (default:64)	
Tunnel TTL		255 (default:255)	
WAN Connection Detection			
Mode		Always On	

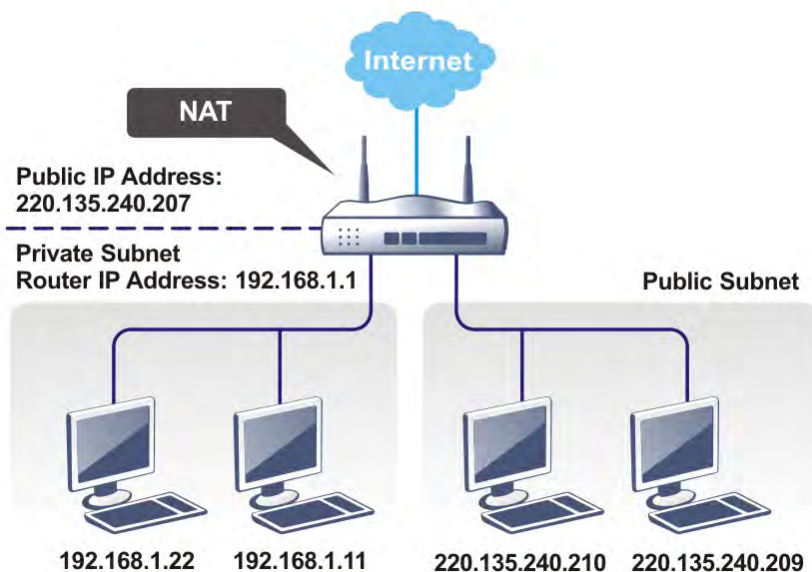
II-2 LAN

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)

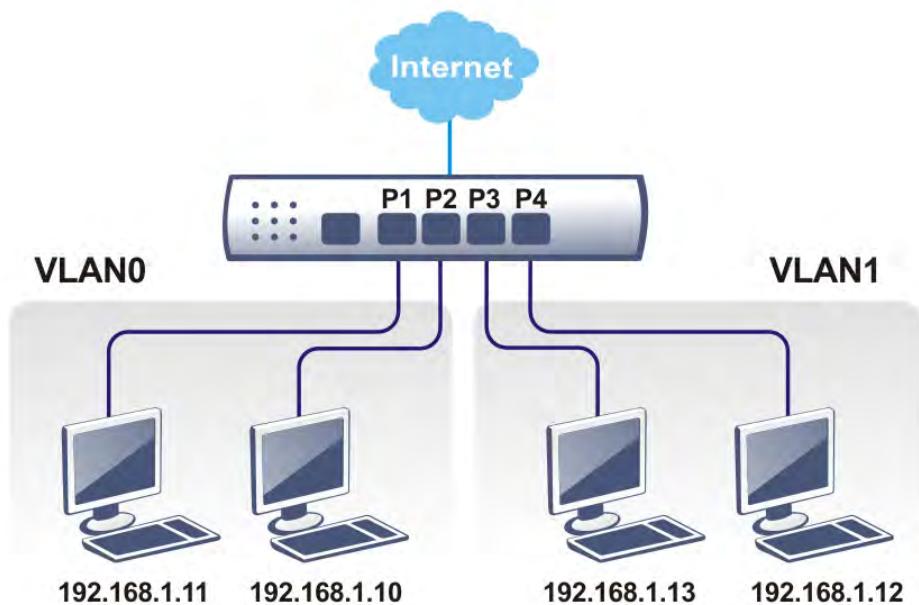
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

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 eight subnets provided by the router which allow users to divide groups into different subnets (LAN1 - LAN8). 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 - LAN8 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	DHCPv6	IP Address		
LAN 1	V	V	V	192.168.1.1	Details Page	IPv6
LAN 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.2.1	Details Page	IPv6
LAN 3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.3.1	Details Page	IPv6
LAN 4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.4.1	Details Page	IPv6
LAN 5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.5.1	Details Page	IPv6
LAN 6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.6.1	Details Page	IPv6
LAN 7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.7.1	Details Page	IPv6
LAN 8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.8.1	Details Page	IPv6
DMZ Port	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.17.1	Details Page	IPv6
IP Routed Subnet	<input type="checkbox"/>	<input checked="" type="checkbox"/>		192.168.0.1	Details Page	

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

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

Inter-LAN Routing

Subnet	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5	LAN 6	LAN 7	LAN 8	DMZ Port
LAN 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
DMZ Port	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Note:

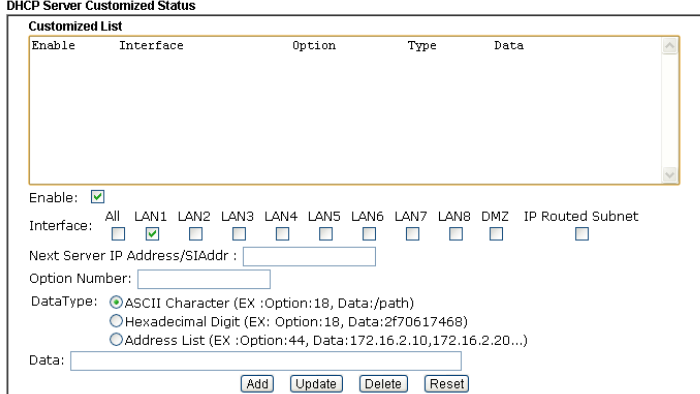
LAN2/3/4/5/6/7/8 are available when VLAN is enabled.

DMZ subnet is default bound to P4, and will overwrite the settings of P4 at LAN>>VLAN page.

[OK](#)

Available settings are explained as follows:

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

	<p>checking the box of Status.</p> <p>DHCP/DHCPv6- LAN1 is configured with DHCP/DHCPv6 in default. If required, please check the DHCP box for each LAN.</p> <p>IP Address - Display the IP address for each LAN item. Such information is set in default and you can not modify it.</p> <p>Details Page - Click it to access into the setting page. Each LAN will have different LAN configuration page. Each LAN must be configured in different subnet.</p> <p>IPv6 - Click it to access into the settings page of IPv6.</p>
<p>Advanced</p>	<p>DHCP packets can be processed by adding option number and data information when such function is enabled.</p> <p>LAN >> General Setup</p>  <p>Note:</p> <ol style="list-style-type: none"> 1. Configuring options 44, 46 or 66 here will overwrite the settings by telnet command "msubnet". 2. Configuring option 3 here will overwrite the setting in "LAN >> General Setup" Details Page's "Gateway IP Address" field. 3. Configuring option 15 here will overwrite the setting in "WAN >> Internet Access >> Static or Dynamic IP" Detail Page's "Domain Name" field. <p>OK</p> <p>Enable - Check the box to enable the function of DHCP Option. Each DHCP option is composed by an option number with data. For example, Option number: 100 Data: abcd</p> <p>When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets.</p> <p>Interface - Choose the interface for such option.</p> <p>Next Server IP Address/SIAddr - Type the IP address of PXE server which is helpful for downloading boot loader via network.</p> <p>Option Number - Type a number for such function.</p> <p>DataType - Choose the type (ASCII or Hex or IP) for the data to be stored.</p> <p>Data - Type the content of the data to be processed by the function of DHCP option.</p>
<p>Force router to use "DNS server IP address"</p>	<p>Force Vigor router to use DNS servers configured in LAN1/LAN2/LAN3/LAN4/LAN5/LAN6/LAN7/LAN8/DMZ Port instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).</p>
<p>Inter-LAN Routing</p>	<p>Check the box to link two or more different subnets (LAN and LAN).</p>

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

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

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

LAN >> General Setup

LAN 1 Ethernet TCP / IP and DHCP Setup	LAN 1 IPv6 Setup
Network Configuration For NAT Usage IP Address <input type="text" value="192.168.1.1"/> Subnet Mask <input type="text" value="255.255.255.0"/> <hr/> RIP Protocol Control <input type="text" value="Disable"/>	DHCP Server Configuration <input type="radio"/> Disable <input checked="" type="radio"/> Enable Server <input type="radio"/> Enable Relay Agent Start IP Address <input type="text" value="192.168.1.10"/> IP Pool Counts <input type="text" value="200"/> (max. 1021) Gateway IP Address <input type="text" value="192.168.1.1"/> Lease Time <input type="text" value="86400"/> (s) <input checked="" type="checkbox"/> Clear DHCP lease for inactive clients periodically <hr/> DNS Server IP Address Primary IP Address <input type="text"/> Secondary IP Address <input type="text"/>

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

OK

Available settings are explained as follows:

Item	Description
Network Configuration	<p>For NAT Usage,</p> <p>IP Address - Type in private IP address for connecting to a local private network (Default: 192.168.1.1).</p> <p>Subnet Mask - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)</p> <p>RIP Protocol Control,</p> <p>Disable - deactivate the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)</p> <p>Enable - activate the RIP protocol.</p>
DHCP Server Configuration	<p>DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatches related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.</p> <p>If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.</p> <p>Disable Server - Let you manually assign IP address to every host in the LAN.</p> <p>Enable Server - Let the router assign IP address to every host in the LAN.</p> <ul style="list-style-type: none"> ● Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be

	<p>192.168.1.2 or greater, but smaller than 192.168.1.254.</p> <ul style="list-style-type: none"> ● 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). <p>Enable Relay Agent -Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.</p> <ul style="list-style-type: none"> ● DHCP Server IP Address - It is available when Enable Relay Agent is checked. Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server. 																
<p>DNS Server IP Address</p>	<p>DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.</p> <p>Primary IP Address -You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field.</p> <p>Secondary IP Address - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.</p> <p>The default DNS Server IP address can be found via Online Status:</p> <div data-bbox="699 1751 1396 1915" data-label="Table"> <p>Online Status</p> <hr/> <p>Physical Connection System Uptime: 22:22:45</p> <table border="1"> <thead> <tr> <th colspan="2">IPv4</th> <th colspan="2">IPv6</th> </tr> </thead> <tbody> <tr> <td>LAN Status</td> <td>Primary DNS: 8.8.8.8</td> <td colspan="2">Secondary DNS: 8.8.4.4</td> </tr> <tr> <td>IP Address</td> <td>TX Packets</td> <td>RX Packets</td> <td></td> </tr> <tr> <td>192.168.1.1</td> <td>0</td> <td>41533</td> <td></td> </tr> </tbody> </table> </div> <p>If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.</p> <p>If the IP address of a domain name is already in the DNS</p>	IPv4		IPv6		LAN Status	Primary DNS: 8.8.8.8	Secondary DNS: 8.8.4.4		IP Address	TX Packets	RX Packets		192.168.1.1	0	41533	
IPv4		IPv6															
LAN Status	Primary DNS: 8.8.8.8	Secondary DNS: 8.8.4.4															
IP Address	TX Packets	RX Packets															
192.168.1.1	0	41533															

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 ~ LAN8 and DMZ

LAN >> General Setup

DMZ Ethernet TCP / IP and DHCP Setup	DMZ IPv6 Setup
<p>Network Configuration</p> <p><input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> <p><input checked="" type="radio"/> For NAT Usage <input type="radio"/> For Routing Usage</p> <p>IP Address <input type="text" value="192.168.17.1"/></p> <p>Subnet Mask <input type="text" value="255.255.255.0"/></p>	<p>DHCP Server Configuration</p> <p><input type="radio"/> Disable <input checked="" type="radio"/> Enable Server <input type="radio"/> Enable Relay Agent</p> <p>Start IP Address <input type="text" value="192.168.17.10"/></p> <p>IP Pool Counts <input type="text" value="100"/> (max. 253)</p> <p>Gateway IP Address <input type="text" value="192.168.17.1"/></p> <p>Lease Time <input type="text" value="259200"/> (s)</p> <p><input checked="" type="checkbox"/> Clear DHCP lease for inactive clients periodically.</p> <hr/> <p>DNS Server IP Address</p> <p>Primary IP Address <input type="text"/></p> <p>Secondary IP Address <input type="text"/></p>

Note: Change IP Address or Subnet Mask in Network Configuration will also change **HA** DMZ Virtual IP to the same domain IP.

OK

Available settings are explained as follows:

Item	Description
Network Configuration	<p>Enable/Disable - Click Enable to enable such configuration; click Disable to disable such configuration.</p> <p>For NAT Usage - Click this radio button to invoke NAT function.</p> <p>For Routing Usage - Click this radio button to invoke this function.</p> <p>IP Address - Type in private IP address for connecting to a local private network (Default: 192.168.1.1).</p> <p>Subnet Mask - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)</p>
DHCP Server Configuration	<p>DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.</p> <p>Disable Server - Let you manually assign IP address to every host in the LAN.</p> <p>Enable Server - Let the router assign IP address to every host in the LAN.</p> <ul style="list-style-type: none"> ● Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP

addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.

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

Enable Relay Agent - 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.

DNS Server IP Address

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

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

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

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

Online Status

Physical Connection System Uptime: 22:22:45

IPV4		IPV6	
LAN Status	Primary DNS: 8.8.8.8		Secondary DNS: 8.8.4.4
IP Address	TX Packets	RX Packets	
192.168.1.1	0	41533	

If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users

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

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

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

LAN >> General Setup

TCP/IP and DHCP Setup for IP Routed Subnet

<p>Network Configuration</p> <p><input type="radio"/> Enable <input checked="" type="radio"/> Disable For Routing Usage</p> <p>IP Address: <input type="text" value="192.168.0.1"/></p> <p>Subnet Mask: <input type="text" value="255.255.255.0"/></p> <hr/> <p>RIP Protocol Control: <input type="text" value="Disable"/></p>	<p>DHCP Server Configuration</p> <p>Start IP Address: <input type="text"/></p> <p>IP Pool Counts: <input type="text" value="0"/> (max. 32)</p> <p>Lease Time: <input type="text" value="259200"/> (s)</p> <p><input type="checkbox"/> Use LAN Port <input checked="" type="checkbox"/> P1 <input checked="" type="checkbox"/> P2</p> <p><input checked="" type="checkbox"/> Use MAC Address</p> <table border="1"> <thead> <tr> <th>Index</th> <th>Matched MAC Address</th> <th>given IP Address</th> </tr> </thead> <tbody> <tr> <td colspan="3" style="height: 100px;"> </td> </tr> </tbody> </table> <p>MAC Address: <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/></p> <p><input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/></p>	Index	Matched MAC Address	given IP Address			
Index	Matched MAC Address	given IP Address					

Available settings are explained as follows:

Item	Description
Network Configuration	<p>Enable/Disable - Click Enable to enable such configuration; click Disable to disable such configuration.</p> <p>For Routing Usage,</p> <ul style="list-style-type: none"> ● 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) <p>RIP Protocol Control,</p> <ul style="list-style-type: none"> ● 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	<p>DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.</p> <p>If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to</p>

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.

LAN 1 Ethernet TCP / IP and DHCP Setup
LAN 1 IPv6 Setup

Enable IPv6

WAN Primary Interface WAN1 ▼

Static IPv6 Address

IPv6 Address / Prefix Length

Unique Local Address(ULA) configuration

Off ▼ / 64

Current IPv6 Address Table

Index	IPv6 Address/Prefix Length	Scope
1	FE80::21D:A AFF:FEF7:COF0/64	Link

DNS Server IPv6 Address Deploy when WAN is up ▼

Primary DNS Server

Secondary DNS Server

Management SLAAC(stateless) ▼

Other Option(O-bit)

DHCPv6 Server

Enable Server Disable Server

Auto IPv6 range

Start IPv6 Address

End IPv6 Address

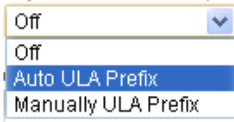
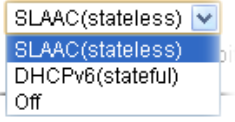
Advance setting

Advance setting

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

Available settings are explained as follows:

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.

	 <p>Auto ULA Prefix - The system will generate the required IPv6 address.</p> <p>Manually ULA Prefix - A user can type the ULA IPv6 address manually.</p>
Current IPv6 Address Table	Display current used IPv6 addresses.
DNS Server IPv6 Address	<p>Deploy when WAN is up - The RA (router advertisement) packets will be sent to LAN PC with DNS server information only when network connection by any one of WAN interfaces is up.</p> <p>Enable - The RA (router advertisement) packets will be sent to LAN PC with DNS server information no matter WAN connection is up or not.</p> <ul style="list-style-type: none"> ● Primary DNS Sever - Type the IPv6 address for Primary DNS server. ● Secondary DNS Server -Type another IPv6 address for DNS server if required. <p>Disable - DNS server will not be used.</p>
Management	<p>Host under LAN can be assigned IP address from Vigor router via the following method.</p>  <ul style="list-style-type: none"> ● SLAAC(stateless) - The IP address (with Prefix) of the host shall be formed according to RA transmitted by Vigor router. ● DHCPv6(stateful) - The IP address of the host shall be assigned after communicating with DHCPv6 server for answering the request of client. ● Off - No IP address is assigned. <p>Other Option (O-bit) - Check this box to enable the O-bit for obtaining additional information (e.g., DNS) from DHCPv6.</p>
DHCPv6 Server	<p>Enable Server -Click it to enable DHCPv6 server. DHCPv6 Server could assign IPv6 address to PC according to the Start/End IPv6 address configuration.</p> <p>Disable Server -Click it to disable DHCPv6 server.</p> <p>Auto IPv6 range - After check the box, Vigor router will assign the IPv6 range automatically.</p> <p>Start IPv6 Address / End IPv6 Address -Type the start and end address for IPv6 server.</p> <p>Advance setting - Click the Edit button to configure advanced IPv6 settings for DHCPv6 server.</p>

DHCPv6 Server

Authentication Protocol

Prefix Delegation Enable Disable

Prefix /

DHCPv6 Prefix Delegation

New Prefix

Suffix

New Prefix Length

Client Link Local Address

Client DUID(option)

Prefix	Prefix Length	Link Local	DUID

Advance setting

More options are offered under the **Advance setting**. Click **Edit** to open the pop-up window.

Router Advertisement Configuration

Enable Disable

Hop Limit

Min Interval Time(sec)

Max Interval Time(sec)

Default Lifetime(sec) (High Availability secondary is 0)

Default Preference

MTU Auto

RIPng Protocol

Enable

Extension WAN

Available WAN

Selected WAN

WAN2
WAN3
WAN4

Router Advertisement Configuration - Click **Enable** to enable router advertisement server. The router advertisement daemon sends Router Advertisement messages, specified by RFC 2461, to a local Ethernet LAN periodically and when requested by a node sending a Router Solicitation message. These messages are required for IPv6 stateless auto-configuration.

Disable - Click it to disable router advertisement server.

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

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

Default Lifetime (sec) - Within such period of time, 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.

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

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, 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 ~ P4) 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 Vigor2862ac:

VLAN Configuration

Enable

	LAN				Wireless LAN(2.4GHz)				Wireless LAN(5GHz)				VLAN Tag			
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
VLAN0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN15	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0

Permit untagged device in P1 to access router

Note:

1. For each VLAN row, selecting Enable VLAN Tag will apply the associated VID to the selected wired LAN port.
2. Wireless LAN traffic is always untagged, but the SSID is still a member of the selected VLAN (group).
3. Each VID must be unique.

OK Clear Cancel

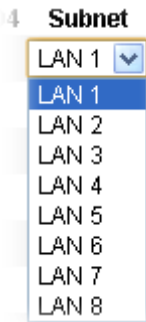


Info

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

Available settings are explained as follows:

Item	Description
Enable	Click it to enable VLAN configuration.
LAN	P1 - P4 - 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	<p>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.</p> 
VLAN Tag	<p>Enable - Check the box to enable the function of VLAN with tag.</p> <p>The router will add specific VLAN number to all packets on the LAN while sending them out.</p> <p>Please type the tag value and specify the priority for the packets sending by LAN.</p> <p>VID - Type the value as the VLAN ID number. The range is form 0 to 4095.</p> <p>Priority - Type the packet priority number for such VLAN. The range is from 0 to 7.</p>
Permit untagged device in P1 to access router	<p>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.</p>



Info

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

Vigor2862 series features a hugely flexible VLAN system. In its simplest form, each of the Gigabit LAN ports can be isolated from each other, for example to feed different companies or departments but keeping their local traffic completely separated.

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

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

LAN >> VLAN Configuration

VLAN Configuration

<input checked="" type="checkbox"/> Enable																
VLAN	LAN				Wireless LAN(2.4GHz)				Wireless LAN(5GHz)				VLAN Tag			
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
VLAN0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input checked="" type="checkbox"/>	0	0
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LAN 2	<input type="checkbox"/>	0	0
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 3	<input type="checkbox"/>	0	0
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0

- 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	DHCPv6	IP Address		
LAN 1	V	V	V	192.168.1.1	Details Page	IPv6
LAN 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.2.1	Details Page	IPv6
LAN 3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.3.1	Details Page	IPv6
LAN 4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.4.1	Details Page	IPv6
LAN 5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.5.1	Details Page	IPv6
LAN 6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.6.1	Details Page	IPv6
LAN 7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.7.1	Details Page	IPv6
LAN 8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.8.1	Details Page	IPv6
DMZ Port	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.17.1	Details Page	IPv6
IP Routed Subnet	<input type="checkbox"/>	<input checked="" type="checkbox"/>		192.168.0.1	Details Page	

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

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

Inter-LAN Routing

Subnet	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5	LAN 6	LAN 7	LAN 8	DMZ Port
LAN 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
DMZ Port	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Note:

LAN2/3/4/5/6/7/8 are available when VLAN is enabled.
DMZ subnet is default bound to P4, and will overwrite the settings of P4 at LAN>>VLAN page.

[OK](#)

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



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

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

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

LAN >> Bind IP to MAC

Bind IP to MAC

Enable Disable

Strict Bind

Apply Strict Bind to Subnet

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

IP Address	Mac Address	HOST ID
192.168.1.10	00-05-5D-E4-D8-EE	A1000351

IP Address

Mac Address : : : : :

Comment

IP Bind List (Limit: 1024 entries) | [Select All](#) | [Sort](#)

Index	IP Address	Mac Address	Host ID	Comment
-------	------------	-------------	---------	---------

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

Note:

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

Available settings are explained as follows:

Item	Description
Enable	Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.
Disable	Click this radio button to disable this function. All the settings on this page will be invalid.
Strict Bind	Check the box to block the connection of the IP/MAC which is not listed in IP Bind List. Apply Strict Bind to Subnet – Choose the subnet(s) for applying the rules of Bind IP to MAC.

	<p>2.168.1.1/doc/lansubed1.htm</p> <p>Apply Strict Bind to Subnet:</p> <p><input type="button" value="Select All"/> <input type="button" value="Clear All"/></p> <table border="1"> <thead> <tr> <th>Subnet</th> <th>IP Address</th> </tr> </thead> <tbody> <tr><td><input type="checkbox"/> LAN1</td><td>192.168.1.1</td></tr> <tr><td><input type="checkbox"/> LAN2</td><td>192.168.2.1</td></tr> <tr><td><input type="checkbox"/> LAN3</td><td>192.168.3.1</td></tr> <tr><td><input type="checkbox"/> LAN4</td><td>192.168.4.1</td></tr> <tr><td><input type="checkbox"/> LAN5</td><td>192.168.5.1</td></tr> <tr><td><input type="checkbox"/> LAN6</td><td>192.168.6.1</td></tr> <tr><td><input type="checkbox"/> LAN7</td><td>192.168.7.1</td></tr> <tr><td><input type="checkbox"/> LAN8</td><td>192.168.8.1</td></tr> <tr><td><input type="checkbox"/> DMZ Port</td><td>192.168.17.1</td></tr> <tr><td><input type="checkbox"/> IP Routed Subnet</td><td>192.168.0.1</td></tr> </tbody> </table> <p><input type="button" value="OK"/> <input type="button" value="Close"/></p>	Subnet	IP Address	<input type="checkbox"/> LAN1	192.168.1.1	<input type="checkbox"/> LAN2	192.168.2.1	<input type="checkbox"/> LAN3	192.168.3.1	<input type="checkbox"/> LAN4	192.168.4.1	<input type="checkbox"/> LAN5	192.168.5.1	<input type="checkbox"/> LAN6	192.168.6.1	<input type="checkbox"/> LAN7	192.168.7.1	<input type="checkbox"/> LAN8	192.168.8.1	<input type="checkbox"/> DMZ Port	192.168.17.1	<input type="checkbox"/> IP Routed Subnet	192.168.0.1
Subnet	IP Address																						
<input type="checkbox"/> LAN1	192.168.1.1																						
<input type="checkbox"/> LAN2	192.168.2.1																						
<input type="checkbox"/> LAN3	192.168.3.1																						
<input type="checkbox"/> LAN4	192.168.4.1																						
<input type="checkbox"/> LAN5	192.168.5.1																						
<input type="checkbox"/> LAN6	192.168.6.1																						
<input type="checkbox"/> LAN7	192.168.7.1																						
<input type="checkbox"/> LAN8	192.168.8.1																						
<input type="checkbox"/> DMZ Port	192.168.17.1																						
<input type="checkbox"/> IP Routed Subnet	192.168.0.1																						
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 to IP Bind List	<p>IP Address – Type the IP address that will be used for the specified MAC address.</p> <p>Mac Address – Type the MAC address that is used to bind with the assigned IP address.</p> <p>Comment – Type a brief description for the entry.</p> <p>Show Comment – Check this box to display the comment on IP Bind List box.</p>																						
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 .																						
IP Bind List	It displays a list for the IP bind to MAC information.																						
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:
 Enable Disable

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

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

OK

Available settings are explained as follows:

Item	Description
Port Mirror	Check Enable to activate this function. Or, check Disable to close this function.
Mirror Port	Select a port to view traffic sent from mirrored ports.
Mirrored Tx Port	Select which ports are necessary to be mirrored for transmitting the packets.
Mirrored Rx Port	Select which ports are necessary to be mirrored for receiving the packets.

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

II-2-5 Wired 802.1x

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

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

LAN >> Wired 802.1X

Wired 802.1X

LAN 802.1X: <input checked="" type="checkbox"/> Enable Authentication Type: External RADIUS ▾ 802.1X ports: <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4

Note:

1. 802.1X enabled LAN ports only support a single attached device using EAPOL authentication. To authenticate multiple devices through a LAN port you need an 802.1X-capable switch. Then configure 802.1X on the attached switch instead.
2. Please configure **External RADIUS** or **Local 802.1X** for authentication.
3. Authentication by External RADIUS supports PEAP and EAP-TLS.

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-3 Hardware Acceleration

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



Info

Such feature is only supported by certain firmware version.

II-3-1 Setup

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

Hardware Acceleration >> Setup

Mode:

Protocol: TCP UDP

Option: Accelerate heaviest traffic sessions

Apply the **Class Rule** in Quality of Service

Specific Hosts:

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

WAN Information:

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

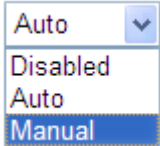
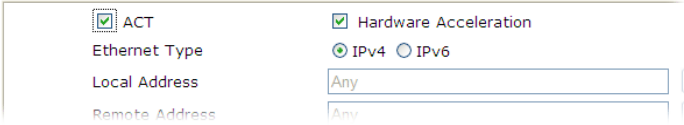
	Status	TX	RX
WAN1-ADSL	Disable	--	--
WAN2-Ethernet	Enable	V	V

Note:

If Hardware Acceleration is enabled, then individual sessions processed by the accelerator will by-pass the following features: Data Flow Monitor, Traffic Graph, WAN Budget.

Available settings are explained as follows:

Item	Description
Mode	<p>Disable - The default setting.</p> <p>Auto - When the hardware acceleration is configured with the Auto mode, the sessions with the heaviest loading and the lower latency traffic will be added into PPA. However,</p>

	<p>the Auto mode does not support UDP protocol by designed.</p> <p>Manual - The Manual mode implements three sub-items-- <i>Accelerate most heavy traffic sessions</i>, <i>Apply the Class Rule in Quality of Service</i>, and <i>Specific Hosts</i>. Each of these sub-items can support TCP and UDP protocol.</p> 
Protocol	<p>There are two types supported by this function, TCP and UDP.</p>
Option	<p>Accelerate heaviest traffic sessions - Such option is available in Auto Mode, too. But the UDP protocol is only supported in this sub-item.</p> <p>Apply the Class Rule in Quality of Service - Users can apply the information provided by QoS in this sub-item.</p> <p>Please visit our website for referring the detailed configuration of QoS.</p> <p>Bandwidth Management >> Quality of Service</p> <hr/> <p>Rule Edit</p>  <p>Specific Hosts - This sub-item provides 5 hosts for adding NAT sessions into the PPA. For the PPA only supports 128 sessions, these hosts will share these sessions. Therefore, the performance will be lower than only one host.</p> <p>Choose this option to specify certain PCs on LAN to apply the hardware acceleration.</p> <ul style="list-style-type: none"> ● Enable - Check the box to make PC(s) specified in the selected index entry to be applied. ● Dest Port Start - Type the starting port for the PC(s) in LAN. ● Dest Port End - Type the ending port for the PC(s) in LAN. ● Private IP/Choose PC - Type the IP address as the selected host. Or click the Choose PC button to specify one IP address from the pop-up window.

Checking the PPA status

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

```

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

```

II-4 NAT

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

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

The benefit of the NAT includes:

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



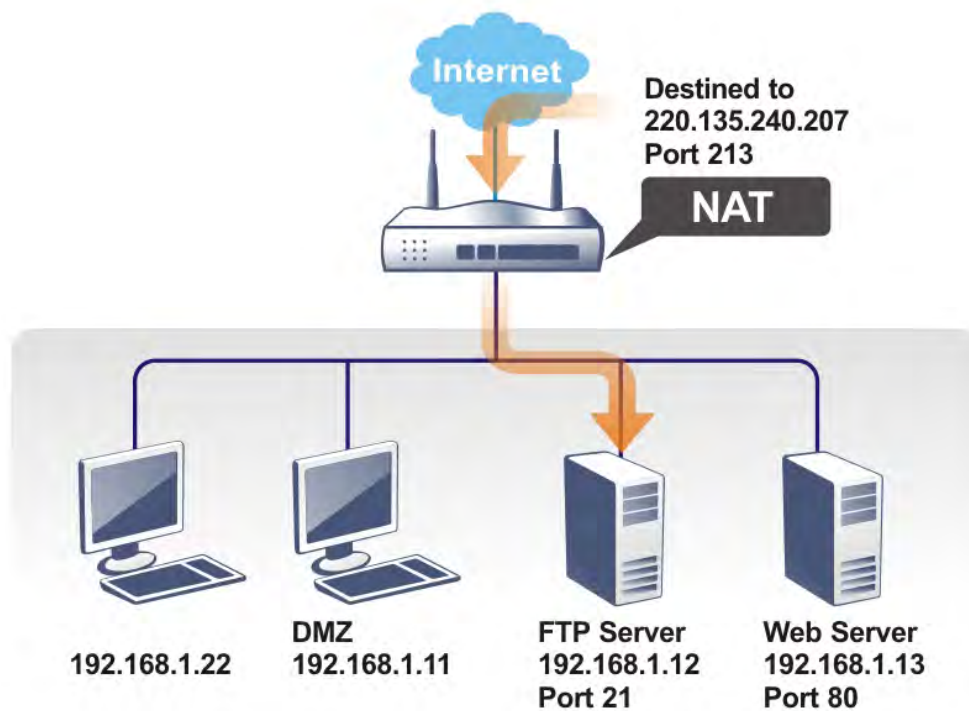
Info

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

Web User Interface

II-4-1 Port Redirection

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



The port redirection can only apply to incoming traffic.

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

NAT >> Port Redirection

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

Index	Service Name	WAN Interface	Protocol	Public Port	Source IP	Private IP	Status
<u>1.</u>		All			Any		x
<u>2.</u>		All			Any		x
<u>3.</u>		All			Any		x
<u>4.</u>		All			Any		x
<u>5.</u>		All			Any		x
<u>6.</u>		All			Any		x
<u>7.</u>		All			Any		x
<u>8.</u>		All			Any		x
<u>9.</u>		All			Any		x
<u>10.</u>		All			Any		x

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

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

Each item is explained as follows:

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

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

NAT >> Port Redirection

Index No. 1

Enable

Mode Range

Service Name

Protocol TCP

WAN Interface ALL

Public Port -

Source IP Any **IP Object**

Private IP -

Private Port

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

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable such port redirection setting.
Mode	Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select Range . In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered, the system will calculate and display the ending IP of private IP automatically.
Service Name	Enter the description of the specific network service.
Protocol	Select the transport layer protocol (TCP or UDP).
WAN Interface	Select the WAN interface used for port redirection. There are eight WAN IP alias that can be selected and used for port redirection. The default setting is All which means all the incoming data from any port will be redirected to specified range of IP address and port.
Public Port	Specify which port can be redirected to the specified Private IP and Port of the internal host. If you choose Range as the port redirection mode, you will see two boxes on this field. Type the required number on the first box (as the starting port) and the second box (as the ending port).
Source IP	Use the drop down list to specify an IP object. Or click IP Object link to create a new one for applying.
Private IP	Specify the private IP address of the internal host providing the service. If you choose Range as the port redirection mode, you will see two boxes on this field. Type a complete IP address in the first box (as the starting point). The second one will be assigned automatically later.
Private Port	Specify the private port number of the service offered by the internal host.

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

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

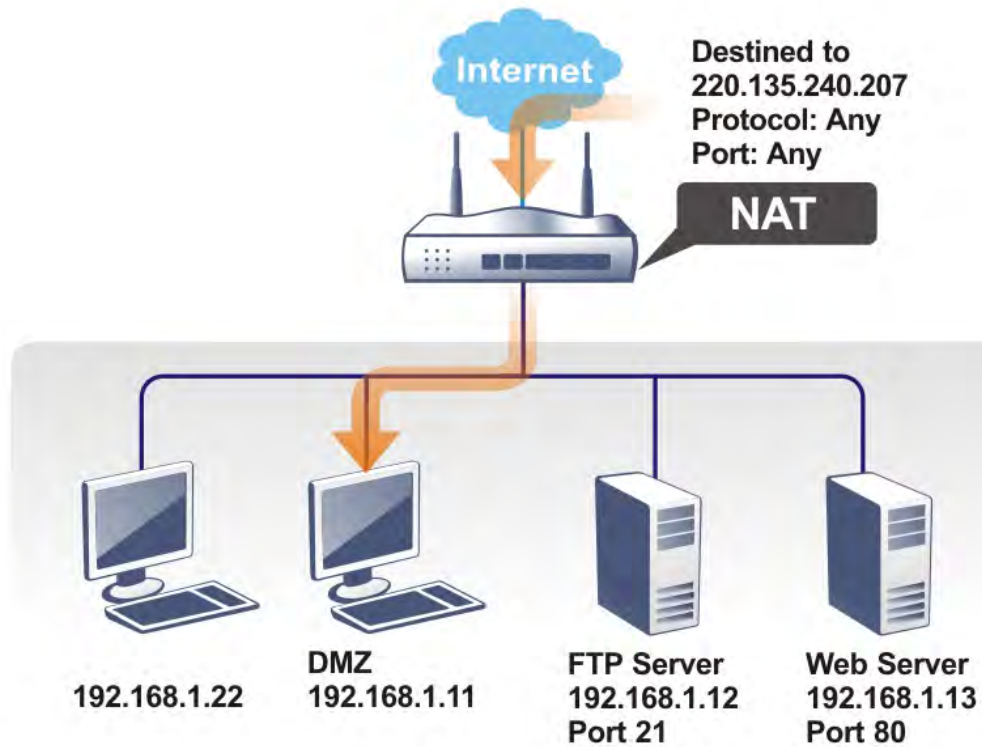
For example, the built-in web user interface in the router is with default port 80, which may conflict with the web server in the local network, `http://192.168.1.13:80`. Therefore, you need to **change the router's http port to any one other than the default port 80** to avoid conflict, such as 8080.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



IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup						
Router Name <input type="text" value="DrayTek"/>								
<input type="checkbox"/> Default:Disable Auto-Logout <input type="checkbox"/> Enable Validation Code in Internet/LAN Access	Management Port Setup <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports							
Internet Access Control <input type="checkbox"/> Allow management from the Internet Domain name allowed <input type="text"/> <input type="checkbox"/> FTP Server <input type="checkbox"/> HTTP Server <input checked="" type="checkbox"/> HTTPS Server <input type="checkbox"/> Telnet Server <input type="checkbox"/> TR069 Server <input type="checkbox"/> SSH Server <input checked="" type="checkbox"/> Disable PING from the Internet	Telnet Port <input type="text" value="23"/> (Default: 23) HTTP Port <input type="text" value="80"/> (Default: 80) HTTPS Port <input type="text" value="443"/> (Default: 443) FTP Port <input type="text" value="21"/> (Default: 21) TR069 Port <input type="text" value="8069"/> (Default: 8069) SSH Port <input type="text" value="22"/> (Default: 22)							
Access List from the Internet <table border="0"> <tr> <td>List</td> <td>index in</td> <td>IP / Mask</td> </tr> <tr> <td></td> <td><u>IP Object</u></td> <td></td> </tr> </table>	List	index in	IP / Mask		<u>IP Object</u>		Brute Force Protection <input type="checkbox"/> Enable brute force login protection <input type="checkbox"/> FTP Server <input type="checkbox"/> HTTP Server <input type="checkbox"/> HTTPS Server <input type="checkbox"/> Telnet Server	
List	index in	IP / Mask						
	<u>IP Object</u>							

II-4-2 DMZ Host

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



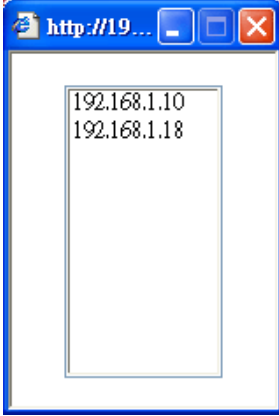
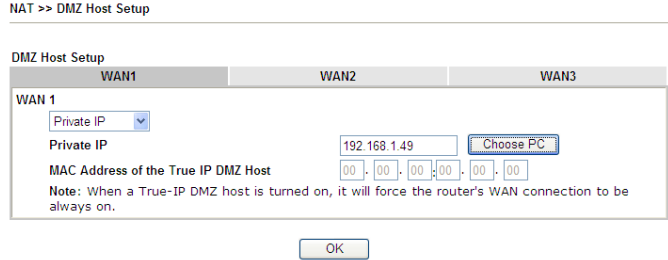
The security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

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

NAT >> DMZ Host Setup

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


Available settings are explained as follows:

Item	Description
WAN 1	Choose Private IP or None first.
Private IP	Enter the private IP address of the DMZ host, or click Choose PC to select one.
Choose IP	<p>Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.</p>  <p>When you have selected one private IP from the above dialog, the IP address will be shown on the following screen. Click OK to save the setting.</p> <p>NAT >> DMZ Host Setup</p> 

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.

NAT >> DMZ Host Setup



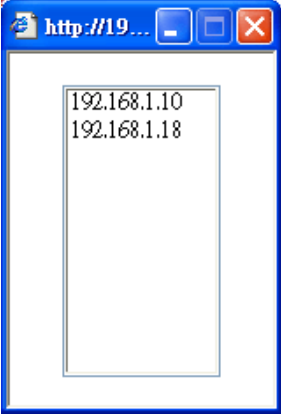
If you previously have set up WAN Alias for PPPoE or Static or Dynamic IP mode in WAN2 interface, you will find them in Aux. WAN IP for your selection.

NAT >> DMZ Host Setup

DMZ Host Setup

WAN1		WAN2		WAN3		WAN4	
WAN 2							
Index	Enable	Aux. WAN IP	Private IP				
1.	<input type="checkbox"/>	10.39.0.10	<input type="text" value="0.0.0.0"/>		<input type="button" value="Choose IP"/>		
2.	<input type="checkbox"/>	10.39.0.150	<input type="text" value="0.0.0.0"/>		<input type="button" value="Choose IP"/>		

Available settings are explained as follows:

Item	Description
Enable	Check to enable the DMZ Host function.
Private IP	Enter the private IP address of the DMZ host, or click Choose PC to select one.
Choose IP	<p>Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.</p>  <p>When you have selected one private IP from the above dialog, the IP address will be shown on the screen. Click OK to save the setting.</p>

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

II-4-3 Open Ports

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

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

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

NAT >> Open Ports

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

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

[Next](#) >>

Note:

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

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.
Source IP	Display the name of the IP object.
Local IP Address	Display the private IP address of the local host offering the service.
Status	Display the state for the corresponding entry. X or V is to represent the Inactive or Active state.

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

Index No. 1

Enable Open Ports

Comment

WAN Interface

Source IP **IP Object**

Private IP

	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	2.	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
3.	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	4.	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
5.	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	6.	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
7.	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	8.	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
9.	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	10.	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

Available settings are explained as follows:

Item	Description
Enable Open Ports	Check to enable this entry.
Comment	Make a name for the defined network application/service.
WAN Interface	Specify the WAN interface that will be used for this entry.
Source IP	Use the drop down list to specify an IP object. Or click IP Object link to create a new one for applying.
WAN IP	Specify the WAN IP address that will be used for this entry. This setting is available when WAN IP Alias is configured.
Private IP	Enter the private IP address of the local host or click Choose PC to select one. Choose IP - Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select the appropriate IP address of the local host in the list.
Protocol	Specify the transport layer protocol. It could be TCP, UDP, or ----- (none) for selection.
Start Port	Specify the starting port number of the service offered by the local host.
End Port	Specify the ending port number of the service offered by the local host.

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

NAT >> Open Ports

Open Ports Setup				Set to Factory Default
Index	Comment	WAN Interface	Local IP Address	Status
<u>1.</u>	P2261	WAN1	192.168.1.49	v
<u>2.</u>				x
<u>3.</u>				x
<u>4.</u>				x
<u>5.</u>				x
<u>6.</u>				x
<u>7.</u>				x

II-4-4 Port Triggering

Port Triggering is a variation of open ports function.

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

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

TCP: 86400 sec.

UDP: 180 sec.

IGMP: 10 sec.

TCP WWW: 60 sec.

TCP SYN: 60 sec.

NAT >> Port Triggering

Port Triggering							Set to Factory Default
Index	Comment	Triggering Protocol	Source IP	Triggering Port	Incoming Protocol	Incoming Port	Status
<u>1.</u>							x
<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
<u>10.</u>							x

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

[Next](#) >>

Available settings are explained as follows:

Item	Description
Comment	Display the text which memorizes the application of this

	rule.
Triggering Protocol	Display the protocol of the triggering packets.
Triggering Port	Display the port of the triggering packets.
Source IP	Display the name of the IP object.
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.

NAT >> Port Triggering

No. 1

Enable
Service User Defined ▾
Comment
Source IP Any ▾ **IP Object**
Triggering Protocol TCP ▾
Triggering Port
Incoming Protocol TCP/UDP ▾
Incoming Port

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

Available settings are explained as follows:

Item	Description
Enable	Check to enable this entry.
Service	Choose the predefined service to apply for such trigger profile. <div style="border: 1px solid black; padding: 2px; margin-top: 5px;"> User Defined ▾ User Defined Real Player QuickTime WMP IRC AIM Talk ICQ PaITalk BitTorrent </div>
Comment	Type the text to memorize the application of this rule.
Source IP	Use the drop down list to specify an IP object. Or click IP Object link to create a new one for applying.
Triggering Protocol	Select the protocol (TCP, UDP or TCP/UDP) for such triggering profile.

Triggering Port	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-4-5 ALG

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

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

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

NAT >> ALG

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

Enable ALG

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

Available settings are explained as follows:

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

II-5 Applications

Dynamic DNS

The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router to update its online WAN IP address mappings on the specified Dynamic DNS server. Once the router is online, you will be able to use the registered domain name to access the router or internal virtual servers from the Internet. It is particularly helpful if you host a web server, FTP server, or other server behind the router.

Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers. The router provides up to three accounts from three different DDNS service providers. Basically, Vigor routers are compatible with the DDNS services supplied by most popular DDNS service providers such as www.dyndns.org, www.no-ip.com, www.dtdns.com, www.changeip.com, www.dynamic-nameserver.com. You should visit their websites to register your own domain name for the router.

LAN DNS / DNS Forwarding

The LAN DNS lets the network administrators host servers with privacy and security. When the network administrators of your office set up FTP, Mail or Web server inside LAN, you can specify specific private IP address (es) to correspondent servers. Thus, even the remote PC is adopting public DNS as the DNS server, the LAN DNS resolution on Vigor2862 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-5-1 Dynamic DNS

Enable the Function and Add a Dynamic DNS Account

1. Assume you have a registered domain name from the DDNS provider, say *hostname.dyndns.org*, and an account with username: *test* and password: *test*.
2. Open Applications>>Dynamic DNS.
3. In the DDNS setup menu, check Enable Dynamic DNS Setup.

Applications >> Dynamic DNS Setup

Dynamic DNS Setup | Set to Factory Default |

Enable Dynamic DNS Setup

Auto-Update interval Min(s) (1~14400)

Accounts:

Index	WAN Interface	Domain Name	Active
<u>1.</u>	WAN1 First	vigor2925.ubddns.org	v
<u>2.</u>	WAN1 First		x
<u>3.</u>	WAN1 First		x
<u>4.</u>	WAN1 First		x
<u>5.</u>	WAN1 First		x
<u>6.</u>	WAN1 First		x

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*.

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

Index : 1

Enable Dynamic DNS Account

WAN Interface:

Service Provider:

Service Type:

Domain Name: .

Login Name: (max. 64 characters)

Password: (max. 64 characters)

Wildcards

Backup MX

Mail Extender:

Determine WAN IP:

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

Index : 1

<input checked="" type="checkbox"/>	Enable Dynamic DNS Account
WAN Interface	WAN1 First ▾
Service Provider	Customized ▾
Provider Host	changeip.org
Service API	<pre>/dynamic/dns/update.asp? u=jos...cp=jos...hostname=j...changeip.org&ip=###IP###&sc md=update&offline=0</pre>
Auth Type	basic ▾
Connection Type	Http ▾
Server Response	
Login Name	chronic6653 (max. 64 characters)
Password (max. 23 characters)
<input type="checkbox"/>	Wildcards
<input type="checkbox"/>	Backup MX
Mail Extender	
Determine Real WAN IP	Internet IP ▾

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
WAN Interface	WAN1/WAN2/WAN3/WAN4 First - While connecting, the router will use WAN1/WAN2/WAN3/WAN4 as the first channel for such account. If WAN1/WAN2/WAN3 /WAN4 fails, the router will use another WAN interface instead. WAN1/WAN2/WAN3/WAN4 Only - While connecting, the router will use WAN1/WAN2/WAN3/WAN4 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 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: <ul style="list-style-type: none"> ● WAN IP - If it is selected and the WAN IP of Vigor router is private, DDNS update will take place right away. ● Internet IP - If it is selected and the WAN IP of Vigor router is private, it will be converted to public IP before DDNS update takes place.

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

Disable the Function and Clear all Dynamic DNS Accounts

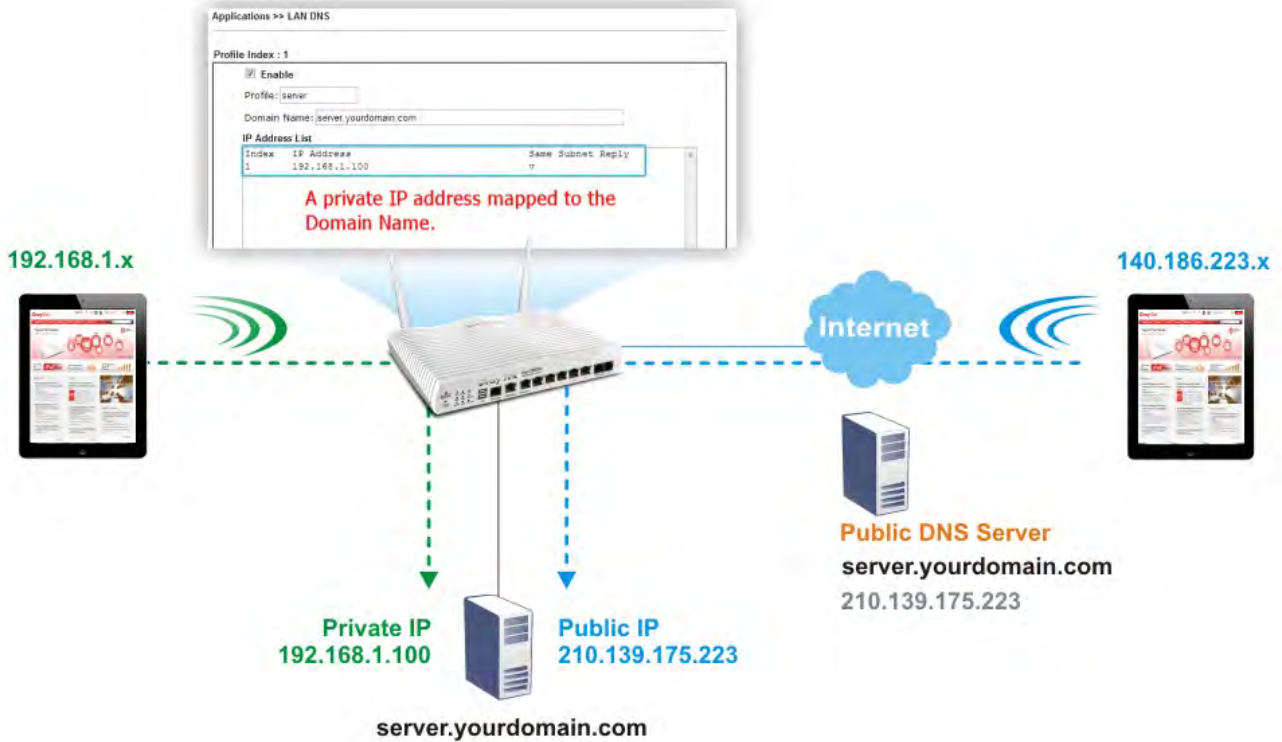
Uncheck **Enable Dynamic DNS Setup**, and click **Clear All** button to disable the function and clear all accounts from the router.

Delete a Dynamic DNS Account

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

II-5-2 LAN DNS / DNS Forwarding

The LAN DNS lets the network administrators host servers with privacy and security. When the network administrators of your office set up FTP, Mail or Web server inside LAN, you can specify specific private IP address (es) to correspondent servers. Thus, even the remote PC is adopting public DNS as the DNS server, the LAN DNS resolution on Vigor2862 series will respond the specified private IP address.



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

Applications >> LAN DNS / DNS Forwarding

LAN DNS Resolution / Conditional DNS Forwarding						Set to Factory Default
Enable	Index	Profile	Domain Name	Forwarding	DNS Server	
<input type="checkbox"/>	1.			-		
<input type="checkbox"/>	2.			-		
<input type="checkbox"/>	3.			-		
<input type="checkbox"/>	4.			-		
<input type="checkbox"/>	5.			-		
<input type="checkbox"/>	6.			-		
<input type="checkbox"/>	7.			-		
<input type="checkbox"/>	8.			-		
<input type="checkbox"/>	9.			-		
<input type="checkbox"/>	10.			-		

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

OK

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profiles and recover to factory settings.
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 address of the DNS Server.

To create a LAN DNS profile:

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

Applications >> LAN DNS / DNS Forwarding

LAN DNS
Conditional DNS Forwarding

Profile Index : 1

Enable

Profile:

Domain Name:

Note:

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

CNAME(Alias Domain Name):

IP Address List

Index	IP Address	Same Subnet Reply

Available settings are explained as follows:

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

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

Available settings are explained as follows:

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

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

II-5-3 DNS Security

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

II-5-3-1 General Setup

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

Application >> DNS Security



DNS Security

General Setup		Domain Diagnose		Refresh
Enable	Interface	Primary DNS	Secondary DNS	Bogus DNS Reply
<input type="checkbox"/>	WAN1	---	---	Pass ▼
<input type="checkbox"/>	WAN2	---	---	Pass ▼
<input type="checkbox"/>	WAN3	---	---	Pass ▼
<input type="checkbox"/>	WAN4	---	---	Pass ▼

Note:



The DNS server supports DNSSEC



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

OK

Available settings are explained as follows:

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

II-5-3-2 Domain Diagnose

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

Application >> DNS Security



DNS Security

General Setup | **Domain Diagnose** | **DNS Cache**

Domain: IPv4 IPv6

Interface:

DNS Server:

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

Result

Domain Name	IP Address	Interface	Verify Result

Available settings are explained as follows:

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

II-5-4 Schedule

The Vigor router has a built-in clock which can update itself manually or automatically by means of Network Time Protocols (NTP). As a result, you can not only schedule the router to dialup to the Internet at a specified time, but also restrict Internet access to certain hours so that users can connect to the Internet only during certain hours, say, business hours. The schedule is also applicable to other functions.

You have to set your time before set schedule. In **System Maintenance>> Time and Date** menu, press **Inquire Time** button to set the Vigor router's clock to current time of your PC. The clock will reset once if you power down or reset the router. There is another way to set up time. You can inquiry an NTP server (a time server) on the Internet to synchronize the router's clock. This method can only be applied when the WAN connection has been built up.

Applications >> Schedule

Schedule : Current System Time | [System time set](#) | [Set to Factory Default](#) |

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

Force on Force down

Available settings are explained as follows:

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

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

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

To add a schedule:

1. Click any index, say Index No. 1.
2. The detailed settings of the schedule with index 1 will be shown below.

Applications >> Schedule

Index No. 1 Current System Time 2017 Oct 16 Mon 2 : 41 : 7 | System time set |

Enable Schedule Setup

Comment: Ready for RD

Start Date (yyyy-mm-dd): 2016 - 1 - 1

Start Time (hh:mm): 1 : 1

Duration Time (hh:mm): 22 : 0

End Time (hh:mm): 23 : 01

Action: Force On

How Often

Once

Weekdays

Sun Mon Tue Wed Thu Fri Sat

Monthly, on date 1

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

Note:

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

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Enable Schedule Setup	Check to enable the schedule.
Comment	Type a short description for such schedule.
Start Date (yyyy-mm-dd)	Specify the starting date of the schedule.
Start Time (hh:mm)	Specify the starting time of the schedule.
Duration Time (hh:mm)	Specify the duration (or period) for the schedule.
End Time (hh:mm)	It will be calculated automatically when Start Time and Duration Time are configured well.
Action	Specify which action Call Schedule should apply during the period of the schedule. Force On -Force the connection to be always on.

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

3. Click OK button to save the settings.

Example

Suppose you want to control the PPPoE Internet access connection to be always on (Force On) from 9:00 to 18:00 for whole week. Other time the Internet access connection should be disconnected (Force Down).

Office
Hour:
(Force On)



Mon - Sun 9:00 am to 6:00 pm

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

II-5-5 RADIUS/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-5-5-1 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.

External RADIUS	Internal RADIUS	External TACACS+
<input type="checkbox"/> Enable		
Server IP Address		<input type="text"/>
Destination Port		<input type="text" value="1812"/>
Shared Secret		<input type="text"/>
Confirm Shared Secret		<input type="text"/>

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

Available settings are explained as follows:

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

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

II-5-5-2 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.

External RADIUS
Internal RADIUS
External TACACS+

Enable

Authentication Port

RADIUS Client Access List

Index	Enable	Shared Secret	IP Address	IP Mask	IPv6 Address	IPv6 Length
1	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="::"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="::"/>	<input type="text" value="0"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="::"/>	<input type="text" value="0"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="::"/>	<input type="text" value="0"/>
5	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="::"/>	<input type="text" value="0"/>
6	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="::"/>	<input type="text" value="0"/>
7	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="::"/>	<input type="text" value="0"/>
8	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="::"/>	<input type="text" value="0"/>
9	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="::"/>	<input type="text" value="0"/>
10	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="::"/>	<input type="text" value="0"/>

Authentication

Method

802.1X Method

Support 802.1X Method

Phase 1: PEAP
Phase 2: MS-CHAPv2

User Profile

Available List

>>

<<

Authentication List

Synchronize Internal RADIUS user list to Local 802.1X user list.

Note:
 1. Only the user profiles which is enabled in **User Management >> User Profile** will be listed here, and it shows in the **System Maintenance >> Internal Service User List**.
 2. RADIUS Client Access List is first match.

Available settings are explained as follows:

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.

	<p>IP Address - Type the IP address of the wired/wireless client.</p> <p>IP Mask - Type the subnet mask required for the IP address.</p> <p>IPv6 Address - Type the IPv6 address of the wired/wireless client.</p> <p>IPv6 Length - Type the prefix length required for the IPv6 address.</p>
Authentication	<p>Specify the way to authenticate the wireless client.</p> <p>PAP Only / PAP/CHAP/MS-CHAP/MS-CHAPv2 - Choose PAP Only. Or choose the one which supports PAP, CHAP, MS-CHAP and MS-CHAPv2.</p> <p>Support 802.1X Method - The built in RADIUS server offered by Vigor router can act as the AAA server. Check the box to enable the function of authentication mechanism.</p>
User Profile	<p>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.</p> <p>Select All - Click it to select all of the user profiles in Available List.</p> <p>Clear All- Click to remove all of the user profiles in Available List.</p> <p>Available List - The user profiles without RADIUS server enabled in User Management >> User Profile will be listed in this field.</p> <p>Authentication List -The user profiles with RADIUS server enabled in User Management >> User Profile will be listed in this field.</p>
Synchronize Internal RADIUS user list to Local 802.1X user list	<p>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.</p> <p>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.</p>

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

II-5-5-3 External TACACS+

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

Applications >> RADIUS/TACACS+

External RADIUS Internal RADIUS External TACACS+

Enable

Server IP Address

Destination Port

Type

Shared Secret

Confirm Shared Secret

OK Clear Cancel

Available settings are explained as follows:

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.

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

II-5-6 Active Directory/LDAP

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

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

II-5-6-1 General Setup

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

Applications >> Active Directory /LDAP

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

General Setup

Active Directory / LDAP Profiles

Enable

Bind Type Simple Mode ▾

Server Address

Destination Port

Use SSL

Regular DN

Regular Password

Note:
 After finishing the configuration of the LDAP profiles, they will be listed in the page of **VPN and Remote Access >> PPP General Setup**. If you want to use the profiles for VPN authentication, check the boxes under PPTP LDAP Profiles in **VPN and Remote Access >> PPP General Setup** first.

Available settings are explained as follows:

Item	Description
Enable	Check to enable such function.
Bind Type	<p>There are three types of bind type supported.</p> <ul style="list-style-type: none"> ● 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. <p>For the regular mode, you'll need to type in the Regular DN and Regular Password.</p>

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

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

II-5-6-2 Profiles

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

Applications >> Active Directory /LDAP

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

General Setup

Active Directory / LDAP Profiles

Index	Name	Distinguished Name
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		

Note:
After finishing the configuration of the LDAP profiles, they will be listed in the page of **VPN and Remote Access >> PPP General Setup**. If you want to use the profiles for VPN authentication, check the boxes under PPTP LDAP Profiles in **VPN and Remote Access >> PPP General Setup** first.

Click any index number link to open the following page.

Applications >> Active Directory /LDAP>>Server Profiles

Index No. 1

Name

Common Name Identifier

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

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 OK to save and exit this page. A new profile has been created.

II-5-7 UPnP

The UPnP (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on the router is "NAT Traversal". This enables applications inside the firewall to automatically open the ports that they need to pass through a router.



Info

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

Applications >> UPnP

UPnP

<input checked="" type="checkbox"/> Enable UPnP Service	Default WAN ▾
<input type="checkbox"/> Enable Connection Control Service	Default WAN
<input type="checkbox"/> Enable Connection Status Service	WAN1
	WAN2
	WAN3
	WAN4

Note:

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

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Enable UPNP Service	Accordingly, you can enable either the Connection Control Service or Connection Status Service.
Default WAN	It is used to specify the WAN interface for applying such function.

The reminder as regards concern about Firewall and UPnP:

Can't work with Firewall Software

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

Security Considerations

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

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

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

II-5-8 IGMP

IGMP is the abbreviation of *Internet Group Management Protocol*. It is a communication protocol which is mainly used for managing the membership of Internet Protocol multicast groups.

II-5-8-1 General Setting

Applications >> IGMP

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

Available settings are explained as follows:

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

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

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

II-5-8-2 Working Group

Applications >> IGMP

General setting	Working groups				
Refresh					
Working Multicast Groups					
Index	Group ID	P1	P2	P3	P4

Available settings are explained as follows:

Item	Description
Refresh	Click this link to renew the working multicast group status.
Group ID	This field displays the ID port for the multicast group. The available range for IGMP starts from 224.0.0.0 to 239.255.255.254.
P1 to P4	It indicates the LAN port used for the multicast group.

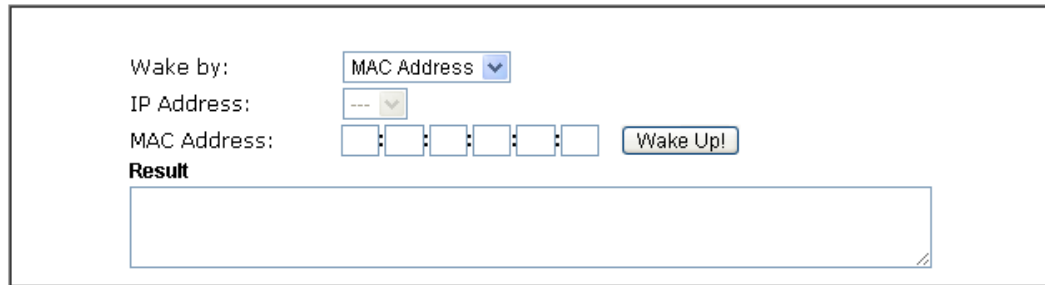
II-5-9 Wake on LAN

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.

Applications >> Wake on LAN

Wake on LAN



Note:

Wake on LAN integrates with **Bind IP to MAC** function, only binded PCs can wake up through IP.

Available settings are explained as follows:

Item	Description
Wake by	Two types provide for you to wake up the binded IP. <ul style="list-style-type: none">● 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-5-10 SMS / Mail Alert Service

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

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

II-5-10-1 SMS Alert

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

Applications >> SMS / Mail Alert Service

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

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

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 phone number of the one who will receive the SMS.
Notify Profile	Use the drop down list to choose a message profile. The recipient will get the content stated in the message profile. You can click the Notify Profile link to define the content of the SMS.
Schedule (1-15)	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.

II-5-10-2 Mail Alert

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

Application >> SMS / Mail Alert Service

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

Note:

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

Available settings are explained as follows:

Item	Description
Index	Check the box to enable such profile.
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.
Mail Address	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.

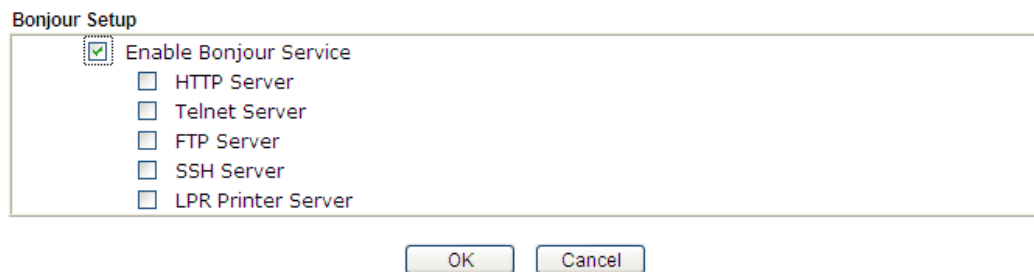
II-5-11 Bonjour

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

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

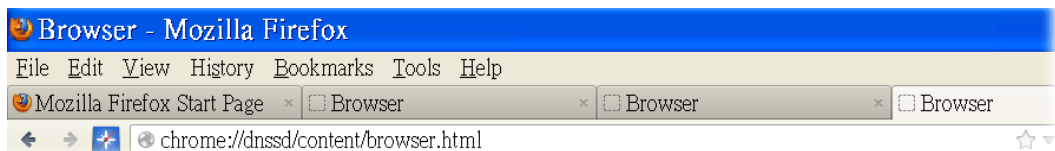
To enable the Bonjour service, click **Application>>Bonjour** to open the following page. Check the box(es) of the server service(s) that you want to share to the LAN clients.

Applications >> Bonjour

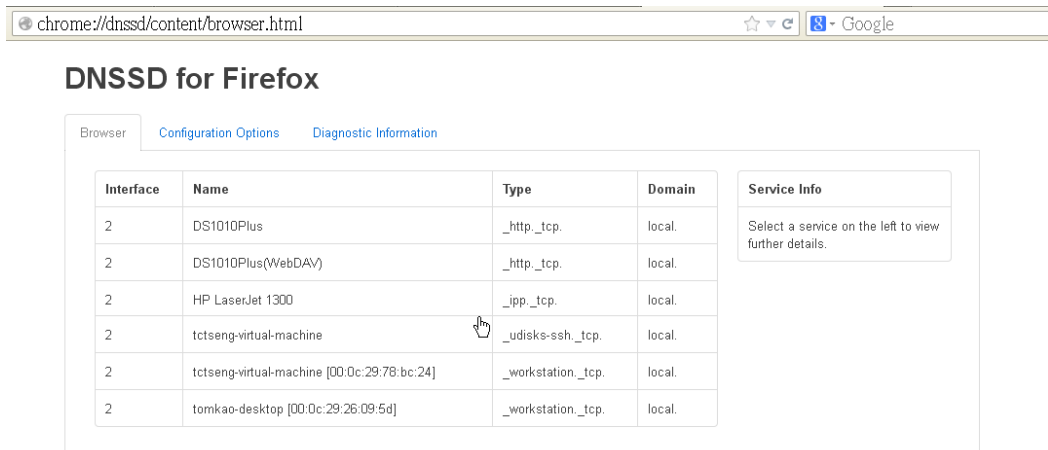


Below shows an example for applying the Bonjour feature that Vigor router can be used as the FTP server.

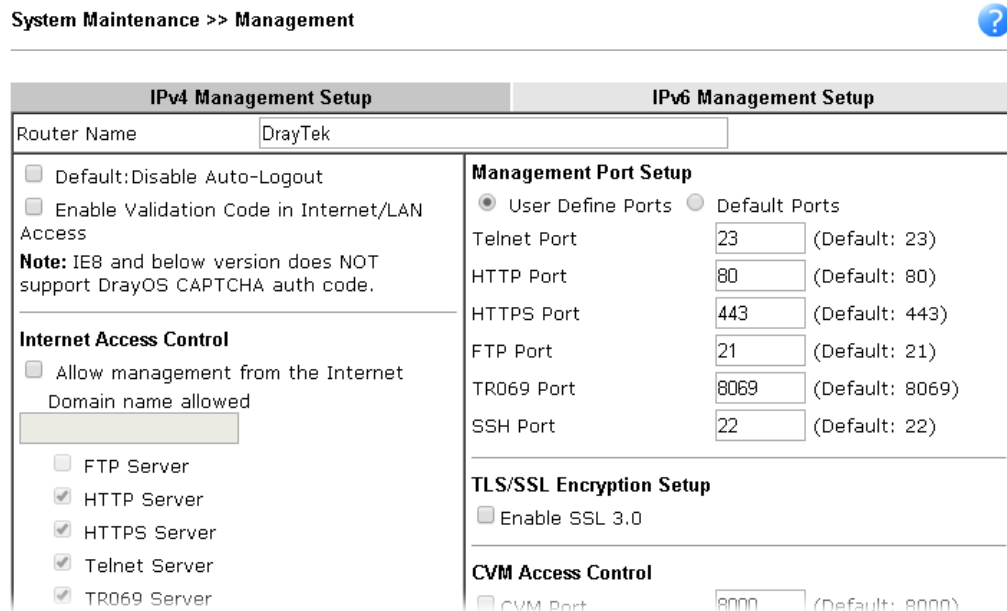
1. Here, we use Firefox and DNSSD to discover the service in such case. Therefore, just ensure the Bonjour client program and DNSSD for Firefox have been installed on the computer.



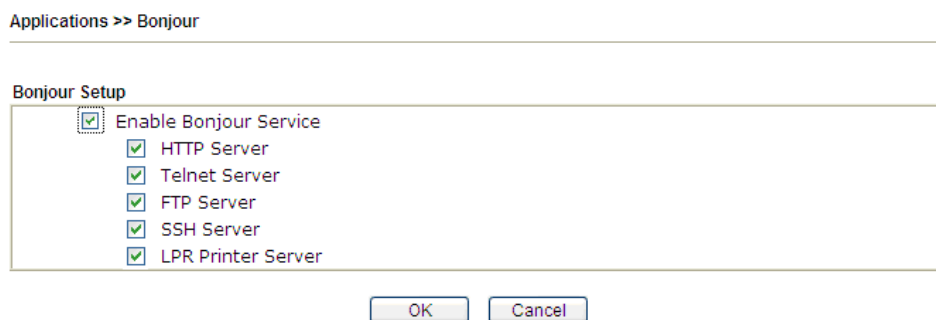
- Open the web browser, Firefox. If Bonjour and DNSSD have been installed, you can open the web page (DNSSD) and see the following results.



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



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



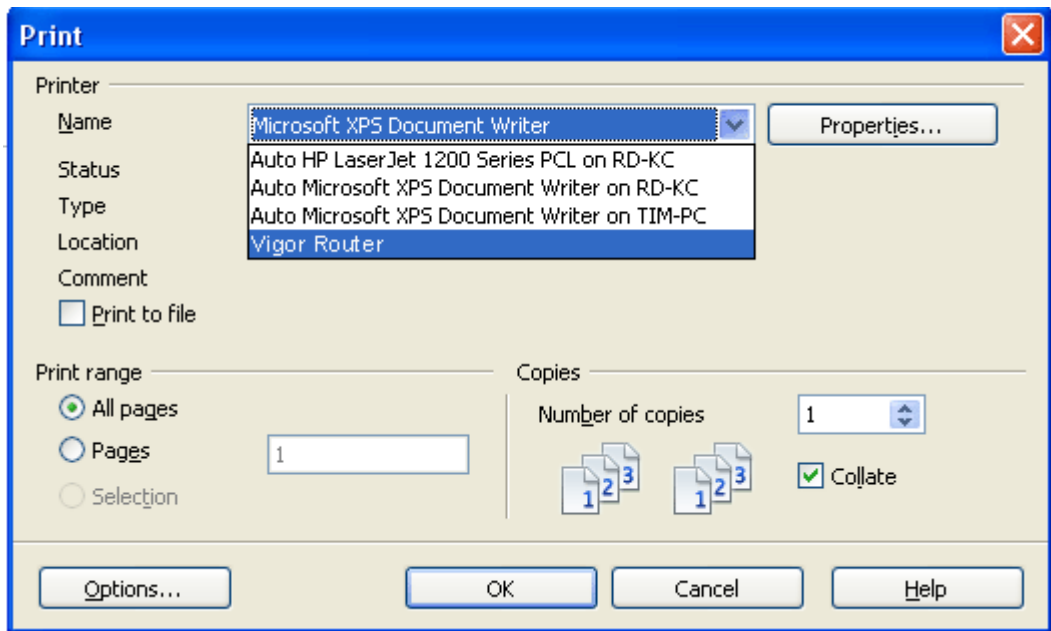
- Open the DNSSD page again. The available items will be changed as the follows. It means the Vigor router (based on Bonjour protocol) is ready to be used as a printer server, FTP server, SSH Server, Telnet Server, and HTTP Server.

DNSSD for Firefox

Browser Configuration Options Diagnostic Information

Interface	Name	Type	Domain	Service Info
2	DS1010Plus	_http_tcp	local.	Select a service on the left to view further details.
2	DS1010Plus(WebDAV)	_http_tcp	local.	
2	HP LaserJet 1300	_ipp_tcp	local.	
2	Vigor Router	_ftp_tcp	local.	
2	Vigor Router	_http_tcp	local.	
2	Vigor Router	_printer_tcp	local.	
2	Vigor Router	_ssh_tcp	local.	
2	Vigor Router	_telnet_tcp	local.	
2	tctseng-virtual-machine	_udisks-ssh_tcp	local.	
2	tctseng-virtual-machine [00:0c:29:78:bc:24]	_workstation_tcp	local.	
2	tomkao-desktop [00:0c:29:26:09:5d]	_workstation_tcp	local.	

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



II-5-12 High Availability

The High Availability (HA) feature refers to the awareness of component failure and the availability of backup resources. The complexity of HA is determined by the availability needs and the tolerance of system interruptions. Systems, provide nearly full-time availability, typically have redundant hardware and software that make the system available despite failures.

The high availability of the Vigor2862 Series is designed to avoid single points-of-failure. When failures occur, the failover process moves processing performed by the failed component (the "primary") to the backup component (the "secondary"). This process remains system-wide resources, recovers partial of failed transactions, and restores the system to normal within a few seconds.

To configure High Availability on, at least two DrayTek routers:

- Enable High Availability on the Primary and Secondary routers.
- Set a high Priority ID number on the Primary router and lower numbers for the Secondary router(s).
- Set the same Redundancy Method/Group ID/Authentication Key on the Primary and Secondary routers.
- Set the Management Interface to the same subnet for the Primary and Secondary routers.
- Enable Virtual IP on the Primary and Secondary routers for each subnet in use and set the same virtual IP on each router.

II-5-12-1 General Setup

Open Applications>>High Availability to get the following page.

Applications >> High Availability

Enable High Availability

Redundancy Method Active-Standby

General Setup	Config Sync	Status	Set to Factory Default
Group ID	<input type="text" value="1"/> (1-255)		
Priority ID	<input type="text" value="10"/> (1-30, 30 is highest priority)		
Authentication Key	<input type="text" value="draytek"/> (Max. 31 characters allowed)		
Protocol	IPv4		
Management Interface	LAN1		
Update DDNS	<input type="checkbox"/> Enable		
Syslog	<input type="checkbox"/> Enable		

IPv4	IPv6	Virtual IP
Index	Enable	Virtual IP
LAN1	<input type="checkbox"/>	<input type="text" value="192.168.1.2"/>
LAN2	<input type="checkbox"/>	<input type="text" value="192.168.2.2"/> !
LAN3	<input type="checkbox"/>	<input type="text" value="192.168.3.2"/> !
LAN4	<input type="checkbox"/>	<input type="text" value="192.168.4.2"/> !
LAN5	<input type="checkbox"/>	<input type="text" value="192.168.5.2"/> !
LAN6	<input type="checkbox"/>	<input type="text" value="192.168.6.2"/> !
LAN7	<input type="checkbox"/>	<input type="text" value="192.168.7.2"/> !
LAN8	<input type="checkbox"/>	<input type="text" value="192.168.8.2"/> !
DMZ	<input type="checkbox"/>	<input type="text" value="192.168.17.2"/> !

Available settings are explained as follows:

Item	Description
Enable High Availability	Check this box to enable HA function.
Redundancy Method	<p>Choose Hot-Standby or Active-Standby as the method for HA.</p> <p>Redundancy Method Active-Standby</p> <p>Hot-Standby</p> <p>Active-Standby</p> <p>Hot-Standby -</p> <p>Such method is suitable for a user which has one ISP account. With such method;</p> <ul style="list-style-type: none"> All WANs of secondary routers will be shut down by HA function. WAN settings of primary and secondary routers can be the same. <p>Note: When Hot-Standby is used, the wireless LAN function on secondary router will be "disabled" directly. Clients can not connect to the secondary</p>

	<p>router any more.</p> <p>Active-Standby - Such method is suitable for a user which has multiple ISP accounts. With such method;</p> <ul style="list-style-type: none"> ● All WANs of secondary routers can be up. Therefore, the user can route its traffic to secondary. ● WAN settings of primary and secondary routers must not be the same.
Group ID	<p>Type a value (1~255).</p> <p>In LAN environment, multiple routers can be divided into several groups. Each router must be specified with one group ID. Different routers with the same ID value will be categorized into the same group.</p> <p>Only one of the routers in the same group will be selected as the primary router.</p>
Priority ID	<p>Type a value (1~30).</p> <p>Different routers must be configured with different IDs.</p> <p>The router with the highest priority will be treated as primary router. If multiple routers have the same priority, the router with lower "IP" will be treated as primary. "IP" is the IP address configured on LAN >> General Setup page, in which LAN is determined by management interface.</p>
Authentication Key	<p>Type a string as the authentication key (maximum 31 characters allowed).</p> <p>It is used for encrypting the DARP to prevent malicious attack.</p>
Protocol	Choose IPv4 or IPv6.
Management Interface	<p>Such interface is used for DARP (DrayTek Address Redundancy Protocol) negotiation between routers. Only the interface which is enabled in LAN>>General Setup is available for selection.</p> <p>However, LAN1 is always enabled.</p>
Update DDNS	<p>Enable - Check the box to update the DDNS server for the secondary device if required.</p> <p>If the primary device fails, and the secondary device must take over the job of data transmitting and receiving. Then the system will update the DDNS server to make the user connect to the specified domain name.</p>
Syslog	Enable - Check the box to record required information on Syslog.
LAN1 ~ LAN8, DMZ	<p>Enable - Check the box to enable the interface.</p> <p>Virtual IP - Type the IP address of the router plays the role of Primary device.</p>

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

II-5-12-2 Config Sync

This page is used to specify the synchronization time for such Vigor router.

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

Enable Config Sync (Max. Sync to 10 routers)

Config Sync Interval:

Day ▾

Hour ▾

Minute ▾

Exclude the following settings from config sync:

WAN Settings

Note:

This feature requires that both routers are the same series, and the High Availability must be enabled for Config Sync to operate.

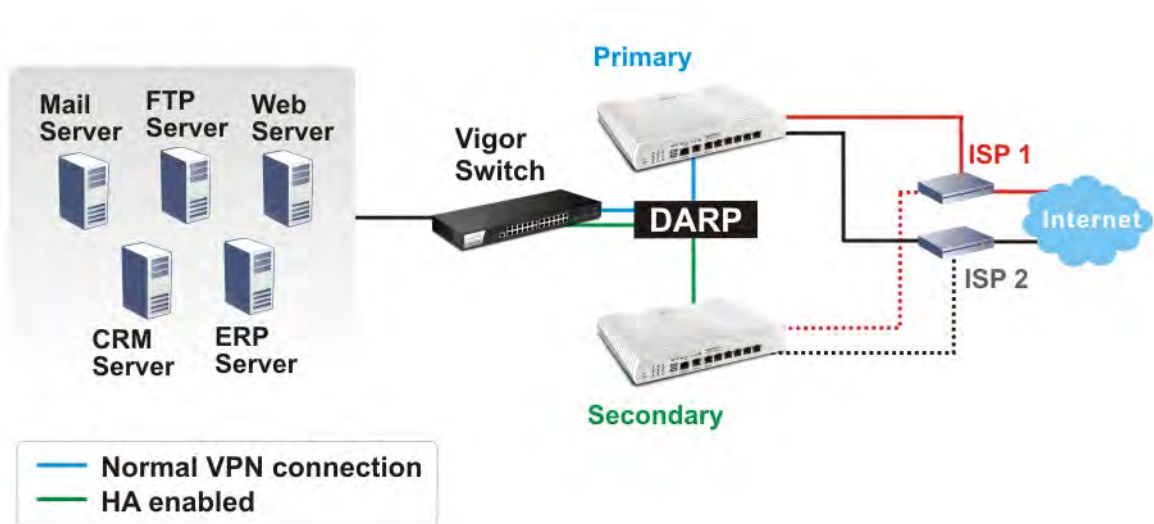
Available settings are explained as follows:

Item	Description
Enable Config Sync (Max. Sync to 10 routers)	Check this box to enable configuration synchronization. To sync configuration from primary to secondary router, both primary and secondary routers need to enable "config sync". Note that config sync can be enabled by Hot-Standby redundancy method only.
Config Sync Interval	Day / Hour / Minute - Primary router will sync its configuration to secondary router based on the time interval set here.
Exclude the following settings from config sync	Settings selected in this field will be excluded when executing configuration synchronization. For example, under active-standby mode, WAN settings will not be synchronized.

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

Example:

Take the following picture as an example. The upper Vigor2862 is regarded as primary device, the lower Vigor2862 is regarded as secondary device. When primary Vigor2862 Series is broken down, the secondary device could replace the primary role to take over all jobs as soon as possible. However, once the primary device is working again, the secondary device would be changed to original role to stand by.



II-5-13 Local 802.1X General Setup

Such page allows you to configure general settings for Local 802.1X server built in Vigor router.

Applications >> Local 802.1X General Setup

Local 802.1X General Setup

Enable

Phase 1 Method: PEAP
Phase 2 Method: MS-CHAPv2

User Profile

Select All Clear All

Available List	Authentication List

>> <<

Sync **User Profile** Setting to Internal Radius

Note:

1. Only the user profiles which is enabled in **User Management >> User Profile** will be listed here.
2. **Wireless LAN(2.4G)**, **Wireless LAN(5G)** and **Wired 802.1X** used the same **User Profile** as its identify and password.

OK Clear Cancel

Available settings are explained as follows:

Item	Description		
Enable	Click it to enable local 802.1X server. At present, such feature can be used for wireless and wired 802.1x authentication.		
User Profile	Select All - Click it to select all of the profiles under Available List. Clear All - Click it to remove all of the profiles under Authentication List.		
Sync User Profile	Make the enabling/disabling setting for both Internal RADIUS and Local 802.1X synchronize for all of the user profiles (User Management>>User Profile). For example, if Local 802.1x is configured as Enabled (checked), the Internal RADIUS will be configured as Enabled too. <div style="border: 1px solid black; padding: 5px;"> <p>3. Internal Services</p> <table border="1" style="width: 100%;"> <tr> <td><input checked="" type="checkbox"/> Internal RADIUS</td> <td><input checked="" type="checkbox"/> Local 802.1X</td> </tr> </table> <p>Note: Internal Services means the account and password of this user profile can be used by other application.</p> <p style="text-align: center;">OK Refresh Clear Cancel</p> </div> If Local 802.1X is configured as Disabled (unchecked), the Internal RADIUS will be changed as Disabled too, even if it is enabled previously.	<input checked="" type="checkbox"/> Internal RADIUS	<input checked="" type="checkbox"/> Local 802.1X
<input checked="" type="checkbox"/> Internal RADIUS	<input checked="" type="checkbox"/> Local 802.1X		

	<p>3. Internal Services</p> <p><input type="checkbox"/> Internal RADIUS <input type="checkbox"/> Local 802.1X</p> <p>Note: Internal Services means the account and password of this user profile can be used by other application.</p> <p>OK Refresh Clear Cancel</p>
OK	Click it to save the settings.
Clear	Click it to remove previous setting configuration.
Cancel	Click it to give up all settings configuration.

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

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.

Applications >> Active Directory /LDAP

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

General Setup | Active Directory / LDAP Profiles

Enable

Bind Type: Regular Mode

Server IP Address: 172.16.2.8

Destination Port: 389

Regular DN: uid=vpntest,ou=vpnuser,dc=ms,dc=draytel

Regular Password: 1234

OK Cancel

There are three types of bind type supported:

- **Simple Mode** - Just simply do the bind authentication without any search action.
- **Anonymous** - Perform a search action first with Anonymous account then do the bind authentication.
- **Regular Mode**- Mostly it is the same with anonymous mode. The different is that, the server will firstly check if you have the search authority.
For the regular mode, you'll need to type in the **Regular DN** and **Regular Password**.

3. Create LDAP server profiles. Click the **Active Directory /LDAP** tab to open the profile web page and click any one of the index number link.

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

Applications >> Active Directory /LDAP>> Server Profiles

Index No. 1

Name	rd1
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

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

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

General Setup

Mode Selection:

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

Notice for User-Based mode:

- In User-Based mode, **Active Rules** in Firewall will be applied to all LAN clients, packets that matches the Active Rules will be blocked or pass immediately, no user authentication is required.
- Only **Inactive Rules** in Firewall can be set for individual user profile. In User-Based mode, packets that do not match Active Rules will need authentication, and the Inactive Rule applied to the specific user profile will then take effect.

Authentication page:

Web Authentication: HTTPS HTTP

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

VPN and Remote Access >> PPP General Setup

PPP General Setup

<p>PPP/MP Protocol</p> <p>Dial-In PPP Authentication: PAP/CHAP/MS-CHAP/MS-CHAPv2</p> <p>Dial-In PPP Encryption(MPPE): Optional MPPE</p> <p>Mutual Authentication (PAP): <input type="radio"/> Yes <input checked="" type="radio"/> No</p> <p>Username: <input type="text"/></p> <p>Password: <input type="text"/></p> <p>IP Address Assignment for Dial-In Users (When DHCP Disable set)</p> <table><tr><td>Assigned IP start LAN 1</td><td><input type="text" value="192.168.1.200"/></td></tr><tr><td>LAN 2</td><td><input type="text" value="192.168.2.250"/></td></tr><tr><td>LAN 3</td><td><input type="text" value="192.168.3.200"/></td></tr><tr><td>LAN 4</td><td><input type="text" value="192.168.4.200"/></td></tr><tr><td>LAN 5</td><td><input type="text" value="192.168.5.200"/></td></tr><tr><td>LAN 6</td><td><input type="text" value="192.168.6.200"/></td></tr></table>	Assigned IP start LAN 1	<input type="text" value="192.168.1.200"/>	LAN 2	<input type="text" value="192.168.2.250"/>	LAN 3	<input type="text" value="192.168.3.200"/>	LAN 4	<input type="text" value="192.168.4.200"/>	LAN 5	<input type="text" value="192.168.5.200"/>	LAN 6	<input type="text" value="192.168.6.200"/>	<p>PPP Authentication Methods</p> <p><input checked="" type="checkbox"/> Remote Dial-in User</p> <p><input checked="" type="checkbox"/> RADIUS</p> <p><input checked="" type="checkbox"/> AD/LDAP</p> <p>PPTP LDAP Profile</p> <p><input checked="" type="checkbox"/> TACACS+</p> <table><tr><td><input checked="" type="checkbox"/></td><td>rd1</td></tr><tr><td><input checked="" type="checkbox"/></td><td>shrd</td></tr></table> <p>Note: Please select 'PAP Only 'Dial-In PPP Authentication',if you want to use AD/LDAP or TACACS+ for PPP Authentication.</p> <p>Note: Default priority is Remote Dial-in User -> RADIUS -> AD/LDAP -> TACACS+.</p> <p>While using Radius or LDAP Authentication:</p> <p>Assign IP from subnet: <input type="text" value="LAN1"/></p>	<input checked="" type="checkbox"/>	rd1	<input checked="" type="checkbox"/>	shrd
Assigned IP start LAN 1	<input type="text" value="192.168.1.200"/>																
LAN 2	<input type="text" value="192.168.2.250"/>																
LAN 3	<input type="text" value="192.168.3.200"/>																
LAN 4	<input type="text" value="192.168.4.200"/>																
LAN 5	<input type="text" value="192.168.5.200"/>																
LAN 6	<input type="text" value="192.168.6.200"/>																
<input checked="" type="checkbox"/>	rd1																
<input checked="" type="checkbox"/>	shrd																

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

Online Status					
Physical Connection			System Uptime: 0day 2:25:59		
IPv4		IPv6			
LAN Status	Primary DNS: 168.95.192.1		Secondary DNS: 168.95.1.1		
IP Address	TX Packets	RX Packets			
10.1.7.1	2069	1036			
WAN 1 Status >> Drop PPPoE					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet	iwiz	PPPoE	2:25:53	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
1.169.185.242	168.95.98.254	14851	9506	11281	912

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.



```
← → ↻ www.changeip.com/dynamic/dns/update.asp?u=jo...&p=jo...&host...
免費的 Hotmail 建議的網站 Home Page 網頁快訊圖庫 從 IE 匯入 Go

200 Successful Update (Address Used: 1.169.185.242)

Updated target: j...changeip.org
Updated 1 host records
Updated 0 zone serial numbers
Reviewed 1 possible records
Total updates: 75
Lockout counter: 1 out of 60
Lockout reset: 60 mins
Elapsed time: 0.01 seconds
NIC version: 2.68

For XML output add &xml=1
Use SSL for better security.
```

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

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

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

Index : 1

Enable Dynamic DNS Account

WAN Interface:

Service Provider:

Provider Host:

Service API:

Auth Type:

Connection Type:

Server Response:

Login Name: (max. 64 characters)

Password: (max. 23 characters)

Wildcards

Backup MX

Mail Extender:

Determine Real WAN 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.

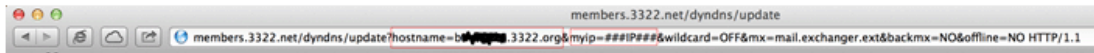
Part B : 3322.net

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

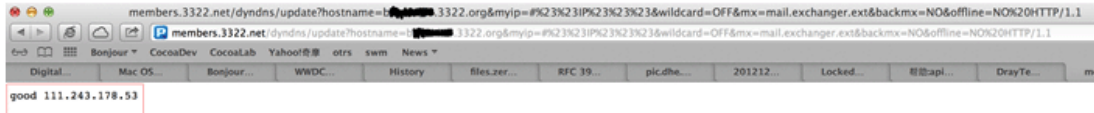
Username: bi*****
 Password: 88*****
 Host name: bi*****.3322.org

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:



And the result will be :



“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.

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

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

Index : 1

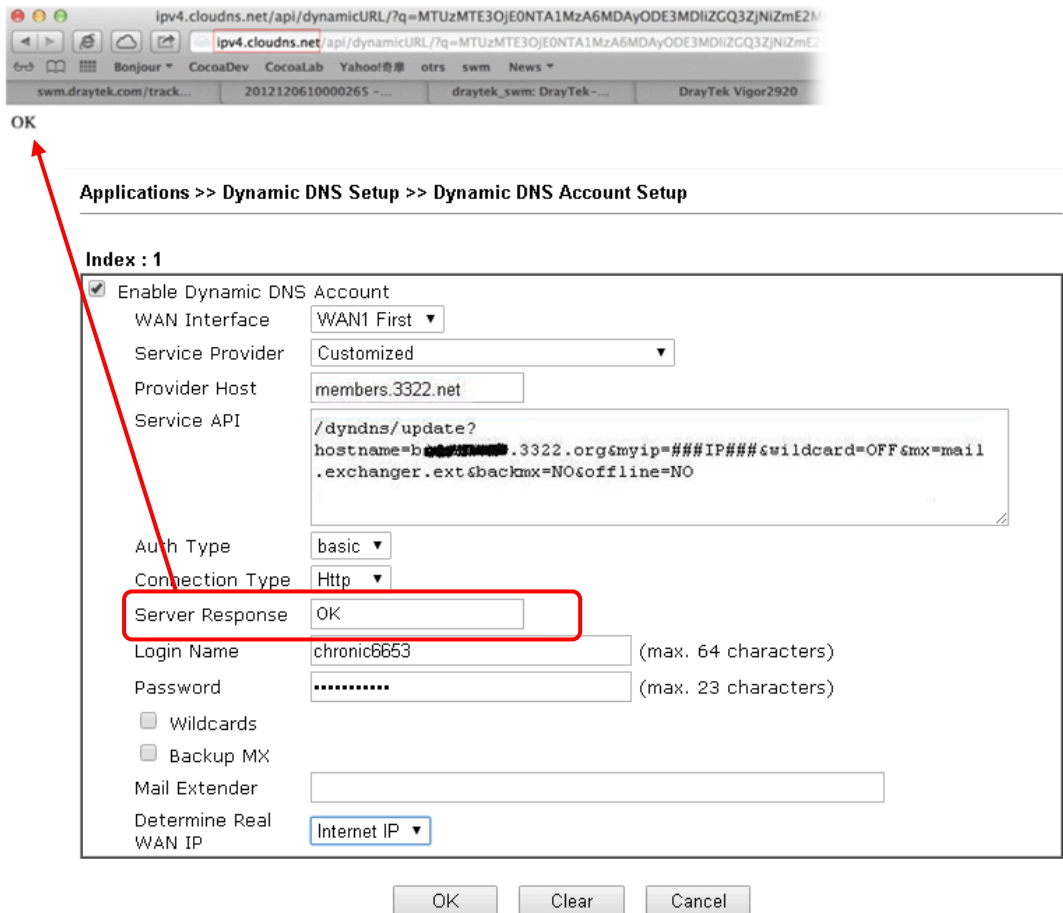
<input checked="" type="checkbox"/> Enable Dynamic DNS Account	
WAN Interface	WAN1 First
Service Provider	Customized
Provider Host	members.3322.net
Service API	<code>/dyndns/update? hostname=yourhost.3322.org&myip=###IP###&wildcard=OFF&mx=mail .exchanger.ext&backmx=NO&offline=NO</code>
Auth Type	basic
Connection Type	Http
Server Response	
Login Name	chronic6653 (max. 64 characters)
Password (max. 23 characters)
<input type="checkbox"/> Wildcards	
<input type="checkbox"/> Backup MX	
Mail Extender	
Determine Real WAN IP	Internet IP

OK Clear Cancel

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.



The screenshot shows a web browser window with the URL `ipv4.cloudns.net/api/dynamicURL/?q=MTUzMTE3OjE0NTA1MzA6MDAyODE3MDIiZGQ3ZjNiZmE2M...`. Below the browser, there is a dialog box titled "Applications >> Dynamic DNS Setup >> Dynamic DNS Account Setup". The dialog box contains the following fields and options:

- Enable Dynamic DNS Account
- WAN Interface: WAN1 First
- Service Provider: Customized
- Provider Host: members.3322.net
- Service API: `/dyndns/update?hostname=#####.3322.org&myip=###IP###&wildcard=OFF&mx=mail.exchanger.ext&backmx=NO&offline=NO`
- Auth Type: basic
- Connection Type: Http
- Server Response: OK (highlighted with a red box)
- Login Name: chronic6653 (max. 64 characters)
- Password: (max. 23 characters)
- Wildcards
- Backup MX
- Mail Extender: [Empty field]
- Determine Real WAN IP: Internet IP

At the bottom of the dialog box, there are three buttons: OK, Clear, and Cancel. A red arrow points from the "OK" button in the browser window to the "Server Response" field in the dialog box.

II-6 Routing

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

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

Load Balance

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

Specify Interface

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

Address Mapping

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

Priority

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

Failover to/Failback

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

Other routing

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



Info

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

Web User Interface

II-6-1 Static Route

Go to **Routing** >> **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

Routing >> Static Route Setup

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

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

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

Available settings are explained as follows:

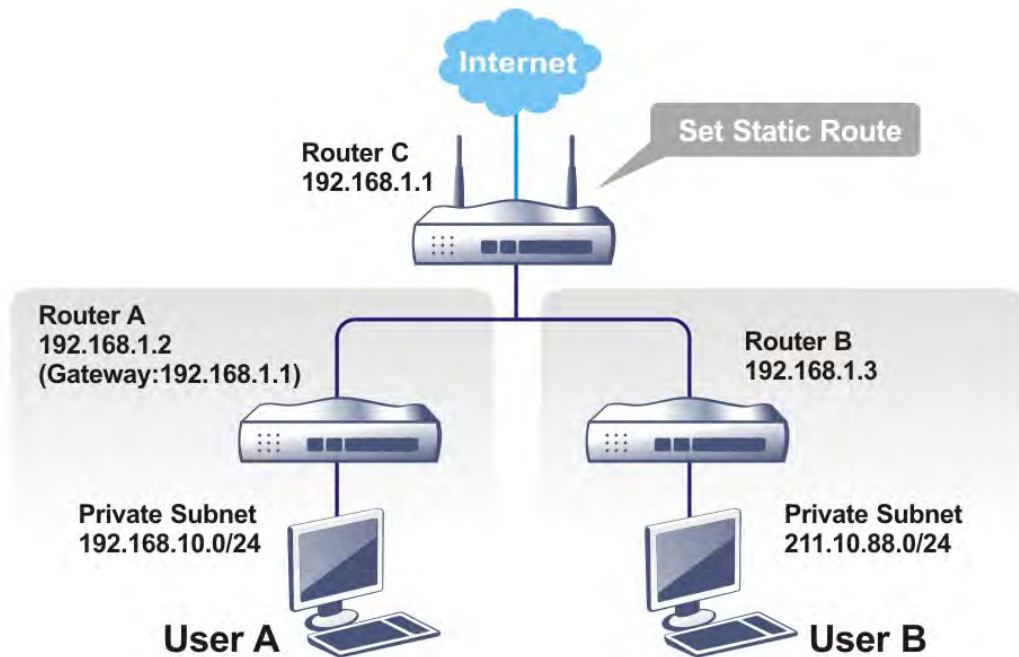
Item	Description						
Index	The number (1 to 30) under Index allows you to open next page to set up static route.						
Destination Address	Displays the destination address of the static route.						
Status	Displays the status of the static route.						
Set to Factory Default	Clear all of the settings and return to factory default settings.						
Viewing Routing Table	Displays the routing table for your reference. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Diagnostics >> View Routing Table</p> <table border="1" style="width: 100%;"> <thead> <tr> <th>Current Running Routing Table</th> <th>IPv6 Routing Table</th> <th>Refresh</th> </tr> </thead> <tbody> <tr> <td colspan="3"> Key: C - connected, S - static, R - RIP, * - default, ~ - private C~ 192.168.1.0/ 255.255.255.0 directly connected LAN1 </td> </tr> </tbody> </table> </div>	Current Running Routing Table	IPv6 Routing Table	Refresh	Key: C - connected, S - static, R - RIP, * - default, ~ - private C~ 192.168.1.0/ 255.255.255.0 directly connected LAN1		
Current Running Routing Table	IPv6 Routing Table	Refresh					
Key: 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.



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



Info

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

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

LAN >> Static Route Setup

Index No. 1

<input type="checkbox"/> Enable	Destination IP Address	???
	Subnet Mask	
	Gateway IP Address	
	Network Interface	LAN1

Note:

WAN5, WAN6, WAN7 are PVCs or VLANs that can be configured on the **Multi-PVC/LAN** page.

OK Cancel Delete

Available settings are explained as follows:

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

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

LAN >> Static Route Setup

Index No. 1

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

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

Diagnostics >> View Routing Table

Current Running Routing Table	IPv6 Routing Table	Refresh
Key: C - connected, S - static, R - RIP, * - default, ~ - private		
S~ 192.168.10.0/ 255.255.255.0	via 192.168.1.2	LAN1
C~ 192.168.1.0/ 255.255.255.0	directly connected	LAN1
S~ 211.100.88.0/ 255.255.255.0	via 192.168.1.3	LAN1

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

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

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

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

Index No. 1

Enable

Destination IPv6 Address / Prefix Len: /

Gateway IPv6 Address:

Network Interface:

Available settings are explained as follows:

Item	Description
Enable	Click it to enable this profile.
Destination IPv6 Address / Prefix Len	Type the IP address with the prefix length for this entry.
Gateway IPv6 Address	Type the gateway address for this entry.

Network Interface	Use the drop down list to specify an interface for this static route.
--------------------------	---

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

II-6-2 Load-Balance /Route Policy

It allows network administrator to manage the outbound traffic more specifically. The policy set in Load-Balance/Route Policy always has higher priority than **Default Route** and **Auto Load Balance** set in WAN >> **Internet Access**, and always has lower priority than the **Firewall Rules**. Administrator may also define a priority to this policy.

This page lists all the policies and shows whether the policy is enabled/disabled, what are the criteria to match, and through which the interface should the traffic to go if the criteria are matched, and also its priority.

Load-Balance/Route Policy



Load-Balance/Route Policy

10 rules per page

[Set to Factory Default](#)

Index	Enable	Comment	Protocol	Interface	Priority	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End	Move Up	Move Down
1	<input type="checkbox"/>		Any	WAN1	200	Any	Any	Any	Any	Any	Any		Down
2	<input type="checkbox"/>		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
3	<input type="checkbox"/>		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
4	<input type="checkbox"/>		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
5	<input type="checkbox"/>		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
6	<input type="checkbox"/>		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
7	<input type="checkbox"/>		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
8	<input type="checkbox"/>		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
9	<input type="checkbox"/>		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
10	<input type="checkbox"/>		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down

<< 1-10 | 11-20 | 21-30 | 31-40 | 41-50 >>

[Next >>](#)

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

OK

Available settings are explained as follows:

Item	Description
Index	Click the number of index to access into the configuration web page.
Enable	Check this box to enable this policy.
Protocol	Display the protocol used for this policy.
Interface	Display the interface to send packets to once the policy is matched.
Priority	Display the priority value for such route policy profile.
Src IP Start	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 (simple and basic) 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

Index: 1 Criteria

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

Source IP

Any

Src IP Start Src IP End

~

Destination IP

Any

Dest IP Start Dest IP End

~

Country Object

 None

 None

 1-Pacific

Available settings are explained as follows:

Item	Description
Source IP	<p>Any - Any IP can be treated as the source IP.</p> <p>Src IP Start - Type the source IP start for the specified WAN interface.</p> <p>Src IP End - Type the source IP end for the specified WAN interface. If this field is blank, it means that all the source IPs inside the LAN will be passed through the WAN interface.</p>
Destination IP	<p>Any - Any IP can be treated as the destination IP.</p> <p>Dest IP Start- Type the destination IP start for the specified WAN interface.</p> <p>Dest IP End - Type the destination IP end for the specified WAN interface. If this field is blank, it means that all the destination IPs will be passed through the WAN interface.</p> <p>Country Object - Specify a country object. All the IPs coming from the country (countries) specified in the object will be passed through the WAN interface.</p>

3. Click Next to get the following page.

Load-Balance/Route Policy

Index: 1 Interface

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

Interface

WAN1

LAN1

LAN2

LAN3

LAN4

LAN5

Available settings are explained as follows:

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

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

Load-Balance/Route Policy

Index: 1 NAT or Routing

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

The current setting is:

Force NAT

Force Routing

Available settings are explained as follows:

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

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

Load-Balance/Route Policy

Index: 1 Configuration Summary

Criteria

Source IP Any

Destination IP ~

Interface

WAN1

More options

Force NAT

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

Index: 1

Enable

Comment

Criteria

Protocol

Source

Network: Mask:

Destination

-

Destination Port

Start: End:

Send via if Criteria Matched

Interface WAN/LAN

VPN

Gateway Default Gateway

Specific Gateway

Packet Forwarding to WAN via Force NAT

Force Routing

Failover to WAN/LAN

VPN

Route Policy

Gateway Default Gateway

Specific Gateway

Priority

Note:

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

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable this policy.
Comment	Type a brief explanation for such profile.
Protocol	Use the drop-down menu to choose a proper protocol for the WAN interface.
Source	<p>Any - Any IP can be treated as the source IP.</p> <p>IP Range - Define a range of IP address as source IP addresses.</p> <p>● Start - Type an address as the starting IP for such</p>

	<p>profile.</p> <ul style="list-style-type: none"> ● End - Type an address as the ending IP for such profile. <p>IP Subnet - Define a subnet containing IP address and mask address.</p> <ul style="list-style-type: none"> ● Network - Type an IP address here. ● Mask - Use the drop down list to choose a suitable mask for the network. <p>IP Object / IP Group- Use the drop down list to choose a preconfigured IP object/group.</p>
Destination	<p>Any - Any IP can be treated as the destination IP.</p> <p>IP Range - Define a range of IP address as destination IP addresses.</p> <ul style="list-style-type: none"> ● Start - Type an address as the starting IP for such profile. ● End - Type an address as the ending IP for such profile. <p>IP Subnet - Define a subnet containing IP address and mask address.</p> <ul style="list-style-type: none"> ● Network - Type an IP address here. ● Mask - Use the drop down list to choose a suitable mask for the network. <p>Domain Name - Specify a domain name as the destination.</p> <ul style="list-style-type: none"> ● Select - Click it to choose an existing domain name defined in Objects Setting>>String Object. ● Delete - Remove current used domain name. ● Add - Create a new domain name as the destination. <p>IP Object / IP Group- Use the drop down list to choose a preconfigured IP object/group.</p> <p>Country Object - Use the drop down list to choose a preconfigured object. Then all IPs within that country will be treated as the destination IP.</p>
Destination Port	<p>Any - Any port number can be treated as the destination port.</p> <p>Dest Port Range -</p> <ul style="list-style-type: none"> ● Start - Type the destination port start for the destination IP. ● 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	<p>Interface - Use the drop down list to choose a WAN or LAN interface or VPN profile. Packets match with the above criteria will be transferred to the interface chosen here.</p> <p>Gateway IP - Specific gateway is used only when you want to forward the packets to the desired gateway. Usually, Default Gateway is selected in default.</p> <p>Packet Forwarding to WAN via - When you choose WAN (e.g., WAN1) as the Interface for packet transmission, you have to specify the way the packet forwarded to. Choose Force NAT or Force Routing.</p> <p>Fallover 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</p>

	<p>via if criteria matched) is down.</p> <ul style="list-style-type: none"> ● WAN/LAN - Use the drop down list to choose an interface as an auto failover interface. ● VPN - Use the drop down list to choose a VPN tunnel as a failover tunnel. ● Route Policy - Use the drop down list to choose an existed route policy profile. ● Gateway IP - Specific gateway is used only when you want to forward the packets to the desired gateway. Usually, Default Gateway is selected in default.
<p>Priority</p>	<p>Packets will be transmitted based on all routes or Route Policy. Vigor router will determine which rule will be adopted for transmitting the packet according to the priority of Static Route and Route Policy.</p> <p>The greater the value is, the lower the priority is. Default value for route policy is "200" which means it has higher priority than the default route.</p> <p>Failback- When Failover to option is enabled, Administrator could also enable Failback to clear the existing session on Failover interface and return to the original interface immediately once the original interface resume its service. When Failback is not enabled, the router will only stop sending packets via the Failover interface when the existing sessions are cleared, and this might take a long time because some application will keep sending packet once a while. Therefore, Failback option is recommended if Administrator wants the traffic to go via the primary interface as soon as possible.</p>

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

Diagnose for Route Policy

The button of **Diagnose** located below the Load-Balance /Route Policy profile is used to trace possible path of the packets sent out of the router.

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.

Click **Diagnose** to get the following page.

Diagnostics >> Route Policy Diagnosis ?

Test how the packets will be routed

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

Packet Information

Protocol

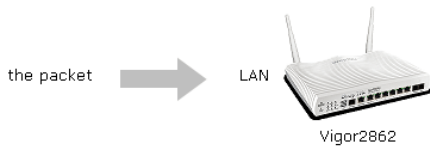
Src IP

Dst IP

Dst Port

Analyze

Analysis



The packet was dropped because the send-to interface of the matched policy "[policy 1](#)" was inactive and there was no failover setting

Matched Route

Matched	Priority
N/A	N/A

Matched Policy

Matched	Priority	failovered
Route Policy 1	200	No

or

Load-Balance/Route Policy >> Diagnose

Test how the packets will be routed

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

Input File

未選擇任何檔案

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

Analyze

Available settings are explained as follows:

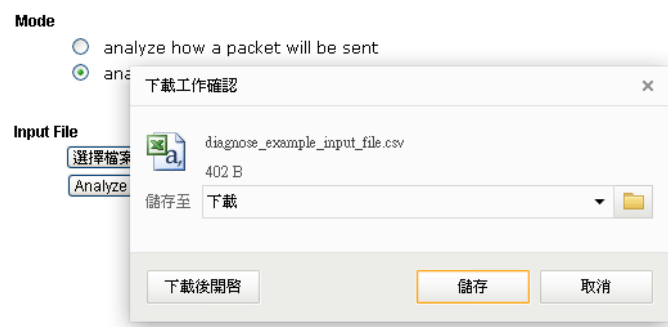
Item	Description
Mode	Analyze a single packet - Choose such mode to make Vigor router analyze how a single packet will be sent by a route policy. Analyze multiple packets... - Choose such mode to make Vigor router analyze how multiple packets in a specified file will be sent by a route policy.
Packet Information	Specify the nature of the packets to be analyzed by Vigor router. ICMP/UDP/TCP/ANY- Specify a protocol for diagnosis. Src IP - Type an IP address as the source IP. Dst IP - Type an IP address as the destination IP.

Dst Port - Use the drop down list to specify the destination port.

Analyze - Click it to perform the job of analyzing. The analyzed result will be shown on the page. If required, click **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" file for saving the result of analysis.



Analyze - Click it to perform the job of analyzing. The analyzed result will be shown on the page. If required, click **export analysis** to export the result as a file.

Load-Balance/Route Policy >> Diagnose

Mode

analyze how a packet will be sent

analyze how multiple packets as specified in the input file will be sent

Input File

(download an example input file)

Analysis

Profile	Input Packet Information			Matched Route		Matched Policy			Final Result	
	Proto	Src IP	Dst IP	Route	Priority	Policy	Priority	Label/Remark	Interface	Reason
LA-branch	ICMP	192.168.1.10	10.10.10.10	N/A	No Match	N/A	No Match	N/A	N/A	The packet was dropped because neither "route" or "policy" was matched.
RV-branch	TCP	192.168.1.20	20.20.20.20	5060	No Match	N/A	No Match	N/A	N/A	The packet was dropped because neither "route" or "policy" was matched.
										The packet was dropped because...

Note that the analysis was based on the current "load-balance/route policy" settings, we do not guarantee it will be 100% the same as the real case.

II-6-3 BGP

Border Gateway Protocol (BGP) is a standardized protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet.

II-6-3-1 Basic Settings

Set general settings for for local router and neighboring routers.

Routing >> BGP

Basic Settings		Static Network		Refresh View Routing Table	
Local					
<input type="checkbox"/> Enable BGP					
Local AS Number	<input type="text" value=""/>	(1~4294967295)			
Hold Time	<input type="text" value="180"/>	(10~65535 Sec)			
Connect Retry Time	<input type="text" value="120"/>	(3~255 Sec)			
Router ID	<input type="text" value="192.168.1.1"/>	(e.g. 1.2.3.4)			
Neighbor					
Enable	Index	AS Number	Profile Name	IP Address	Status
<input type="checkbox"/>	1				None
<input type="checkbox"/>	2				None
<input type="checkbox"/>	3				None
<input type="checkbox"/>	4				None
<input type="checkbox"/>	5				None
<input type="checkbox"/>	6				None
<input type="checkbox"/>	7				None
<input type="checkbox"/>	8				None

OK

Available settings are explained as follows:

Item	Description
Local	
Enable BGP	Check the box to enable basic BGP function for local router.
Local AS Number	Set the AS number for local router.
Hold Time	Set the time interval (in seconds) to determine the peer is dead when the router is unable to receive any keepalive message from the peer within the time.
Connect Retry Time	If the router fails to connect to neighboring router, it requires a period of time to reconnect. Set the time interval to do reconnection.
Router ID	Specify the LAN subnet for the router.
Neighbor	
Enable	Check the box to enable the basic BGP function for neighboring router.
Index	Click the index number link to configure neighbor profile.

AS Number	Display the AS Number for neighboring router.
Profile Name	Display the name of the neighboring profile.
IP Address	Display the IP address specified for the neighboring profile.
Status	Display the connection status for local router and neighboring router.

II-6-3-1 Static Network

This page allows you to configure up to eight neighboring routers for exchanging the routing information with the local router.

Routing >> BGP

Basic Settings		Static Network		View Routing Table
Select	Index	IP Address	Subnet Mask	
<input type="checkbox"/>	1	<input type="text"/>	<input type="text"/>	
<input type="checkbox"/>	2	<input type="text"/>	<input type="text"/>	
<input type="checkbox"/>	3	<input type="text"/>	<input type="text"/>	
<input type="checkbox"/>	4	<input type="text"/>	<input type="text"/>	
<input type="checkbox"/>	5	<input type="text"/>	<input type="text"/>	
<input type="checkbox"/>	6	<input type="text"/>	<input type="text"/>	
<input type="checkbox"/>	7	<input type="text"/>	<input type="text"/>	
<input type="checkbox"/>	8	<input type="text"/>	<input type="text"/>	

Available settings are explained as follows:

Item	Description
Select	Check the box to enable the configuration for the selected index entry.
IP Address	Type the IP address for a router.
Subnet Mask	Type the mask value for the IP address.

Application Notes

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

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

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

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

192.168.1.1/doc/wipalias.htm

WAN1 IP Alias (Multi-NAT)

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

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

- Check **Enable**.
- Enter the WAN IP address.
- Click **OK** to save.

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

- Go to **Load Balance/Route policy**. Create a Route Policy for specific IP address to send from specific WAN IP Address.

Load-Balance/Route Policy

Index: 1

Enable

Comment

Criteria

Protocol

Source Start: End:

Destination

Destination Port

Send via if Criteria Matched

Interface WAN/LAN

VPN

Gateway Default Gateway Specific Gateway

Packet Forwarding to WAN via Force NAT Force Routing

Failover to WAN/LAN VPN Route Policy

Gateway Default Gateway Specific Gateway

Priority

Failback

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

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

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

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

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

Criteria

Protocol: Any

Source: IP Range

Start: 192.168.1.20 End: 192.168.1.30

Destination: Domain Name

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

Add

Destination Port: Any

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

192.168.1.1/loc/strobjslt.htm

Objects Setting >> String Object

Index	String
1	Floor_1
32	Floor_2
33	sdapot
34	portal.draytek.com
65	Floor_3
66	Draytek Hotspot
67	portal.draytek.com
102	Floor_1

OK Cancel

Index: 1

Enable

Comment: Floor_1

Criteria

Protocol: Any

Source: IP Range

Start: 192.168.1.20 End: 192.168.1.30

Destination: Domain Name

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

Add

Destination Port: Any

Send via if Criteria Matched

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

Start: 192.168.1.20 End: 192.168.1.30

Destination: Domain Name

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

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

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

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

Add (up to 5)

Destination Port: Any

Send via if Criteria Matched

Auto-create String Objects

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

Start: 192.168.1.20 End: 192.168.1.30

Destination: Domain Name

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

Add(up to 5)

Destination Port: Any

Send via if Criteria Matched

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

Objects Setting >> String Object

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

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

[Add](#)

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

Part III Wireless LAN



Wireless

Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access.

III-1 Wireless LAN (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 Vigor2862 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.

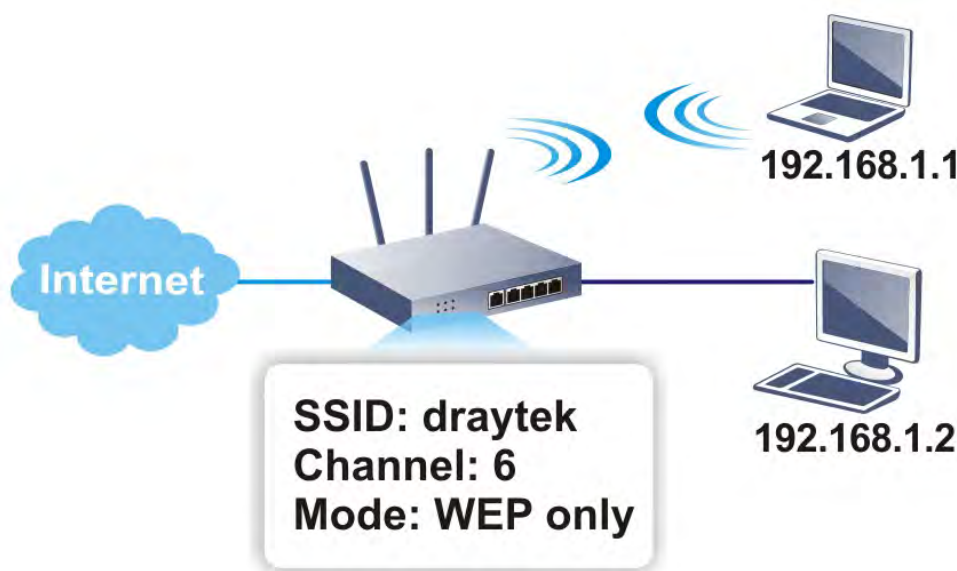
Vigor2862 wireless router is a highly integrated wireless local area network (WLAN) for 5 GHz 802.11ac or 2.4/5 GHz 802.11n WLAN applications. It supports channel operations of 20/40 MHz at 2.4 GHz and 20/40/80 MHz at 5 GHz. Vigor2862 “ac” series router can support data rates up to 1.3 Gbps in 802.11ac 80 MHz channels. Vigor2862 “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.

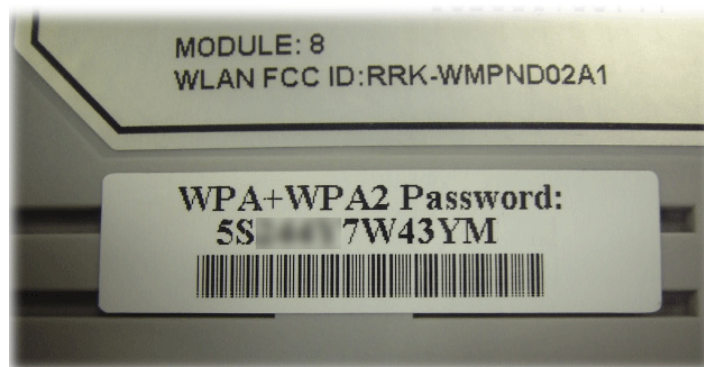
In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

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.



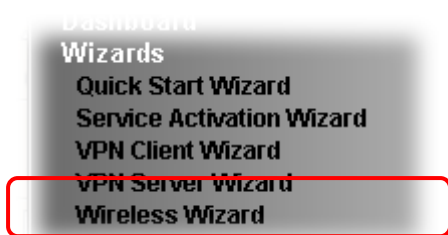
Web User Interface

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 Vigor2862 series. In this case, Vigor2862ac is used as an example.

Wireless Wizard

Host AP Configuration

Wireless 2.4GHz Settings

Name:

Mode:

Channel:

Security Key:

Wireless 5GHz Settings

Use the same SSID and Security Key as above

Name:

Mode:

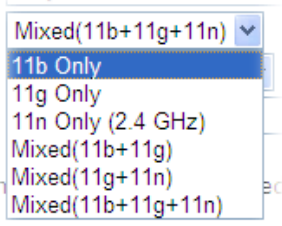
Channel:

Security Key:

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

Available settings are explained as follows:

Item	Description
Wireless 2.4GHz Settings	
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 11b Only, 11g Only,

	<p>11n Only (2.4GHz), Mixed (11b+11g), Mixed (11g+11n), and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mix (11b+11g+11n) mode.</p> 
Channel	Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.
Security Key	<p>The wireless mode offered by this wizard is WPA2/PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p> <p>Either 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").</p>
Use the same SSID and Security Key as above	Check the box to use the same settings configured 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	<p>The wireless mode offered by this wizard is WPA2/PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.</p> <p>Either 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").</p>
Next	Click it to get into the next setting page.
Cancel	Exit the wireless wizard without saving any changes.

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

Wireless Wizard

Guest AP Configuration

Wireless 2.4GHz Settings

Enable Disable

SSID:

Security Key:

Bandwidth Limit: Enable Total Upload kbps Total Download kbps

Wireless 5GHz Settings

Enable Disable

Use the same SSID and Security Key as above

SSID:

Security Key:

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

Available settings are explained as follows:

Item	Description
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...").
Bandwidth Limit	Enable - Check the box to set the bandwidth limit for data transmission in upload and download. It controls the data transmission rate through wireless connection. Total Upload - Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps. Total Download - Type the transmitting rate for data download. Default value is 30,000 kbps.
Wireless 5GHz Settings	
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...").
Next	Click it to get into the next setting page.
Cancel	Exit the wireless wizard without saving any changes.

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

Wireless Wizard

Configuration Summary

Wireless 2.4GHz Settings	Wireless 5GHz Settings
Mode: Mixed(11b+11g+11n) Channel: Channel 6, 2437MHz	Mode: Mixed (11a+11n+11ac) Channel: Channel 36, 5180MHz
Host AP SSID Name: 2862-marketing Security Key: *****	Host AP SSID Name: DrayTek2862_5Gmarketing Security Key: *****
Guest AP Status: Enabled SSID Name: DrayTek_Guest Security Key: ***** Bandwidth Limit: Disabled	Guest AP Status: Enabled SSID Name: DrayTek_5G_Guest Security Key: *****

- 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.

Wireless LAN(2.4GHz) >> General Setup

General Setting (IEEE 802.11)

Enable Wireless LAN

Mode :

Channel:

	Enable	Active	Hide	SSID	SSID	Isolate Member	Isolate VPN
1	<input checked="" type="checkbox"/>	V	<input type="checkbox"/>	<input type="text" value="DrayTek"/>	<input type="text" value="DrayTek"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	X	<input type="checkbox"/>	<input type="text" value="DrayTek_Guest"/>	<input type="text" value="DrayTek_Guest"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	X	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	X	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

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

When **High Availability** is set as Hot-Standby redundant method and displayed as Secondary State with Stable condition on the page of **High Availability Status**, the wireless function will be disabled.

Associated **Schedule** Profiles: , , ,

Enable Special SSID Schedule Profiles

Note:

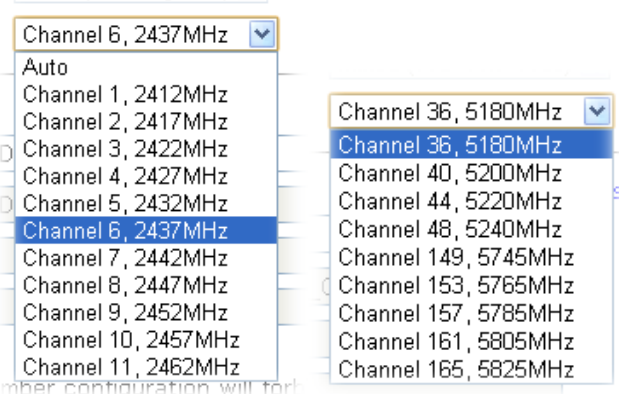
1. Only schedule profiles that have the action "Force Down" are applied to the WLAN, all other actions are ignored. Valid settings are profile indexes 1 to 15.
2. If you **Enable Special SSID Schedule Profiles**, the selected SSID will be forced down.

Note:

Channel setting should not be changed while Wireless 2.4G WAN mode is in use.

Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Mode	<p>For 2.4GHz: At present, the router can connect to 11b Only, 11g Only, 11n Only(2.4 GHz), Mixed (11b+11g), Mixed (11g+11n), and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.</p> <p>For 5GHz: At present, the router can connect to 11a Only, 11n Only(5 GHz), Mixed (11a+11n), and Mixed (11a+11n+11ac) stations simultaneously. Simply choose Mixed (11a+11n+11ac) mode.</p> <p>In which, 802.11b/g operates on 2.4G band, 802.11a operates on 5G band, 802.11n operates on either 2.4G or 5G band, and 802.11ac operates on 5G band only.</p>
Channel	Means the channel of frequency of the wireless LAN. The default channel is 6 (for 2.4GHz) / 36 (for 5GHz). You may

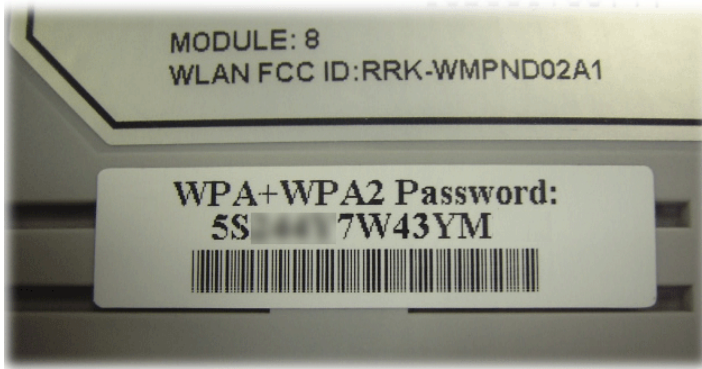
	<p>switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.</p> <p>For 2.4GHz: For 5 GHz:</p> 
<p>Hide SSID</p>	<p>Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity.</p>
<p>SSID</p>	<p>Means the identification of the wireless LAN. SSID can be any text numbers or various special characters.</p>
<p>Isolate</p>	<p>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.</p>
<p>Schedule</p>	<p>Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in Applications >> Schedule setup. The default setting of this field is blank and the function will always work.</p>
<p>Enable Special SSID Schedule Profiles</p>	<p>Selected SSID (2 /3 /4) will be forced up /down based on the schedule profile used.</p> <p><input checked="" type="checkbox"/> Enable Special SSID Schedule Profiles</p> <p>Schedule Profile <input type="text" value="1"/> <input type="checkbox"/> SSID2 <input checked="" type="checkbox"/> SSID3 <input type="checkbox"/> SSID4</p> <p>Schedule Profile <input type="text"/> <input type="checkbox"/> SSID2 <input type="checkbox"/> SSID3 <input type="checkbox"/> SSID4</p> <p>Schedule Profile <input type="text"/> <input type="checkbox"/> SSID2 <input type="checkbox"/> SSID3 <input type="checkbox"/> SSID4</p> <p>Schedule Profile <input type="text"/> <input type="checkbox"/> SSID2 <input type="checkbox"/> SSID3 <input type="checkbox"/> SSID4</p> <p><small>Note:</small></p>

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.



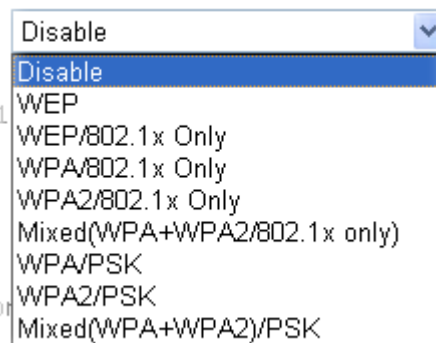
By clicking the **Wireless LAN>>Security Settings**, a new web page will appear so that you could configure the settings of WPA and WEP.

Wireless LAN(2.4GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
<p>Mode: Mixed(WPA+WPA2)/PSK <input type="button" value="v"/></p> <p><u>WPA</u></p> <p>Encryption Mode: TKIP for WPA/AES for WPA2</p> <p>Pre-Shared Key(PSK): <input type="text" value="*****"/></p> <p>Password Strength: <input type="button" value="Weak"/> <input type="button" value="Medium"/> <input type="button" value="Strong"/> </p> <p>Strong password requirements:</p> <ol style="list-style-type: none"> 1. Have at least 7 characters, including numbers and letters. 2. Have at least one upper-case letter and one lower-case letter. 3. Including non-alphanumeric characters is a plus. <p>Type 8~63 ASCII character or 64 Hexadecimal digits leading by "0x", for example "cfigs01a2..." or "0x655abcd....".</p> <p><u>WEP</u></p> <p>Encryption Mode: 64-Bit <input type="button" value="v"/></p> <p><input checked="" type="radio"/> Key 1 : <input type="text" value="*****"/></p> <p><input type="radio"/> Key 2 : <input type="text" value="*****"/></p> <p><input type="radio"/> Key 3 : <input type="text" value="*****"/></p> <p><input type="radio"/> Key 4 : <input type="text" value="*****"/></p> <p>Note:</p> <p>For 64 bit WEP key configurations, please insert 5 ASCII characters or 10 Hexadecimal digits leading by "0x". Examples are "AB312" or "0x4142333132".</p> <p>For 128 bit WEP key configurations, please insert 13 ASCII characters or 26 Hexadecimal digits leading by "0x".</p>			

Available settings are explained as follows:

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



Info

You should also set Wireless LAN(2.4GHz) 802.1X Setting simultaneously if 802.1x mode is selected.

Disable - Turn off the encryption mechanism.

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

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

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

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

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

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

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

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

WPA

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...").

Pre-Shared Key (PSK) - Either 8-63 ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

Password Strength - The system will display the password strength (represented with the word of weak, medium or strong) of the PSK specified above.

WEP

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).

Encryption Mode:

64-Bit
 64-Bit
 128-Bit

All wireless devices must support the same WEP encryption bit size and have the same key. **Four keys** can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.

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

III-1-4 Access Control

In the **Access Control**, the router may restrict wireless access to certain wireless clients only by locking their MAC address into a black or white list. The user may block wireless clients by inserting their MAC addresses into a black list, or only let them be able to connect by inserting their MAC addresses into a white list.

In the **Access Control** web page, users may configure the **white/black** list modes used by each SSID and the MAC addresses applied to their lists.

Wireless LAN(2.4GHz) >> Access Control

Access Control

Enable Mac Address Filter SSID 1 SSID 2
 SSID 3 SSID 4

MAC Address Filter(Limit: 64 entries)

Index	Attribute	MAC Address	Apply SSID	Comment

Client's MAC Address : : : : : :

Apply SSID : SSID 1 SSID 2 SSID 3 SSID 4

Attribute : s: Isolate the station from LAN

Comment :

Backup Access Control: Upload From File:

Note:
Support AP ACL configuration file restoration.

Available settings are explained as follows:

Item	Description
Enable Mac Address Filter	Select to enable the MAC Address filter for wireless LAN

	identified with SSID 1 to 4 respectively. All the clients (expressed by MAC addresses) listed in the box can be grouped under different wireless LAN. For example, they can be grouped under SSID 1 and SSID 2 at the same time if you check SSID 1 and SSID 2.
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Apply SSID	After entering the client's MAC address, check the box of the SSIDs desired to insert this MAC address into their access control list.
Attribute	s: Isolate the station from LAN - select to isolate the wireless connection of the wireless client of the MAC address from LAN.
Comment	Type a brief description for the specified client's MAC address.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.
OK	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.
Backup Access Control	Settings on this web page can be saved as a file which can be restored in the future by this device or other device.
Upload From File	Restore wireless access control settings and applied onto this device.

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

III-1-5 WPS

WPS (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point (vigor router) with the encryption of WPA and WPA2.



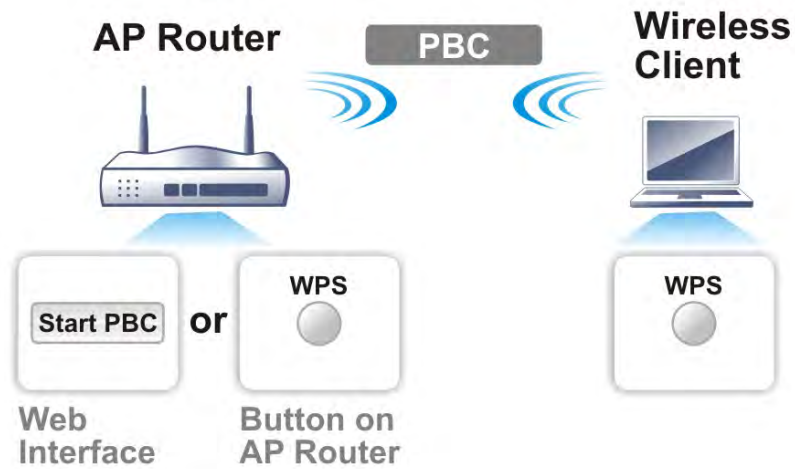
Info

WPS is available for the wireless station with WPS supported.

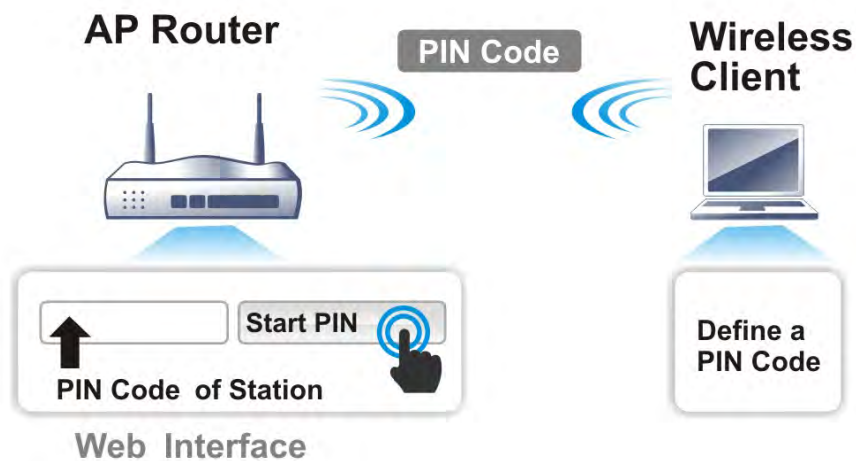
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for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

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

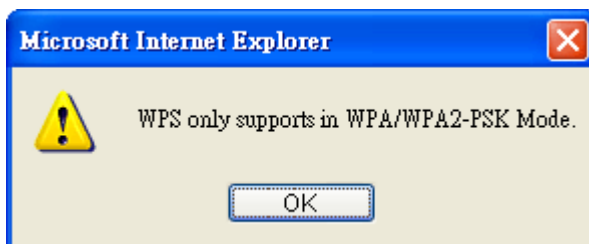
- On the side of Vigor 2862 series which served as an AP, press **WPS** button once on the front panel of the router or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.



- 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
Authentication Mode	Disable


Device Configure


Configure via Push Button	<input type="button" value="Start PBC"/>
Configure via Client PinCode	<input type="text"/> <input type="button" value="Start PIN"/>


Status: The Authentication Mode is NOT WPA/WPA2 PSK!!

Note:

WPS can help your wireless client automatically connect to the Access point.

 : WPS is Disabled.

 : WPS is Enabled.

 : Waiting for WPS requests from wireless clients.

Available settings are explained as follows:

Item	Description
Enable WPS	Check this box to enable WPS setting.
WPS Status	Display related system information for WPS. If the wireless security (encryption) function of the router is properly configured, you can see 'Configured' message here.
SSID	Display the SSID1 of the router. WPS is supported by SSID1 only.
Authentication Mode	Display current authentication mode of the router. Only WPA2/PSK and WPA/PSK support WPS.
Configure via Push Button	Click Start PBC to invoke Push-Button style WPS setup procedure. The router will wait for WPS requests from wireless clients about two minutes. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Please input the PIN code specified in wireless client you wish to connect, and click Start PIN button. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)

III-1-6 WDS

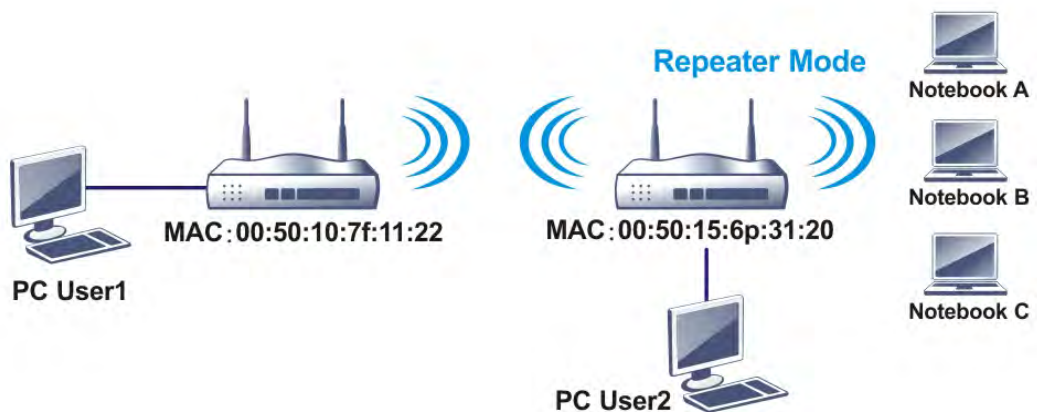
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

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

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

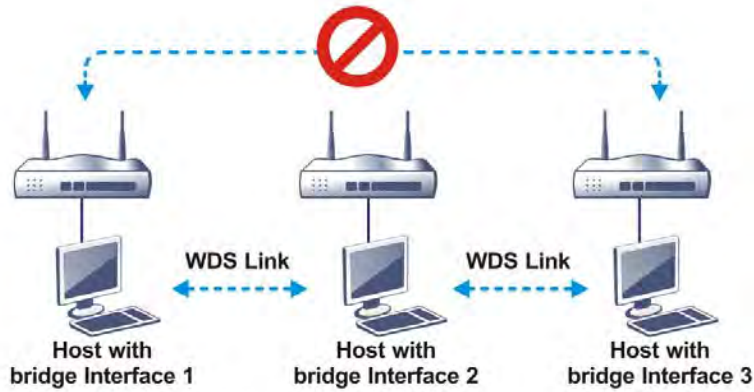


The application for the WDS-Repeater mode is depicted as below:



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

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



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

Wireless LAN(2.4GHz) >> WDS Settings

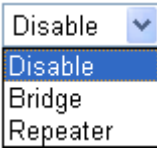
[Set to Factory Default](#)

WDS Settings

<p>Mode: Bridge</p> <hr/> <p>Security:</p> <p><input checked="" type="radio"/> Disable <input type="radio"/> Pre-shared Key</p> <hr/> <p>Pre-shared Key:</p> <p>Type:</p> <p><input type="radio"/> WPA <input checked="" type="radio"/> WPA2</p> <p>Key : <input style="width: 100px;" type="password" value="*****"/></p> <p>Note: WPA and WPA2 are not compatible with DrayTek WPA. Type 8~63 ASCII characters or 64 hexadecimal digits leading by "0x", for example "cfigs01a2..." or "0x655abcd....".</p>	<p>Bridge</p> <p>Enable Peer MAC Address</p> <p><input type="checkbox"/> <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/></p> <p><input type="checkbox"/> <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/></p> <p><input type="checkbox"/> <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/></p> <p><input type="checkbox"/> <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/></p> <p>Note: Disable unused links to get better performance.</p> <hr/> <p>Repeater</p> <p>Enable Peer MAC Address</p> <p><input type="checkbox"/> <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/></p> <p><input type="checkbox"/> <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/></p> <p><input type="checkbox"/> <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/></p> <p><input type="checkbox"/> <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/></p> <hr/> <p>Access Point Function:</p> <p><input checked="" type="radio"/> Enable <input type="radio"/> Disable</p> <hr/> <p>Status:</p> <p><input type="checkbox"/> Send "Hello" message to peers.</p> <p style="text-align: center;"><input type="button" value="Link Status"/></p> <p>Note: The status is valid only when the peer also supports this function.</p>
--	--

Available settings are explained as follows:

Item	Description
Mode	Choose the mode for WDS setting. Disable mode will not invoke any WDS setting. Bridge mode is designed to fulfill the first type of application. Repeater mode is for the second one.

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

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

III-1-7 Advanced Setting

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

Wireless LAN(2.4GHz) >> Advanced Setting

HT Physical Mode

Operation Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel Bandwidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40 <input type="radio"/> 40
Guard Interval	<input type="radio"/> long <input checked="" type="radio"/> auto
Aggregation MSDU(A-MSDU)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Long Preamble	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Tx Power	<input checked="" type="radio"/> 100% <input type="radio"/> 80% <input type="radio"/> 60% <input type="radio"/> 30% <input type="radio"/> 20% <input type="radio"/> 10%
WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Fragment Length (256 - 2346)	<input type="text" value="2346"/> bytes
RTS Threshold (1 - 2347)	<input type="text" value="2347"/> bytes
Country Code	<input type="text"/> (Reference)

OK

Available settings are explained as follows:

Item	Description
Operation Mode	<p>Mixed Mode - the router can transmit data with the ways supported in both 802.11a/b/g and 802.11n standards. However, the entire wireless transmission will be slowed down if 802.11g or 802.11b wireless client is connected.</p> <p>Green Field - to get the highest throughput, please choose such mode. Such mode can make the data transmission 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.</p>
Channel Bandwidth	<p>20- the router will use 20Mhz for data transmission and receiving between the AP and the stations.</p> <p>20/40 - Vigor Router will scan for nearby wireless AP, and then use 20MHz if the number of AP is more than 10, or use 40MHz if it's not.</p> <p>40- the router will use 40Mhz for data transmission and receiving between the AP and the stations.</p>
Guard Interval	It is to assure the safety of propagation delays and reflections for the sensitive digital data. If you choose auto as guard interval, the AP router will choose short guard interval (increasing the wireless performance) or long guard interval for data transmit based on the station capability.
Aggregation MSDU (A-MSDU)	Aggregation MSDU can combine frames with different sizes. It is used for improving MAC layer's performance for some brand's clients. The default setting is Enable .
Long Preamble	This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with

	128 bit sync field. However, some original 11b wireless network devices only support long preamble. Click Enable to use Long Preamble if needed to communicate with this kind of devices.
TX Power	Set the power percentage for transmission signal of access point. The greater the value is, the higher intensity of the signal will be.
WMM Capable	WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC_BE , AC_BK, AC_VI and AC_VO for WMM. To apply WMM parameters for wireless data transmission, please click the Enable radio button.
APSD Capable	APSD (automatic power-save delivery) is an enhancement over the power-save mechanisms supported by Wi-Fi networks. It allows devices to take more time in sleeping state and consume less power to improve the performance by minimizing transmission latency. The default setting is Disable .
Fragment Length (256 - 2346)	Set the Fragment threshold. Do not modify default value if you don't know what it is, default value is 2346.
RTS Threshold (1 - 2347)	Minimize the collision (unit is bytes) between hidden stations to improve wireless performance. Set the RTS threshold. Do not modify default value if you don't know what it is, default value is 2347.
Country Code	Vigor router broadcasts country codes by following the 802.11d standard. However, some wireless stations will detect / scan the country code to prevent conflict occurred. If conflict is detected, wireless station will be warned and is unable to make network connection. Therefore, changing the country code to ensure successful network connection will be necessary for some clients.

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

III-1-8 Station Control

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

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

Wireless LAN(2.4GHz) >> Station Control

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

Note:

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

OK Cancel

Available settings are explained as follows:

Item	Description
SSID	Display the SSID that the wireless station will use it to connect with Vigor router.
Enable	Check the box to enable the station control function.
Connection Time / Reconnection Time	Use the drop down list to choose the duration for the wireless client connecting /reconnecting to Vigor router. Or, 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.
Hotspot Web Portal	Click it to access in to Hotspot Web Portal page for modifying the settings if required.

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

III-1-9 Bandwidth Management

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

Wireless LAN >> Bandwidth Management

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

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

OK Cancel

Available settings are explained as follows:

Item	Description
SSID	Display the specific SSID name.
Enable	Check this box to enable the bandwidth management for clients.
Bandwidth Limit Type	Auto Adjustment - Bandwidth limit is determined by the system automatically. Per Station Limit - Bandwidth limit is determined according to the limitation of the wireless client.
Total Upload Limit	It is available when Auto Adjustment is selected. Type a value to define the maximum data traffic (uploading) for all of the wireless clients connecting to Vigor2862.
Total Download Limit	It is available when Auto Adjustment is selected. Type a value to define the maximum data clientstations connecting to Vigor2862.
Upload Limit	It is available when Per Station Limit is selected. Type a value to define the maximum data traffic (uploading) for each wireless client connecting to Vigor2862.
Download Limit	It is available when Per Station Limit is selected Type a value to define the maximum data traffic (downloading) for each wireless client connecting to Vigor2862.

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

III-1-10 AP Discovery

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

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

Wireless LAN(2.4GHz) >> Access Point Discovery

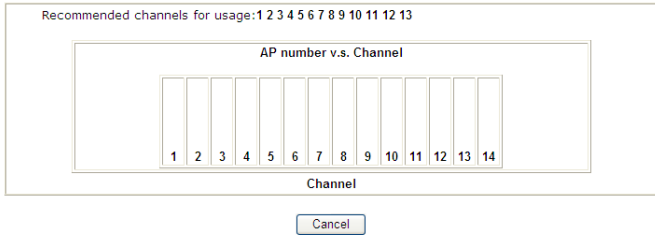
Access Point List

Index	BSSID	Channel	RSSI	SSID	Authentication
<input type="button" value="Scan"/>					
See Statistics .					
Add to WDS Settings :					
AP's MAC address			<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>		
<input type="button" value="Add to"/>			<input checked="" type="radio"/> Bridge <input type="radio"/> Repeater		

Note:

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

Available settings are explained as follows:

Item	Description
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button.
Statistics	It displays the statistics for the channels used by APs. <small>Wireless LAN >> Site Survey Statistics</small> 
Add to	If you want the found AP applying the WDS settings, please type in the AP's MAC address on the bottom of the page and click Bridge or Repeater. Next, click Add to . Later, the MAC address of the AP will be added to Bridge or Repeater field of WDS settings page.

III-1-11 Airtime Fairness

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

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

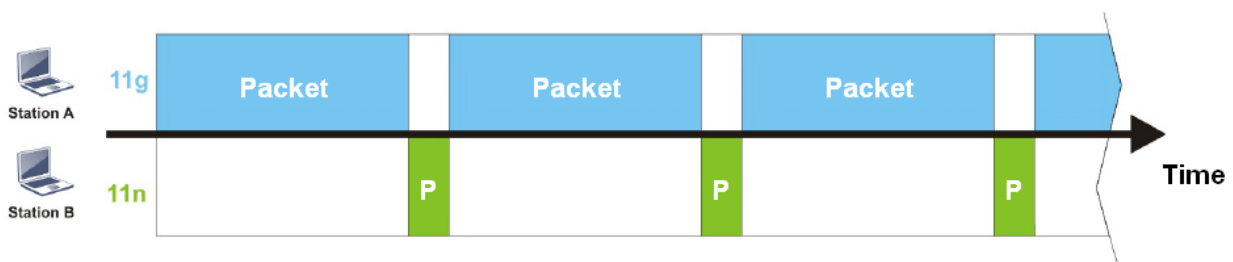
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

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

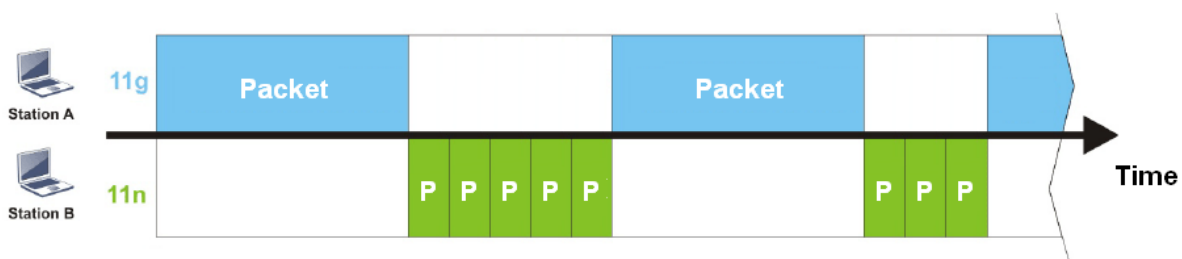
The principle behind the IEEE802.11 channel access mechanisms is that each station has *equal probability* to access the channel. When wireless stations have similar data rate, this principle leads to a fair result. In this case, stations get similar channel access time which is called airtime.

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

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



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



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

Suitable environment:

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

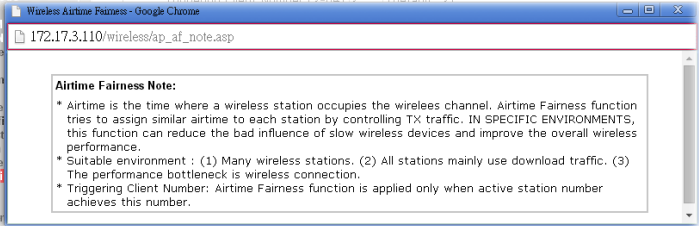
Wireless LAN(2.4GHz) >> Airtime Fairness

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

Note:

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

Available settings are explained as follows:

Item	Description
Enable Airtime Fairness	<p>Try to assign similar airtime to each wireless station by controlling TX traffic.</p> <p>Airtime Fairness - Click the link to display the following screen of airtime fairness note.</p> <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;">  </div> <p>Triggering Client Number -Airtime Fairness function is applied only when active station number achieves this number.</p>

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

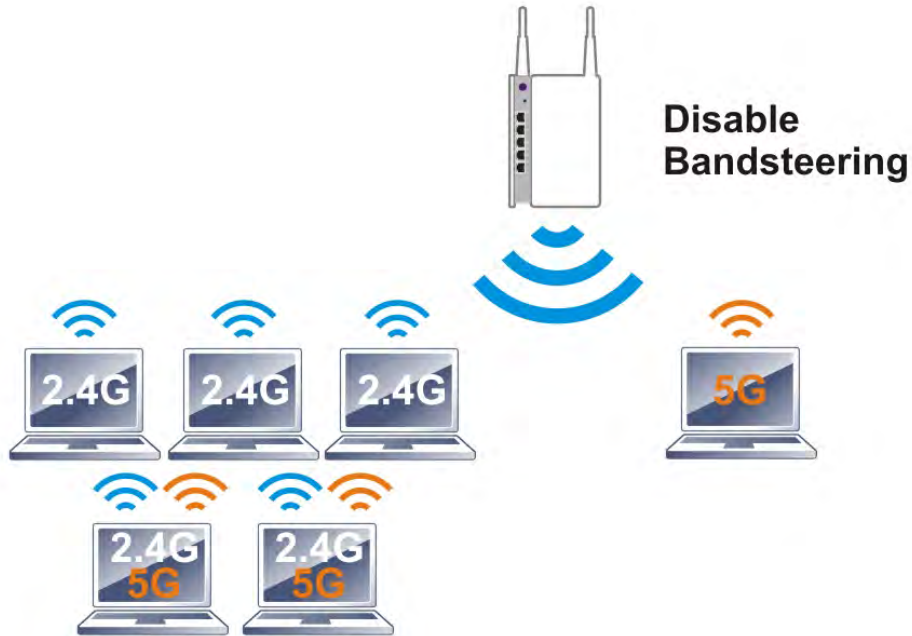


Info

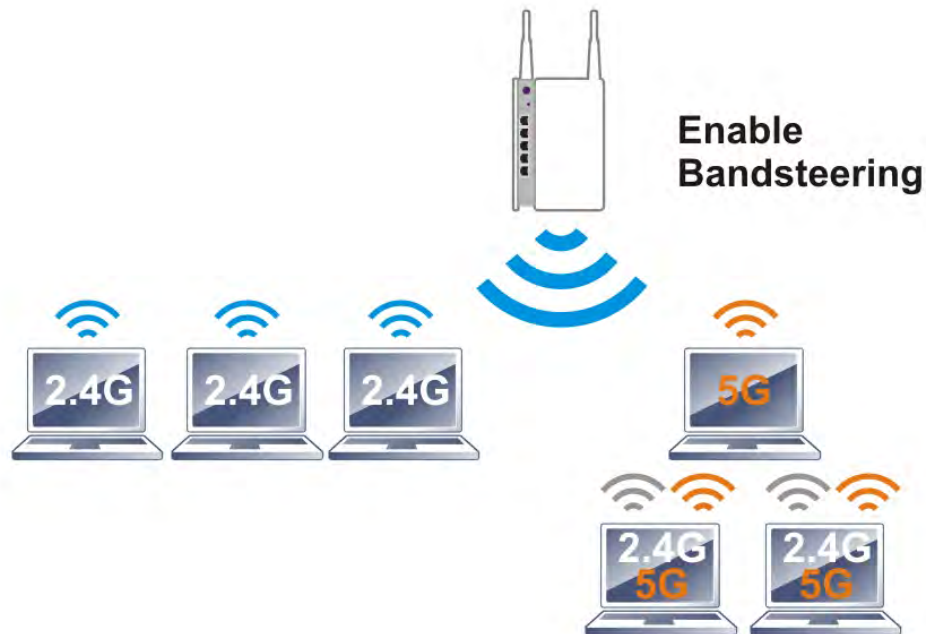
Airtime Fairness function and Bandwidth Limit function should be mutually exclusive. So their webs have extra actions to ensure these two functions are not enabled simultaneously.

III-1-12 Band Steering

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



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



Info

To make Band Steering work successfully, SSID and security on 2.4GHz also MUST be broadcasted on 5GHz.

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

Wireless LAN(2.4GHz) >> Band Steering

Enable **Band Steering**
 Check Time for WLAN Client 5G Capability second(s) (1 ~ 60) (Default: 30)

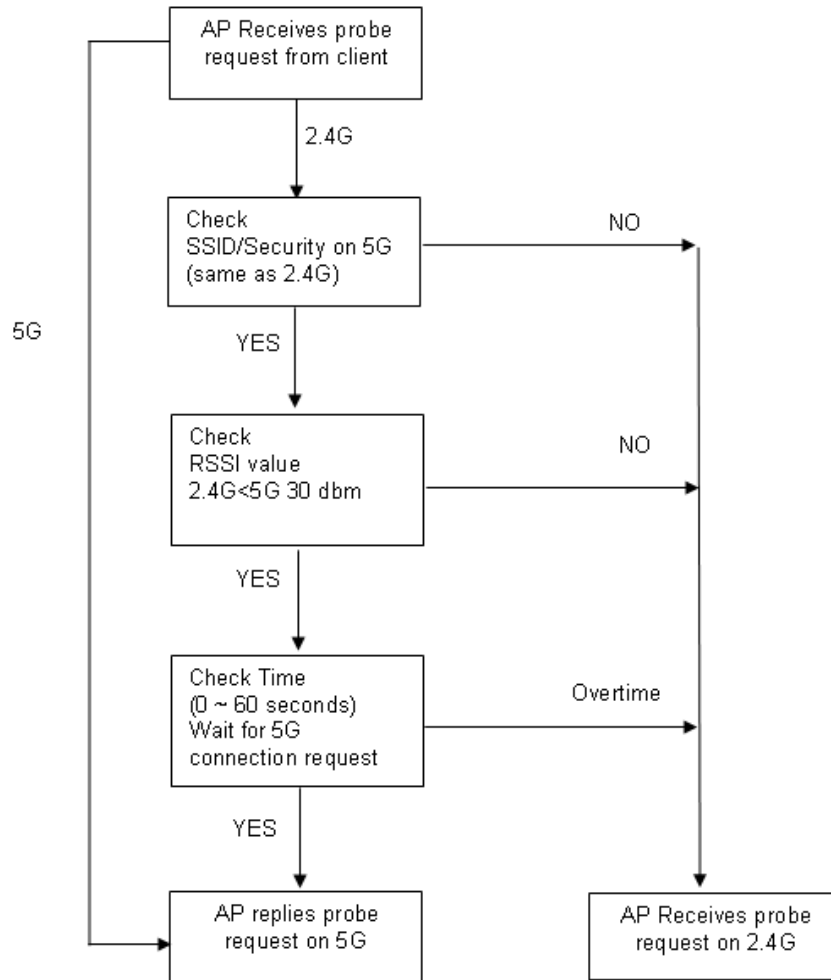
Note:
Please setup at least one pair of 2.4GHz and 5GHz Wireless LAN with the same SSID and security.

Available settings are explained as follows:

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

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

Below shows how Band Steering works.



How to Use Band Steering?

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

Wireless LAN(2.4GHz) >> Band Steering

Enable **Band Steering**
 Check Time for WLAN Client 5G Capability second(s) (1 ~ 60) (Default: 30)

Note:

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

3. Click **OK** to save the settings.
4. Open **Wireless LAN (2.4GHz)>>General Setup** and **Wireless LAN (5GHz)>> General Setup**. Configure SSID as *DrayTek2862_BandSteering* for both pages. Click **OK** to save the settings.

Wireless LAN(2.4GHz) >> General Setup

General Setting (IEEE 802.11)

Enable Wireless LAN
 Mode :
 Channel:

Enable	Active	Hide SSID	SSID	Isolate Member	Isolate VPN
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	DrayTek2862_BandSteering	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DrayTek_Guest	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>

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

Wireless LAN(5GHz) >> General Setup

General Setting (IEEE 802.11)

Enable Wireless LAN
 Mode :
 Channel:

Enable	Active	Hide SSID	SSID	Isolate Member	Isolate VPN
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	DrayTek2862_BandSteering	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DrayTek_5G_Guest	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>

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

Same settings for 2.4GHz and 5GHz

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

Wireless LAN(2.4GHz) >> Security Settings

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

Same value for 2.4GHz and 5GHz

Wireless LAN(5GHz) >> Security Settings

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

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

III-1-13 Roaming

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

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

Wireless LAN(2.4GHz) >> Roaming

Router-assisted Client Roaming Parameters

Disable RSSI Requirement

Strictly Minimum RSSI -73 dBm (42 %) (Default: -73)

Minimum RSSI -66 dBm (60 %) (Default: -66)

with Adjacent AP RSSI over 5 dB (Default: 5)

Available settings are explained as follows:

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

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

III-1-14 Station List

Station List provides the knowledge of connecting wireless clients now along with its status code. Each tab (general, advanced, neighbor) will display different status information (including IP address, MAC address, Associated with, AID, RSSI, Rate, BW, PSM, WMM, PhMd, MCS, Venfor, Approx. Distance, SSID, Visit Time and so on).

Wireless LAN(2.4GHz) >> Station List

Station List

General Advanced Neighbor

Index	Status	IP Address	MAC Address	Associated with
<div style="text-align: center; margin-top: 50px;">Refresh</div>				

Status Codes :
C: Connected, No encryption.
E: Connected, WEP.
P: Connected, WPA.
A: Connected, WPA2.
B: Blocked by Access Control.
N: Connecting.
F: Fail to pass WPA/PSK authentication.

Add to Access Control :

Client's MAC address : : : : :

Note:

After a station connects to the router successfully, it may be turned off without notice. In that case, it will still be on the list until the connection expires.

Add

Available settings are explained as follows:

Item	Description
Refresh	Click this button to refresh the status of station list.
Add	Click this button to add current typed MAC address into Access Control.

This page is left blank.

Part IV VPN



VPN



SSL VPN



Certificate
Management

A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link.

It is a form of VPN that can be used with a standard Web browser.

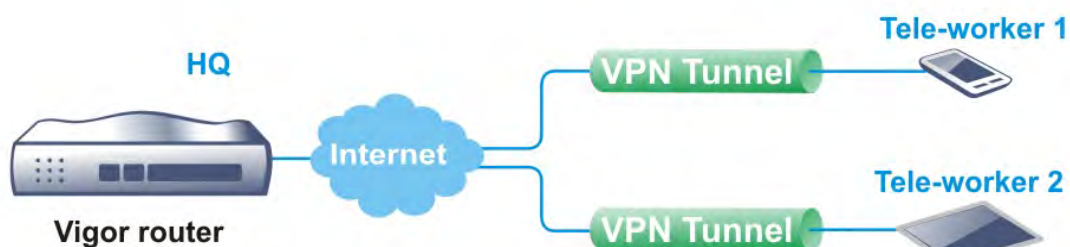
A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Here Vigor router support digital certificates conforming to standard X.509.

IV-1 VPN and Remote Access

A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link.

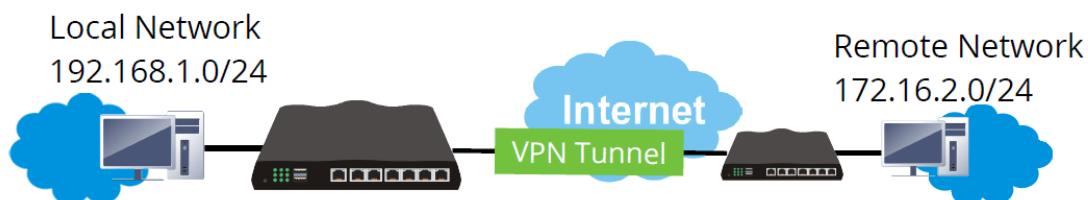
The VPN built is suitable for:

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



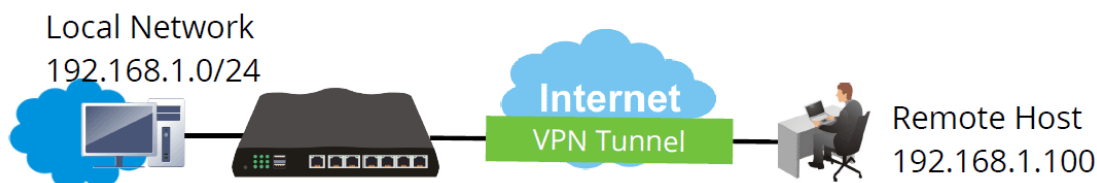
Site-to-Site (LAN-to-LAN)

- A connection between two router's LAN networks.
- Allows employees in branch offices and head office to share the same network resources.



Remote Access (Remote Dial-in)

- A connection between the remote host and router's LAN network. The host will use an IP address in the local subnet.
- Allows employees to access the company's internal resources when they are traveling.



Web User Interface

IV-1-1 VPN Client Wizard

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

1. Open Wizards>>VPN Client Wizard. The following page will appear.

VPN Client Wizard

Choose VPN Establishment Environment

LAN-to-LAN VPN Client Mode Selection:

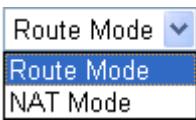
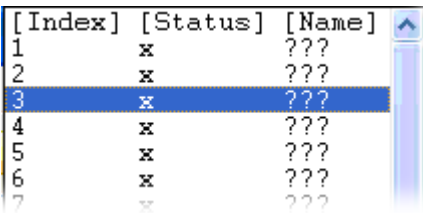
Please choose a LAN-to-LAN Profile:

Note:

1. Please use Route Mode for typical LAN-to-LAN tunnels.
2. If the remote network is only expecting a single client or IP and is not configured to route the subnet then select NAT Mode.
3. If you are unsure of your configuration select Route Mode.

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
LAN-to-LAN Client Mode Selection	Choose the client mode. Route Mode/NAT Mode - If the remote network only allows you to dial in with single IP, please choose NAT mode, otherwise please choose Route Mode. 
Please choose a LAN-to-LAN Profile	There are 32 VPN profiles for users to set. 

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

VPN Client Wizard

VPN Connection Setting

Security Ranking: Very High L2TP over IPsec High IPsec / SSL Medium PPTP (Encryption) Low L2TP / PPTP (None Encryption)	Throughput Ranking: Very High L2TP / PPTP (None Encryption) High IPsec Medium L2TP over IPsec / PPTP (Encryption) Low SSL
--	--

Select VPN Type:

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

< Back Next > Finish Cancel

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



Info

The following descriptions for VPN Type are based on the Route Mode specified in LAN-to-LAN Client Mode Selection.

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

VPN Client PPTP Encryption Settings

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

When you choose IPsec, you will see the following graphic:

VPN Client IPsec Settings

Profile Name	???
VPN Dial-Out Through	WAN1 First
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
IKE Authentication Method	
<input checked="" type="radio"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input type="radio"/> Digital Signature (X.509)	
Peer ID	None
Local ID	
<input checked="" type="radio"/> Alternative Subject Name First	
<input type="radio"/> Subject Name First	
Local Certificate	None
IPsec Security Method	
<input checked="" type="radio"/> Medium (AH)	
<input type="radio"/> High (ESP)	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

When you choose SSL, you will see the following graphic:

VPN Client Wizard

Profile Name	???
VPN Dial-Out Through	WAN1 First
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
Server Port (for SSL Tunnel):	443
Username	???
Password	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

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

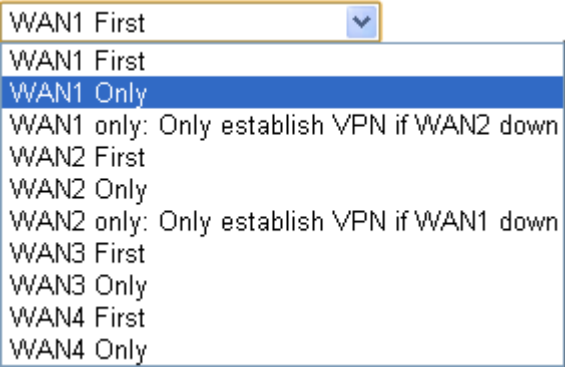
VPN and Remote Access >> VPN Client Wizard

VPN Client L2TP over IPsec (Nice to Have) Settings

Profile Name	VPN-2
VPN Dial-Out Through	WAN1 First
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
IKE Authentication Method	
<input checked="" type="radio"/> Pre-Shared Key
Confirm Pre-Shared Key
<input type="radio"/> Digital Signature (X.509)	
Peer ID	None
Local ID	
<input type="radio"/> Alternative Subject Name First	
<input type="radio"/> Subject Name First	
Local Certificate	None
IPsec Security Method	
<input checked="" type="radio"/> Medium (AH)	
<input type="radio"/> High (ESP)	DES without Authentication
Username	???
Password	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such profile. The length of the file is limited to 10 characters.

VPN Dial-Out Through	<p>Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only.</p>  <p>WAN1 First/ WAN2 First /WAN3 First/WAN4 First- While connecting, the router will use WAN1/WAN2/WAN3/WAN4 as the first channel for VPN connection. If WAN1/WAN2/WAN3/WAN4 fails, the router will use another WAN interface instead.</p> <p>WAN1 Only /WAN2 Only/WAN3 Only/WAN4 Only - While connecting, the router will use WAN1/WAN2/WAN3/WAN4 as the only channel for VPN connection.</p> <p>WAN1 Only: Only establish VPN if WAN2 down - If WAN2 failed, the router will use WAN1 for VPN connection.</p> <p>WAN2 Only: Only establish VPN if WAN1 down - If WAN1 failed, the router will use WAN2 for VPN connection.</p>
Always On	Check to enable router always keep VPN connection.
Server IP/Host Name for VPN	Type the IP address of the server or type the host name for such VPN profile.
IKE Authentication Method	<p>IKE Authentication Method usually applies to those are remote dial-in user or node (LAN to LAN) which uses dynamic IP address and IPsec-related VPN connections such as L2TP over IPsec and IPsec tunnel.</p> <p>Pre-Shared Key- Specify a key for IKE authentication.</p> <p>Confirm Pre-Shared Key-Confirm the pre-shared key.</p>
Digital Signature (X.509)	<p>Click Digital Signature to invoke this function.</p> <p>Peer ID - Choose the peer ID selection from the drop down list.</p> <p>Local ID - Choose Alternative Subject Name First or Subject Name First.</p> <p>Local Certificate - Use the drop down list to choose one of the certificates for using. You have to configure one certificate at least previously in Certificate Management >> Local Certificate. Otherwise, the setting you choose here will not be effective.</p>
IPsec Security Method	<p>Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.</p> <p>High - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.</p>
User Name	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above.

	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:	No
Server IP/Host Name:	172.16.3.8
IKE Authentication Method:	Pre-Shared Key
IPsec Security Method:	AH-SHA1
Remote Network IP:	0.0.0.0
Remote Network Mask:	255.255.255.0

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

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

Available settings are explained as follows:

Item	Description
Go to the VPN Connection Management	Click this radio button to access VPN and Remote Access>>Connection Management for viewing VPN Connection status.
Do another VPN Server Wizard Setup	Click this radio button to set another profile of VPN Server through VPN Server Wizard.
View more detailed configuration	Click this radio button to access VPN and Remote Access>>LAN to LAN for viewing detailed configuration.

IV-1-2 VPN Server Wizard

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

1. Open **Wizards>>VPN Server Wizard**. The following page will appear.

VPN Server Wizard

Choose VPN Establishment Environment

VPN Server Mode Selection: Remote Dial-in User (Teleworker ▼)

Please choose a LAN-to-LAN Profile: 1 x ??? ▼

Please choose a Dial-in User Accounts: 8 x ??? ▼

Allowed Dial-in Type:

- PPTP
- IPsec
- L2TP with IPsec Policy None ▼
- SSL Tunnel

< Back
Next >
Finish
Cancel

Available settings are explained as follows:

Item	Description
VPN Server Mode Selection	Choose the direction for the VPN server. Site to Site VPN - To set a LAN-to-LAN profile automatically, please choose Site to Site VPN. Remote Dial-in User -You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in via VPN connection.
Please choose a LAN-to-LAN Profile	This item is available when you choose Site to Site VPN (LAN-to-LAN) as VPN server mode. There are 32 VPN profiles for users to set.
Please choose a Dial-in User Accounts	This item is available when you choose Remote Dial-in User (Teleworker) as VPN server mode. There are 32 VPN tunnels for users to set.
Allowed Dial-in Type	This item is available after you choose any one of dial-in user account profiles. Next, you have to select suitable dial-in type for the VPN server profile. There are several types provided here (similar to VPN Client Wizard).

	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec <input checked="" type="checkbox"/> L2TP with IPsec Policy <input checked="" type="checkbox"/> SSL Tunnel
--	---

None
 None
 Nice to Have
 Must

Different Dial-in Type will lead to different configuration page. In addition, adjustable items for each dial-in type will be changed according to the VPN Server Mode (Site to Site VPN and Remote Dial-in User) selected.

- 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:

VPN Server Wizard

VPN Authentication Setting

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

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

VPN Server Wizard

VPN Authentication Setting

Profile Name	???
PPTP / L2TP / L2TP over IPsec / SSL Tunnel Authentication	
Username	???
Password	
IPsec / L2TP over IPsec Authentication	
<input checked="" type="checkbox"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input type="checkbox"/> Digital Signature (X.509)	
Peer ID	None
Local ID	
<input type="radio"/> Alternative Subject Name First	
<input type="radio"/> Subject Name First	
Peer IP/VPN Client IP	
Peer ID	
Site to Site Information	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

When you check IPsec, you will see the following graphic:

VPN Server Wizard

VPN Authentication Setting

Profile Name	???
IPsec / L2TP over IPsec Authentication	
<input checked="" type="checkbox"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input type="checkbox"/> Digital Signature (X.509)	
Peer ID	None
Local ID	
<input type="radio"/> Alternative Subject Name First	
<input type="radio"/> Subject Name First	
Peer IP/VPN Client IP	
Peer ID	
Site to Site Information	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such profile. The length of the file is limited to 10 characters.
User Name	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 11 characters.
Password	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 11 characters.

Pre-Shared Key	For IPsec/L2TP IPsec authentication, you have to type a pre-shared key. The length of the name is limited to 64 characters.
Confirm Pre-Shared Key	Type the pre-shared key again for confirmation.
Digital Signature (X.509)	Check the box of Digital Signature to invoke this function. Peer ID - Choose the peer ID selection from the drop down list. Local ID - Choose Alternative Subject Name First or Subject Name First .
Peer IP/VPN Client IP	Type the WAN IP address or VPN client IP address for the remote client.
Peer ID	Type the ID name for the remote client. The length of the name is limited to 47 characters.
Remote Network IP	Please type one LAN IP address (according to the real location of the remote host) for building VPN connection.
Remote Network Mask	Please 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:	2
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

Server Wizard Setup	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.

IV-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**.

VPN and Remote Access >> Remote Access Control Setup

Remote Access Control Setup

<input checked="" type="checkbox"/>	Enable PPTP VPN Service
<input checked="" type="checkbox"/>	Enable IPSec VPN Service
<input checked="" type="checkbox"/>	Enable L2TP VPN Service
<input checked="" type="checkbox"/>	Enable SSL VPN Service

Note:

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

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

IV-1-4 PPP General Setup

This submenu only applies to PPP-related VPN connections, such as PPTP, L2TP, L2TP over IPsec.

VPN and Remote Access >> PPP General Setup

PPP General Setup

<p>PPP/MP Protocol</p> <p>Dial-In PPP Authentication: <input type="text" value="PAP/CHAP/MS-CHAP/MS-CHAPv2"/></p> <p>Dial-In PPP Encryption(MPPE): <input type="text" value="Optional MPPE"/></p> <p>Mutual Authentication (PAP): <input type="radio"/> Yes <input checked="" type="radio"/> No</p> <p>Username: <input type="text"/></p> <p>Password: <input type="text"/></p> <p>IP Address Assignment for Dial-In Users (When DHCP Disable set)</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th></th> <th>Start IP Address</th> <th>IP Pool Counts</th> </tr> </thead> <tbody> <tr><td>LAN 1</td><td>192.168.1.200</td><td>50</td></tr> <tr><td>LAN 2</td><td>192.168.2.200</td><td>50</td></tr> <tr><td>LAN 3</td><td>192.168.3.200</td><td>50</td></tr> <tr><td>LAN 4</td><td>192.168.4.200</td><td>50</td></tr> <tr><td>LAN 5</td><td>192.168.5.200</td><td>50</td></tr> <tr><td>LAN 6</td><td>192.168.6.200</td><td>50</td></tr> <tr><td>LAN 7</td><td>192.168.7.200</td><td>50</td></tr> <tr><td>LAN 8</td><td>192.168.8.200</td><td>50</td></tr> <tr><td>DMZ</td><td>192.168.17.200</td><td>50</td></tr> </tbody> </table>		Start IP Address	IP Pool Counts	LAN 1	192.168.1.200	50	LAN 2	192.168.2.200	50	LAN 3	192.168.3.200	50	LAN 4	192.168.4.200	50	LAN 5	192.168.5.200	50	LAN 6	192.168.6.200	50	LAN 7	192.168.7.200	50	LAN 8	192.168.8.200	50	DMZ	192.168.17.200	50	<p>PPP Authentication Methods</p> <p><input checked="" type="checkbox"/> Remote Dial-in User</p> <p><input checked="" type="checkbox"/> RADIUS</p> <p><input checked="" type="checkbox"/> AD/LDAP</p> <p>PPTP LDAP Profile</p> <p><input checked="" type="checkbox"/> TACACS+</p> <p>Note:</p> <ol style="list-style-type: none"> Please select 'PAP Only' 'Dial-In PPP Authentication',if you want to use AD/LDAP or TACACS+ for PPP Authentication. Default priority is Remote Dial-in User -> RADIUS -> AD/LDAP -> TACACS+. Vigor router also supports Frame-IP-Address from RADIUS server to assign IP address to VPN client. <p>While using Radius or LDAP Authentication:</p> <p>Assign IP from subnet: <input type="text" value="LAN1"/></p>
	Start IP Address	IP Pool Counts																													
LAN 1	192.168.1.200	50																													
LAN 2	192.168.2.200	50																													
LAN 3	192.168.3.200	50																													
LAN 4	192.168.4.200	50																													
LAN 5	192.168.5.200	50																													
LAN 6	192.168.6.200	50																													
LAN 7	192.168.7.200	50																													
LAN 8	192.168.8.200	50																													
DMZ	192.168.17.200	50																													

OK

Available settings are explained as follows:

Item	Description
Dial-In PPP Authentication	<p>PAP Only - elect this option to force the router to authenticate dial-in users with the PAP protocol.</p> <p>PAP/CHAP/MS-CHAP/MS-CHAPv2 - Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication.</p>
Dial-In PPP Encryption (MPPE)	<p>Optional MPPE - This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit "no MPPE encrypted packets". Otherwise, the MPPE encryption scheme will be used to encrypt the data.</p> <ul style="list-style-type: none"> ● Require MPPE (40/128bits) - Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data.

	<ul style="list-style-type: none"> ● Maximum MPPE - This option indicates that the router will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.
Mutual Authentication (PAP)	<p>The Mutual Authentication function is mainly used to communicate with other routers or clients who need bi-directional authentication in order to provide stronger security, for example, Cisco routers. So you should enable this function when your peer router requires mutual authentication. You should further specify the User Name and Password of the mutual authentication peer.</p> <p>The length of the name/password is limited to 23/19 characters.</p>
IP Address Assignment for Dial-In Users (when DHCP Disable set)	<p>Enter a start IP address for the dial-in PPP connection for LAN1.</p> <p>LAN2 ~ LAN8 will be available if it is enabled. Refer to LAN>>General Setup for enabling the LAN interface.</p>
PPP Authentication Methods	<p>Select the method(s) to be used for authentication in PPP connection.</p> <p>PPP Authentication Methods</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Remote Dial-in User <input checked="" type="checkbox"/> RADIUS <input checked="" type="checkbox"/> AD/LDAP
PPTP LDAP Profile	<p>Configured LDAP profiles will be listed under such item. Simply check the one you want to enable the PPP authentication by LDAP server profiles.</p> <p>However, if there is no profile listed, simply click the link of PPTP LDAP Profile to create/add some new LDAP profiles you want.</p>
While using Radius or LDAP Authentication	<p>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.</p>

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

IV-1-5 IPsec General Setup

In IPsec General Setup, there are two major parts of configuration.

There are two phases of IPsec.

- Phase 1: negotiation of IKE parameters including encryption, hash, Diffie-Hellman parameter values, and lifetime to protect the following IKE exchange, authentication of both peers using either a Pre-Shared Key or Digital Signature (x.509). The peer that starts the negotiation proposes all its policies to the remote peer and then remote peer tries to find a highest-priority match with its policies. Eventually to set up a secure tunnel for IKE Phase 2.
- Phase 2: negotiation IPsec security methods including Authentication Header (AH) or Encapsulating Security Payload (ESP) for the following IKE exchange and mutual examination of the secure tunnel establishment.

There are two encapsulation methods used in IPsec, **Transport** and **Tunnel**. The **Transport** mode will add the AH/ESP payload and use original IP header to encapsulate the data payload only. It can just apply to local packet, e.g., L2TP over IPsec. The **Tunnel** mode will not only add the AH/ESP payload but also use a new IP header (Tunneled IP header) to encapsulate the whole original IP packet.

Authentication Header (AH) provides data authentication and integrity for IP packets passed between VPN peers. This is achieved by a keyed one-way hash function to the packet to create a message digest. This digest will be put in the AH and transmitted along with packets. On the receiving side, the peer will perform the same one-way hash on the packet and compare the value with the one in the AH it receives.

Encapsulating Security Payload (ESP) is a security protocol that provides data confidentiality and protection with optional authentication and replay detection service.

VPN and Remote Access >> IPsec General Setup

VPN IKE/IPsec General Setup
Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method

Certificate for Dial-in None ▾

Pre-Shared Key

Pre-Shared Key

Confirm Pre-Shared Key

IPsec Security Method

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

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

Available settings are explained as follows:

Item	Description
IKE Authentication Method	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

	<p>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.</p>
IPsec Security Method	<p>Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.</p> <p>High (ESP) - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.</p>

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

IV-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

X509 Peer ID Accounts: [Set to Factory Default](#)

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

Available settings are explained as follows:

Item	Description
Set to Factory Default	Click it to clear all indexes.
Index	Click the number below Index to access into the setting page

	of IPsec Peer Identity.
Name	Display the profile name of that index.

Click each index to edit one peer digital certificate. There are three security levels of digital signature authentication: Fill each necessary field to authenticate the remote peer. The following explanation will guide you to fill all the necessary fields.

VPN and Remote Access >> IPsec Peer Identity

Profile Index : 4

Profile Name

Enable this account

Accept Any Peer ID

Accept Subject Alternative Name

Type

Domain Name

Accept Subject Name

Country (C)

State (ST)

Location (L)

Organization (O)

Organization Unit (OU)

Common Name (CN)

Email (E)

Available settings are explained as follows:

Item	Description
Profile Name	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.

IV-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.

VPN and Remote Access >> Remote Dial-in User



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

Index	User	Active	Status	Index	User	Active	Status
1.	???	<input type="checkbox"/>	---	17.	???	<input type="checkbox"/>	---
2.	???	<input type="checkbox"/>	---	18.	???	<input type="checkbox"/>	---
3.	???	<input type="checkbox"/>	---	19.	???	<input type="checkbox"/>	---
4.	???	<input type="checkbox"/>	---	20.	???	<input type="checkbox"/>	---
5.	???	<input type="checkbox"/>	---	21.	???	<input type="checkbox"/>	---
6.	???	<input type="checkbox"/>	---	22.	???	<input type="checkbox"/>	---
7.	???	<input type="checkbox"/>	---	23.	???	<input type="checkbox"/>	---
8.	???	<input type="checkbox"/>	---	24.	???	<input type="checkbox"/>	---
9.	???	<input type="checkbox"/>	---	25.	???	<input type="checkbox"/>	---
10.	???	<input type="checkbox"/>	---	26.	???	<input type="checkbox"/>	---
11.	???	<input type="checkbox"/>	---	27.	???	<input type="checkbox"/>	---
12.	???	<input type="checkbox"/>	---	28.	???	<input type="checkbox"/>	---
13.	???	<input type="checkbox"/>	---	29.	???	<input type="checkbox"/>	---
14.	???	<input type="checkbox"/>	---	30.	???	<input type="checkbox"/>	---
15.	???	<input type="checkbox"/>	---	31.	???	<input type="checkbox"/>	---
16.	???	<input type="checkbox"/>	---	32.	???	<input type="checkbox"/>	---

Note:

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

Download Smart VPN Client:

[Smart VPN Client for Windows PC](#)

[Smart VPN Android/iOS App](#)

Available settings are explained as follows:

Item	Description
Set to Factory Default	Click to clear all indexes.
Index	Click the number below Index to access into the setting page of Remote Dial-in User.
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.

VPN and Remote Access >> Remote Dial-in User

Index No. 1

<p>User account and Authentication</p> <p><input checked="" type="checkbox"/> Enable this account</p> <p>Idle Timeout <input type="text" value="300"/> second(s)</p> <hr/> <p>Allowed Dial-In Type</p> <p><input checked="" type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> IPsec Tunnel</p> <p><input checked="" type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/></p> <p><input checked="" type="checkbox"/> SSL Tunnel</p> <p><input type="checkbox"/> Specify Remote Node</p> <p>Remote Client IP <input type="text"/></p> <p>or Peer ID <input type="text"/></p> <p>Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block</p> <p>Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block <i>(for some IGMP,IP-Camera,DHCP Relay..etc.)</i></p> <hr/> <p>Subnet</p> <p><input type="text" value="LAN 1"/></p> <p><input type="checkbox"/> Assign Static IP Address</p> <p><input type="text" value="0.0.0.0"/></p>	<p>Username <input style="background-color: #cccccc;" type="text" value="???"/></p> <p>Password(Max 19 char) <input style="background-color: #cccccc;" type="text"/></p> <p><input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP)</p> <p>PIN Code <input style="background-color: #cccccc;" type="text"/></p> <p>Secret <input style="background-color: #cccccc;" type="text"/></p> <hr/> <p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p>IKE Pre-Shared Key <input style="background-color: #cccccc;" type="text"/></p> <p><input type="checkbox"/> Digital Signature(X.509)</p> <p><input type="text" value="None"/></p> <hr/> <p>IPsec Security Method</p> <p><input checked="" type="checkbox"/> Medium(AH)</p> <p>High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p> <p>Local ID (optional) <input style="background-color: #cccccc;" type="text"/></p>
--	--

Available settings are explained as follows:

Item	Description
User account and Authentication	<p>Enable this account - Check the box to enable this function.</p> <p>Idle Timeout- If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.</p>
Allowed Dial-In Type	<p>PPTP - Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.</p> <p>IPsec Tunnel - Allow the remote dial-in user to make an IPsec VPN connection through Internet.</p> <p>L2TP with IPsec Policy - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below:</p> <ul style="list-style-type: none"> ● None - Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection. ● Nice to Have - Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. ● Must -Specify the IPsec policy to be definitely applied on the L2TP connection. <p>SSL Tunnel - Allow the remote dial-in user to make an SSL</p>

	<p>VPN connection through Internet.</p> <p>Specify Remote Node -You can specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode).</p> <p>Uncheck the checkbox means the connection type you select above will apply the authentication methods and security methods in the general settings.</p> <p>Netbios Naming Packet -</p> <ul style="list-style-type: none"> ● Pass - Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. ● Block - When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel. <p>Multicast via VPN - Some programs might send multicast packets via VPN connection.</p> <ul style="list-style-type: none"> ● Pass - Click this button to let multicast packets pass through the router. ● Block - This is default setting. Click this button to let multicast packets be blocked by the router. <p>User Name - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 23 characters.</p> <p>Password - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 19 characters.</p> <p>Enable Mobile One-Time Passwords (mOTP) - Check this box to make the authentication with mOTP function.</p> <p>PIN Code - Type the code for authentication (e.g., 1234).</p> <p>Secret - Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).</p>
Subnet	<p>Chose one of the subnet selections for such VPN profile.</p> <p>Assign Static IP Address - Please type a static IP address for the subnet you specified.</p>
IKE Authentication Method	<p>This group of fields is applicable for IPsec Tunnels and L2TP with IPsec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPsec tunnel either with or without specifying the IP address of the remote node.</p> <p>Pre-Shared Key - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key.</p> <p>Digital Signature (X.509) - Check the box of Digital Signature to invoke this function and Select one predefined Profiles set in the VPN and Remote Access >>IPsec Peer Identity.</p>
IPsec Security Method	<p>This group of fields is a must for IPsec Tunnels and L2TP with IPsec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method.</p> <p>Medium-Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it.</p> <p>High-Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select</p>

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.

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

VPN and Remote Access >> LAN to LAN ?

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

View: All Trunk

Index	Name	Active	Status	Index	Name	Active	Status
1.	???	<input type="checkbox"/>	---	17.	???	<input type="checkbox"/>	---
2.	???	<input type="checkbox"/>	---	18.	???	<input type="checkbox"/>	---
3.	???	<input type="checkbox"/>	---	19.	???	<input type="checkbox"/>	---
4.	???	<input type="checkbox"/>	---	20.	???	<input type="checkbox"/>	---
5.	???	<input type="checkbox"/>	---	21.	???	<input type="checkbox"/>	---
6.	???	<input type="checkbox"/>	---	22.	???	<input type="checkbox"/>	---
7.	???	<input type="checkbox"/>	---	23.	???	<input type="checkbox"/>	---
8.	???	<input type="checkbox"/>	---	24.	???	<input type="checkbox"/>	---
9.	???	<input type="checkbox"/>	---	25.	???	<input type="checkbox"/>	---
10.	???	<input type="checkbox"/>	---	26.	???	<input type="checkbox"/>	---
11.	???	<input type="checkbox"/>	---	27.	???	<input type="checkbox"/>	---
12.	???	<input type="checkbox"/>	---	28.	???	<input type="checkbox"/>	---
13.	???	<input type="checkbox"/>	---	29.	???	<input type="checkbox"/>	---
14.	???	<input type="checkbox"/>	---	30.	???	<input type="checkbox"/>	---
15.	???	<input type="checkbox"/>	---	31.	???	<input type="checkbox"/>	---
16.	???	<input type="checkbox"/>	---	32.	???	<input type="checkbox"/>	---

[XXXXXX:This Dial-out profile has already joined for VPN 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.

VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles:

View: All Trunk

Name	Activate	Members	Status
Loadbalan1	v	VPN-2	Offline
		Connection	Offline

[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:

VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles:

View: All Trunk

Name	Activate	Members	Status

OK

Cancel

[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]

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 <input type="text" value="???"/> <input type="checkbox"/> Enable this profile	Call Direction <input checked="" type="radio"/> Both <input type="radio"/> Dial-Out <input type="radio"/> Dial-in Tunnel Mode <input type="radio"/> GRE Tunnel <input type="checkbox"/> Always on Idle Timeout <input type="text" value="300"/> second(s) <input type="checkbox"/> Enable PING to keep IPsec tunnel alive PING to the IP <input type="text"/>
VPN Dial-Out Through <input type="text" value="WAN1 First"/>	
Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay...etc.)	

2. Dial-Out Settings

Type of Server I am calling <input checked="" type="radio"/> PPTP <input type="radio"/> IPsec Tunnel <input type="text" value="IKEv1"/> <input type="radio"/> L2TP with IPsec Policy <input type="text" value="None"/> <input type="radio"/> SSL Tunnel	Username <input type="text" value="???"/> Password(Max 15 char) <input type="text"/> PPP Authentication <input type="text" value="PAP/CHAP/MS-CHAP/MS-CHAPv2"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <input type="text"/> Server Port (for SSL Tunnel): <input type="text" value="443"/>	IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key <input type="text" value="IKE Pre-Shared Key"/> <input type="radio"/> Digital Signature(X.509) Peer ID <input type="text" value="None"/> Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First Local Certificate <input type="text" value="None"/>
	IPsec Security Method <input type="radio"/> Medium(AH) <input checked="" type="radio"/> High(ESP) <input type="text" value="AES with Authentication"/> <input type="button" value="Advanced"/>
	Index(1-15) in Schedule Setup: <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>

Available settings are explained as follows:

Item	Description
Common Settings	<p>Profile Name - Specify a name for the profile of the LAN-to-LAN connection.</p> <p>Enable this profile - Check here to activate this profile.</p> <p>VPN Dial-Out Through - Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only.</p> <ul style="list-style-type: none"> ● WAN1 First/ WAN2 First/ WAN3 First /WAN4 First- While connecting, the router will use WAN1/WAN2/WAN3/WAN4 as the first channel for VPN connection. If WAN1/WAN2/WAN3/WAN4 fails, the router will use another WAN interface instead. ● WAN1 Only /WAN2 Only/WAN 3 Only/WAN 4 Only- While connecting, the router will use WAN1/WAN2/WAN3/WAN4 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

	<p>connection.</p> <ul style="list-style-type: none"> ● WAN2 Only: Only establish VPN if WAN1 down - If WAN1 failed, the router will use WAN2 for VPN connection. <p>Netbios Naming Packet</p> <ul style="list-style-type: none"> ● Pass - click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. ● Block - When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel. <p>Multicast via VPN - Some programs might send multicast packets via VPN connection.</p> <ul style="list-style-type: none"> ● Pass - Click this button to let multicast packets pass through the router. ● Block - This is default setting. Click this button to let multicast packets be blocked by the router. <p>Call Direction - Specify the allowed call direction of this LAN-to-LAN profile.</p> <ul style="list-style-type: none"> ● Both: -initiator/responder ● Dial-Out- initiator only ● Dial-In- responder only. <p>Tunnel Mode - At present, a tunnel (GRE tunnel) without encryption is offered to fit the requirement of specific client.</p> <p>Always On-Check to enable router always keep VPN connection.</p> <p>Idle Timeout: The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.</p> <p>Enable PING to keep alive - This function is to help the router to determine the status of IPsec VPN connection, especially useful in the case of abnormal VPN IPsec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address.</p> <p>Enable PING to keep alive is used to handle abnormal IPsec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial. Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer disconnects without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection).</p> <p>PING to the IP - Enter the IP address of the remote host that located at the other-end of the VPN tunnel.</p>
Dial-Out Settings	<p>Type of Server I am calling - PPTP - Build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server.</p>

IPsec Tunnel - Build an IPsec VPN connection to the server through Internet.

L2TP with IPsec Policy - Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below:

- **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 advanced settings

Main mode Aggressive mode

IKE phase 1 mode: Auto

IKE phase 1 proposal: HMAC_SHA1/HMAC_MD5

IKE phase 2 proposal: (900 - 86400)

IKE phase 1 key lifetime: 28800 (900 - 86400)

IKE phase 2 key lifetime: 3600 (600 - 86400)

Perfect Forward Secret: Disable Enable

Local ID:

Note: If you select "Auto" in IKE phase 1 proposal, the router will send the following proposals to negotiate with the remote site. The proposals include: DES_(MD5|SHA)_G1, 3DES_MD5_G1, 3DES_MD5_G2, 3DES_(MD5|SHA)_G5, AES128_MD5_(G2|G5), AES256_SHA_(G2|G5), AES256_SHA_G14

OK Close

IKE phase 1 mode -Select from **Main mode** and **Aggressive mode**. The ultimate outcome is to exchange security proposals to create a protected secure channel. **Main mode** is more secure than **Aggressive mode** since more exchanges are done in a secure channel to set up the IPsec session. However, the **Aggressive mode** is faster. The default value in Vigor router is **Main mode**.

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

Local ID-In **Aggressive mode**, Local ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters.

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

<p>Allowed Dial-In Type</p> <p><input checked="" type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> IPsec Tunnel</p> <p><input checked="" type="checkbox"/> L2TP with IPsec Policy None</p> <p><input checked="" type="checkbox"/> SSL Tunnel</p> <p><input type="checkbox"/> Specify Remote VPN Gateway</p> <p>Peer VPN Server IP <input style="width: 100px;" type="text"/></p> <p>or Peer ID <input style="width: 100px;" type="text"/></p>	<p>Username <input data-bbox="1150 226 1362 255" style="width: 100px;" type="text" value="???"/></p> <p>Password(Max 11 char) <input data-bbox="1150 271 1362 300" style="width: 100px;" type="text"/></p> <p>VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off</p> <hr/> <p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p>IKE Pre-Shared Key <input data-bbox="1150 421 1362 450" style="width: 100px;" type="text"/></p> <p><input type="checkbox"/> Digital Signature(X.509)</p> <p>None</p> <p>Local ID</p> <p><input checked="" type="radio"/> Alternative Subject Name First</p> <p><input type="radio"/> Subject Name First</p> <hr/> <p>IPsec Security Method</p> <p><input checked="" type="checkbox"/> Medium(AH)</p> <p>High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p>
--	---

4. GRE Settings

<input type="checkbox"/> Enable IPsec Dial-Out function GRE over IPsec		
<input type="checkbox"/> Logical Traffic	My GRE IP <input style="width: 100px;" type="text"/>	Peer GRE IP <input style="width: 100px;" type="text"/>

5. TCP/IP Network Settings

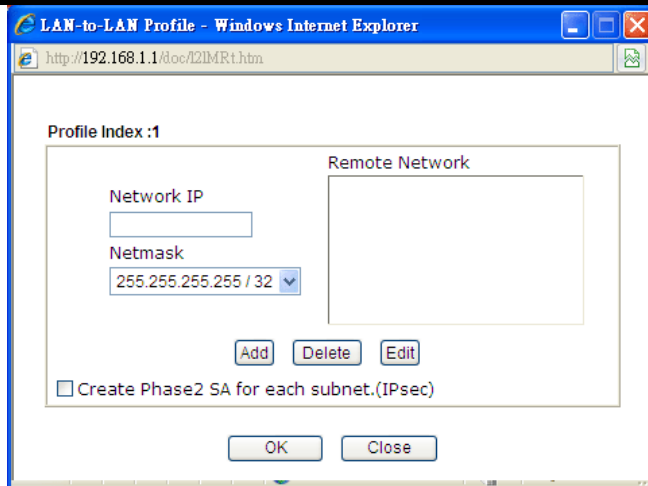
<p>My WAN IP <input style="width: 100px;" type="text" value="0.0.0.0"/></p> <p>Remote Gateway IP <input style="width: 100px;" type="text" value="0.0.0.0"/></p> <p>Remote Network IP <input style="width: 100px;" type="text" value="0.0.0.0"/></p> <p>Remote Network Mask <input style="width: 100px;" type="text" value="255.255.255.0"/></p> <p>Local Network IP <input style="width: 100px;" type="text" value="192.168.1.1"/></p> <p>Local Network Mask <input style="width: 100px;" type="text" value="255.255.255.0"/></p> <p style="text-align: center;"><input type="button" value="More"/></p>	<p>RIP Direction Disable</p> <p>From first subnet to remote network, you have to do Route</p> <p><input type="checkbox"/> IPsec VPN with the Same Subnets</p> <hr/> <p><input type="checkbox"/> Change default route to this VPN tunnel (Only active if one single WAN is up)</p>
--	---

Available settings are explained as follows:

Item	Description
Dial-In Settings	<p>Allowed Dial-In Type - Determine the dial-in connection with different types.</p> <ul style="list-style-type: none"> ● PPTP - Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below. ● IPsec Tunnel- Allow the remote dial-in user to trigger an IPsec VPN connection through Internet. ● L2TP with IPsec Policy - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below: <ul style="list-style-type: none"> ■ None - Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection. ■ Nice to Have - Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. ■ Must - Specify the IPsec policy to be definitely

	<p>applied on the L2TP connection.</p> <ul style="list-style-type: none"> ● SSL Tunnel- Allow the remote dial-in user to trigger an SSL VPN connection through Internet. <p>Specify Remote VPN Gateway - You can specify the IP address of the remote dial-in user or peer ID (should be the same with the ID setting in dial-in type) by checking the box. Also, you should further specify the corresponding security methods on the right side.</p> <p>If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings.</p> <p>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.</p> <p>Password - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 11 characters.</p> <p>VJ Compression - VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select PPTP or L2TP with or without IPsec policy above.</p> <p>IKE Authentication Method - This group of fields is applicable for IPsec Tunnels and L2TP with IPsec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPsec tunnel either with or without specify the IP address of the remote node.</p> <ul style="list-style-type: none"> ● Pre-Shared Key - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key. ● Digital Signature (X.509) -Check the box of Digital Signature to invoke this function and select one predefined Profiles set in the VPN and Remote Access >>IPsec Peer Identity. <ul style="list-style-type: none"> ■ Local ID - Specify which one will be inspected first. ■ Alternative Subject Name First - The alternative subject name (configured in Certificate Management>>Local Certificate) will be inspected first. ■ Subject Name First - The subject name (configured in Certificate Management>>Local Certificate) will be inspected first. <p>IPsec Security Method - This group of fields is a must for IPsec Tunnels and L2TP with IPsec Policy when you specify the remote node.</p> <ul style="list-style-type: none"> ● Medium- Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active. ● High- Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
GRE over IPsec Settings	<p>Enable IPsec Dial-Out function GRE over IPsec: Check this box to verify data and transmit data in encryption with GRE over IPsec packet after configuring IPsec Dial-Out setting. Both ends must match for each other by setting same virtual</p>

	<p>IP address for communication.</p> <p>Logical Traffic: Such technique comes from RFC2890. Define logical traffic for data transmission between both sides of VPN tunnel by using the characteristic of GRE. Even hacker can decipher IPsec encryption, he/she still cannot ask LAN site to do data transmission with any information. Such function can ensure the data transmitted on VPN tunnel is really sent out from both sides. This is an optional function. However, if one side wants to use it, the peer must enable it, too.</p> <p>My GRE IP: Type the virtual IP for router itself for verified by peer.</p> <p>Peer GRE IP: Type the virtual IP of peer host for verified by router.</p>
<p>TCP/IP Network Settings</p>	<p>My WAN IP -This field is only applicable when you select PPTP or L2TP with or without IPsec policy above. The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.</p> <p>Remote Gateway IP - This field is only applicable when you select PPTP or L2TP with or without IPsec policy above. The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.</p> <p>Remote Network IP/ Remote Network Mask - Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPsec, this is the destination clients IDs of phase 2 quick mode.</p> <p>Local Network IP / Local Network Mask - Display the local network IP and mask for TCP / IP configuration. You can modify the settings if required.</p> <p>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.</p>



RIP Direction - The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable.

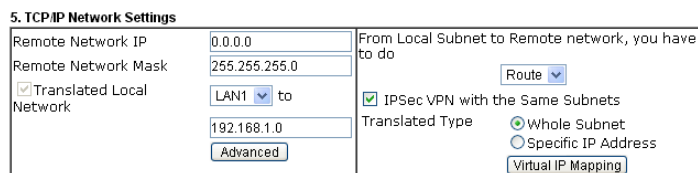
From first subnet to remote network, you have to do - If the remote network only allows you to dial in with single IP, please choose **NAT**, otherwise choose **Route**.

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.

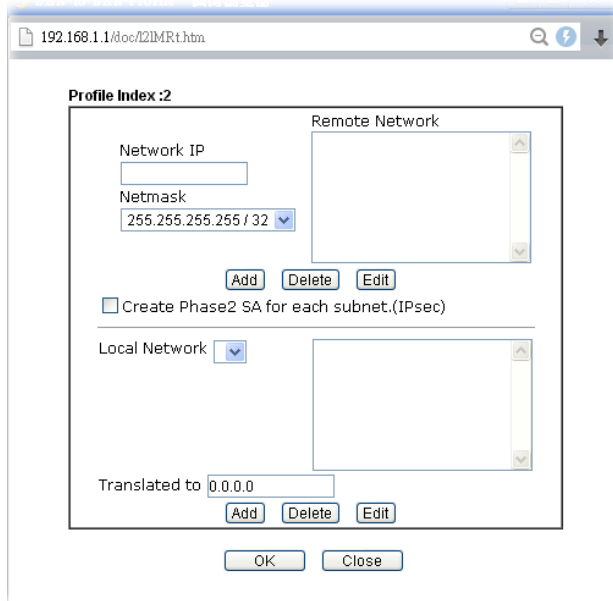
After checking the box of **IPSec VPN with the Same subnet**, the options under **TCP/IP Network Settings** will be changed as shown below:



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.

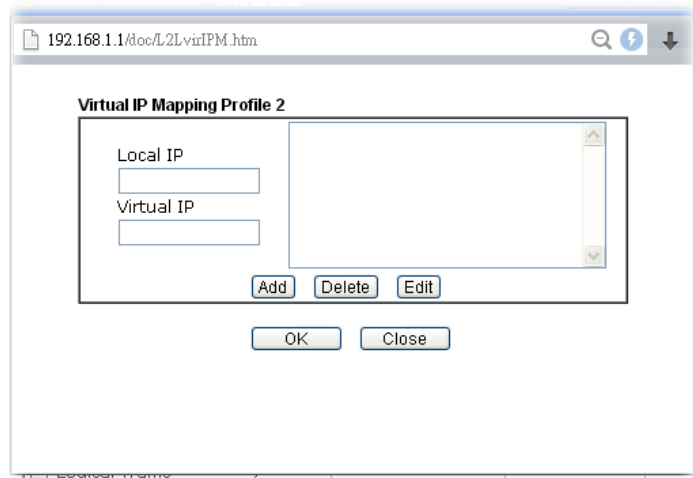
Advanced - Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.



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.

IV-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



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

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

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

Advanced

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

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

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

Advanced

General Setup

Status Enable Disable

Profile Name

Member1

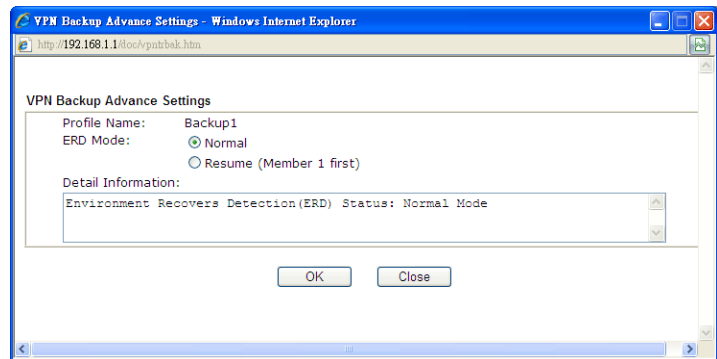
Member2

Active Mode Backup Load Balance

Available settings are explained as follows:

Item	Description
Backup Profile List	<p>Set to Factory Default - Click to clear all VPN TRUNK-VPN Backup mechanism profile.</p> <p>No. - The order of VPN TRUNK-VPN Backup mechanism profile.</p> <p>Status - "v" means such profile is enabled; "x" means such profile is disabled.</p> <p>Name - Display the name of VPN TRUNK-VPN Backup mechanism profile.</p> <p>Member1 - Display the dial-out profile selected from the Member1 drop down list below.</p> <p>Active - "Yes" means normal condition. "No" means the state might be disabled or that profile currently is set with Dial-in mode (for call direction) in LAN-to-LAN.</p> <p>Type - Display the connection type for that profile, such as IPsec, PPTP, L2TP, L2TP over IPsec (NICE), L2TP over IPsec(MUST) and so on.</p> <p>Member2 - Display the dial-out profile selected from the Member2 drop down list below.</p>

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.

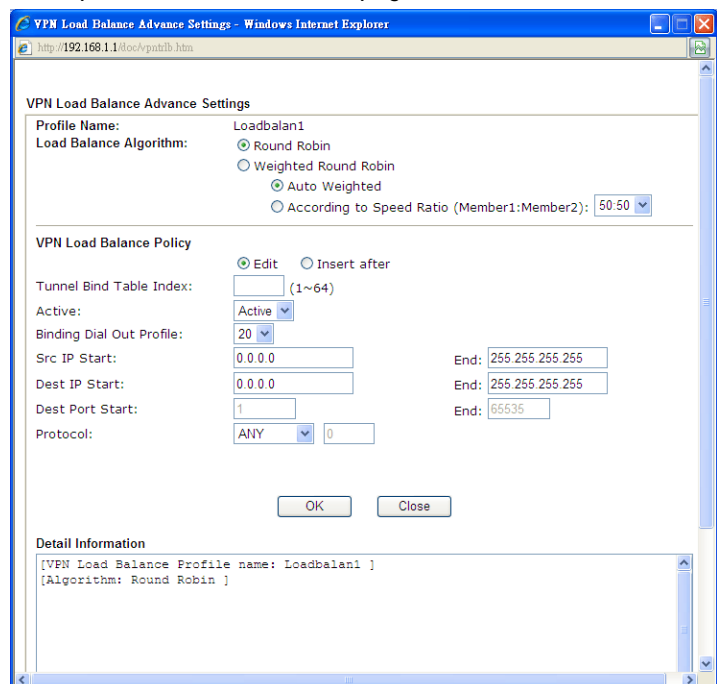
Member1 - Display the dial-out profile selected from the Member1 drop down list below.

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	<p>Status- After choosing one of the profile listed above, please click Enable to activate this profile. If you click Disable, the selected or current used VPN TRUNK-Backup/Load Balance mechanism profile will not have any effect for VPN tunnel.</p> <p>Profile Name- Type a name for VPN TRUNK profile. Each profile can group two VPN connections set in LAN-to-LAN. The saved VPN profiles in LAN-to-LAN will be shown on Member1 and Member2 fields. The length of the name is limited to 11 characters.</p> <p>Member 1/Member2 - Display the selection for LAN-to-LAN dial-out profiles (configured in VPN and Remote Access >> LAN-to-LAN) for you to choose for grouping under certain VPN TRUNK-VPN Backup/Load Balance mechanism profile.</p> <ul style="list-style-type: none"> ● 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. <p>Active Mode - Display available mode for you to choose. Choose Backup or Load Balance for your router.</p> <p>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.</p> <p>Update - Click this button to save the changes to the Status (Enable or Disable), profile name, member1 or member2.</p> <p>Delete - Click this button to delete the selected VPN TRUNK profile. The corresponding members (LAN-to-LAN profiles) grouped in the deleted VPN TRUNK profile will be released and that profiles in LAN-to-LAN will be displayed in black.</p>

Time for activating VPN TRUNK — VPN Backup mechanism profile

VPN TRUNK - VPN Backup mechanism will be activated automatically after the initial connection of single VPN Tunnel off-line. The content in Member1/2 within VPN TRUNK - VPN Backup mechanism backup profile is similar to dial-out profile configured in LAN-to-LAN web page. VPN TRUNK - VPN Backup mechanism backup profile will process and handle everything unless it is off-line once it is activated.

Time for activating VPN TRUNK — VPN Load Balance mechanism profile

After finishing the connection for one tunnel, the other tunnel will dial out automatically within two seconds. Therefore, you can choose any one of members under VPN Load Balance for dialing out.

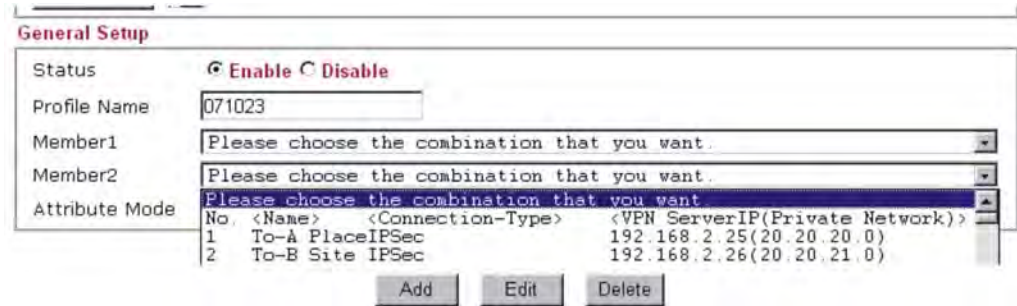
Time for activating VPN TRUNK — Dial-out when VPN Load Balance Disconnected

For there is one Tunnel created and connected successfully, to keep the load balance effect between two tunnels, auto-dial will be executed within two seconds.

To close two tunnels of load balance after connecting, please click **Disable** for **Status** in **General Setup** field.

How can you set a VPN TRUNK-VPN Backup/Load Balance mechanism profile?

1. First of all, go to **VPN and Remote Access>>LAN-to-LAN**. Set two or more LAN-to-LAN profiles first that will be used for Member1 and Member2. If you do not set enough LAN-to-LAN profiles, you cannot operate VPN TRUNK - VPN Backup /Load Balance mechanism profile management well.
2. Access into **VPN and Remote Access>>VPN TRUNK Management**.
3. Set one group of VPN TRUNK - VPN Backup/Load Balance mechanism backup profile by choosing **Enable** radio button; type a name for such profile (e.g., 071023); choose one of the LAN-to-LAN profiles from Member1 drop down list; choose one of the LAN-to-LAN profiles from Member2 drop down list; and click **Add** at last.



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:

View: All Trunk

Index	Name	Active	Status
<u>1.</u>	To-A Place	V	offline
<u>2.</u>	To-B Site	V	offline
<u>3.</u>	To-C Place	V	offline
<u>4.</u>	To-D Site	V	offline
5.	???	X	---

How can you set a GRE over IPsec profile?

1. Please go to LAN to LAN to set a profile with IPsec.
2. If the router will be used as the VPN Server (i.e., with virtual address 192.168.50.200). Please type 192.168.50.200 in the field of My GRE IP. Type IP address (192.168.50.100) of the client in the field of Peer GRE IP. See the following graphic for an example.

4. GRE Settings

Enable IPsec Dial-Out function GRE over IPsec

Logical Traffic

My GRE IP Peer GRE IP

5. TCP/IP Network Settings

My WAN IP

Remote Gateway IP

Remote Network IP

Remote Network Mask

Local Network IP

Local Network Mask

RIP Direction

From first subnet to remote network, you have to do

IPsec VPN with the Same Subnets

Change default route to this VPN tunnel (Only active if one single WAN is up)

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.

4. GRE Settings

Enable IPsec Dial-Out function GRE over IPsec

Logical Traffic

My GRE IP Peer GRE IP

5. TCP/IP Network Settings

My WAN IP

Remote Gateway IP

Remote Network IP

Remote Network Mask

Local Network IP

Local Network Mask

RIP Direction

From first subnet to remote network, you have to do

IPsec VPN with the Same Subnets

Change default route to this VPN tunnel (Only active if one single WAN is up)

Advanced Load Balance and Backup

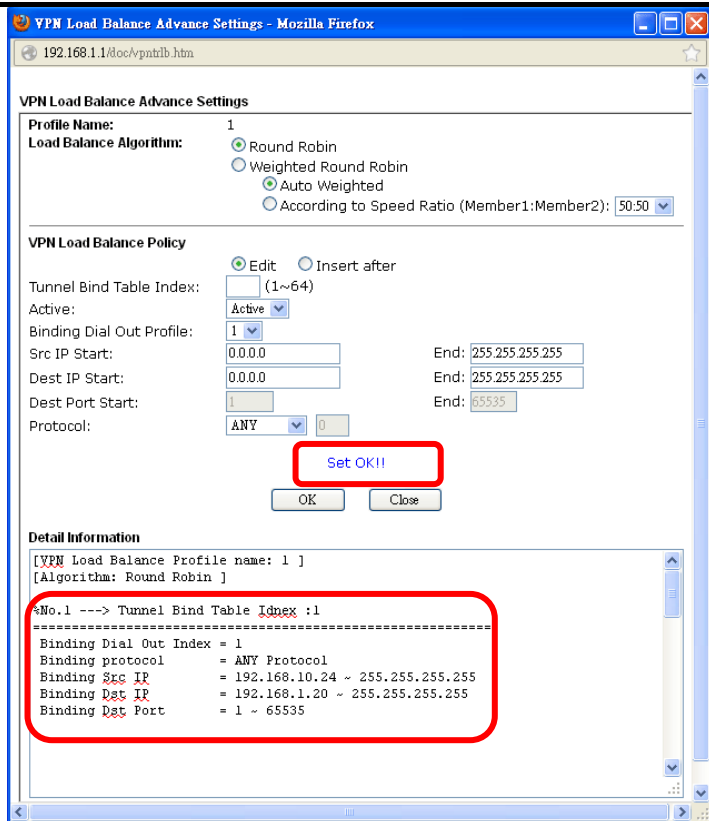
After setting profiles for load balance, you can choose any one of them and click Advance for more detailed configuration. The windows for advanced load balance and backup are different. Refer to the following explanation:

Advanced Load Balance

Available settings are explained as follows:

Item	Description
Profile Name	List the load balance profile name.
Load Balance Algorithm	<p>Round Robin - Based on packet base, both tunnels will send the packet alternatively. Such method can reach the balance of packet transmission with fixed rate.</p> <p>Weighted Round Robin -Such method can reach the balance of packet transmission with flexible rate. It can be divided into Auto Weighted and According to Speed Ratio. Auto Weighted can detect the device speed (10Mbps/100Mbps) and switch with fixed value ratio (3:7) for packet transmission. If the transmission rate for packets on both sides of the tunnels is the same, the value of Auto Weighted should be 5.5. According to Speed Ratio allows user to adjust suitable rate manually. There are 100 groups of rate ratio for Member1:Member2 (range from 1:99 to 99:1).</p>
VPN Load Balance Policy	<p>Below shows the algorithm for Load Balance.</p> <p>Edit - Click this radio button for assign a blank table for configuring Binding Tunnel.</p> <p>Insert after - Click this radio button to adding a new binding tunnel table.</p>

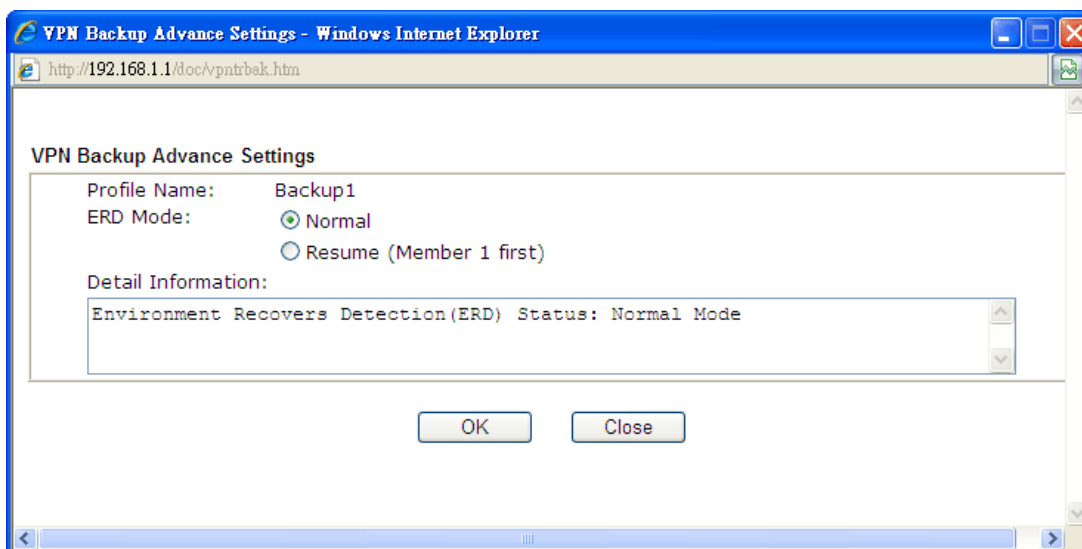
	<p>Tunnel Bind Table Index- 128 Binding tunnel tables are provided by this device. Specify the number of the tunnel for such Load Balance profile.</p> <p>Active - In-active/Delete can delete this binding tunnel table. Active can activate this binding tunnel table.</p> <p>Binding Dial Out Index - Specify connection type for transmission by choosing the index (LAN to LAN Profile Index) for such binding tunnel table.</p> <p>Scr IP Start /End- Specify source IP addresses as starting point and ending point.</p> <p>Dest IP Start/End - Specify destination IP addresses as starting point and ending point.</p> <p>Dest Port Start /End- Specify destination service port as starting point and ending point.</p> <p>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.</p> <p>TCP means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and TCP Service Port also fits the number here, such binding tunnel table can be established. UDP means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and UDP Service Port also fits the number here, such binding tunnel table can be established. TCP/UDP means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and TCP/UDP Service Port also fits the number here, such binding tunnel table can be established. ICMP means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and ICMP Service Port also fits the number here, such binding tunnel table can be established. IGMP means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and IGMP Service Port also fits the number here, such binding tunnel table can be established. Other means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here with different TCP Service Port/UDP Service Port/ICMP/IGMP, such binding tunnel table can be established.</p>
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



Available settings are explained as follows:

Item	Description
Profile Name	List the backup profile name.
ERD Mode	ERD means "Environment Recovers Detection". Normal - choose this mode to make all dial-out VPN TRUNK

	backup profiles being activated alternatively. Resume - when VPN connection breaks down or disconnects, 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.

IV-1-10 Connection Management

You can find the summary table of all VPN connections. You may disconnect any VPN connection by clicking **Drop** button. You may also aggressively Dial-out by using Dial-out Tool and clicking **Dial** button.

VPN and Remote Access >> Connection Management

Dial-out Tool

General Mode:	<input type="text" value=""/>	<input type="button" value="Dial"/>
Backup Mode:	<input type="text" value=""/>	<input type="button" value="Dial"/>
Load Balance Mode:	<input type="text" value=""/>	<input type="button" value="Dial"/>

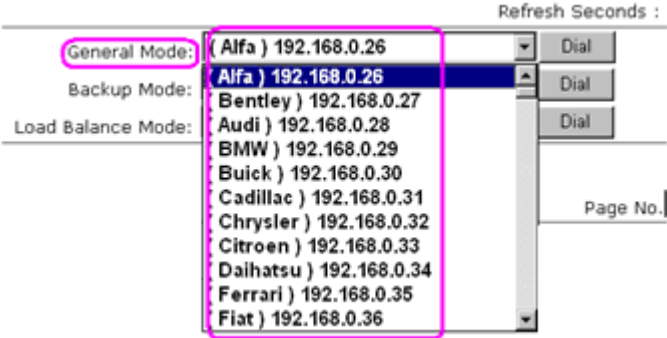
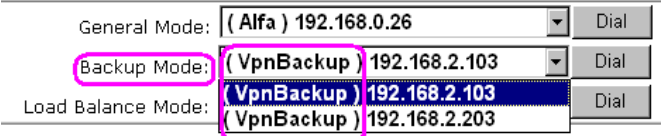
VPN Connection Status

LAN-to-LAN VPN Status			Remote Dial-in User Status					
VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(bps)	Rx Pkts	Rx Rate(bps)	UpTime

xxxxxxxx : Data is encrypted.

xxxxxxxx : Data isn't encrypted.

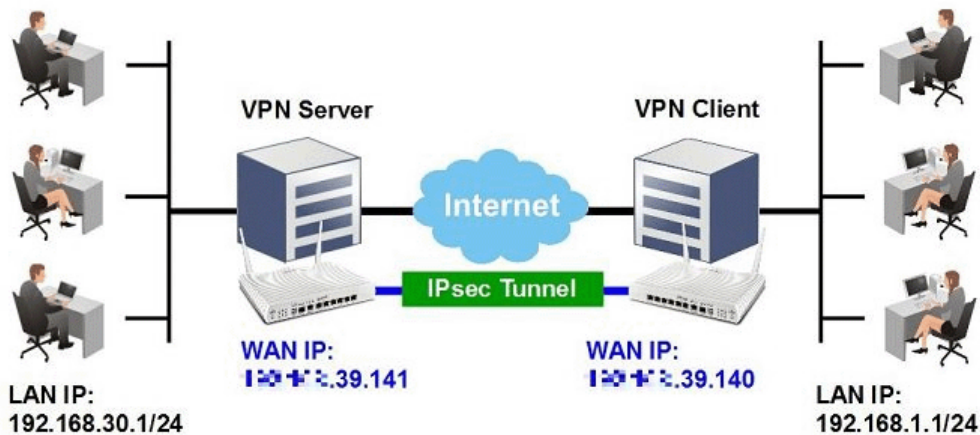
Available settings are explained as follows:

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

Application Notes

A-1 How to Build a LAN-to-LAN VPN Between Vigor Routers via IPsec Main Mode

This document introduces how to set up Main mode IPsec Tunnel between two Vigor Routers. IPsec VPN with Main mode use the IP address of VPN client as identifier, and the IP address must be set on VPN server; therefore, if the VPN client doesn't have a static IP, please use Aggressive mode instead.



VPN Server (Dial-In Site) Setup

1. Create a Dial-In profile for VPN user, go to **VPN and Remote Access >> LAN to LAN**, click on an available index to add a new profile.

VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles:

[Set to Factory Default](#)

View: All Trunk

Index	Name	Active	Status	Index	Name	Active	Status
1.	???	<input type="checkbox"/>	---	17.	???	<input type="checkbox"/>	---
2.	???	<input type="checkbox"/>	---	18.	???	<input type="checkbox"/>	---
3.	???	<input type="checkbox"/>	---	19.	???	<input type="checkbox"/>	---
4.	???	<input type="checkbox"/>	---	20.	???	<input type="checkbox"/>	---

2. Set up the dial-in profile.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="Host"/>	Call Direction <input type="radio"/> Both <input type="radio"/> Dial-Out <input checked="" type="radio"/> Dial-in
<input checked="" type="checkbox"/> Enable this profile	<input type="checkbox"/> Always on
VPN Dial-Out Through WAN1 First	Idle Timeout <input type="text" value="300"/> second(s)
Netbios Naming Packet <input type="radio"/> Pass <input type="radio"/> Block	<input type="checkbox"/> Enable PING to keep IPsec tunnel alive
Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block	PING to the IP <input type="text"/>
(for some IGMP,IP-Camera,DHCP Relay..etc.)	

In Common Settings,

- (a) Enter the **Profile Name**.
- (b) Enable this profile.
- (c) Set **Call Direction** to **Dial-in**.

In Dial-In Setting,

3. Dial-In Settings

Allowed Dial-In Type <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input type="checkbox"/> L2TP with IPsec Policy None ▼ <input type="checkbox"/> SSL Tunnel	Username <input type="text" value="???"/> Password(Max 11 char) <input type="text"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
<input checked="" type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text" value="39.140"/> or Peer ID <input type="text"/>	IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="text" value="....."/> <input type="checkbox"/> Digital Signature(X.509) None ▼ Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First
	IPsec Security Method <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES

IKE Authentication Method

Pre-Shared Key <input type="text" value="....."/>
Confirm Pre-Shared Key <input type="text" value="....."/>

- (d) Make sure Allowed Dial-in Type has **IPsec Tunnel** enabled.
 - (e) Enable **Specify Remote VPN Gateway** and enter **Peer VPN Server IP** as the public IP of VPN client router.
 - (f) Click on **IKE Pre-Shared Key** and enter the Pre-shared Key.
 - (g) Select the **IPsec Security Method** that are allowed to use.
3. In **TCP/IP Network Settings**, enter VPN Client's LAN network in **Remote Network IP** and **Remote Network Mask**. Click **OK** to save the profile.

5. TCP/IP Network Settings

My WAN IP	<input type="text" value="0.0.0.0"/>	RIP Direction	Disable ▼
Remote Gateway IP	<input type="text" value="0.0.0.0"/>	From first subnet to remote network, you have to do	<input type="text"/>
Remote Network IP	<input type="text" value="192.168.1.1"/>		Route ▼
Remote Network Mask	<input type="text" value="255.255.255.0"/>	<input type="checkbox"/> IPsec VPN with the Same Subnets	
Local Network IP	<input type="text" value="192.168.30.1"/>	<input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)	
Local Network Mask	<input type="text" value="255.255.255.0"/>		

VPN Client (Dial-out Site) Setup

1. Create a Dial-out profile to VPN server: Go to VPN and Remote Access >> LAN to LAN, click on an available index to add a new profile.

VPN and Remote Access >> LAN to LAN ?

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

View: All Trunk

Index	Name	Active	Status	Index	Name	Active	Status
1.	???	<input type="checkbox"/>	---	17.	???	<input type="checkbox"/>	---
2.	???	<input type="checkbox"/>	---	18.	???	<input type="checkbox"/>	---
3.	???	<input type="checkbox"/>	---	19.	???	<input type="checkbox"/>	---

2. Setup the dial-out profile.

In Common Settings,

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="Client"/>	Call Direction <input type="radio"/> Both <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-in
<input checked="" type="checkbox"/> Enable this profile	<input type="checkbox"/> Always on
VPN Dial-Out Through <input type="text" value="WAN1 First"/>	Idle Timeout <input type="text" value="300"/> second(s)
Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block	<input type="checkbox"/> Enable PING to keep IPsec tunnel alive
Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block <small>(for some IGMP,IP-Camera,DHCP Relay..etc.)</small>	PING to the IP <input type="text"/>

- (a) Enter a Profile Name.
- (b) Enable this profile.
- (c) Set Call Direction to Dial-Out.

In Dial-out Setting,

2. Dial-Out Settings

- (d) Select **IPsec Tunnel** for **Type of Sever I am Calling**.
- (e) Enter VPN Server's WAN IP or domain name in **Sever IP/Host Name for VPN**.
- (f) Click **IKE Pre-Shared Key** and enter the same Pre-Shared key as VPN Server.
- (g) Click on **Advanced** in **IPsec Security Method**.

In IKE advanced settings,

- (h) Select **Main Mode** for **IKE phase 1 mode**.
 - (i) Make sure phase 1 and phase 2 proposal are using the security methods which are accepted by VPN server.
 - (j) Click **OK** to save.
3. In **TCP/IP Network Settings**, enter VPN Server's LAN Network in **Remote Network IP** and **Remote Network Mask**. Click **OK** to save the profile.

5. TCP/IP Network Settings

My WAN IP	0.0.0.0	RIP Direction	Disable ▾
Remote Gateway IP	0.0.0.0	From first subnet to remote network, you have to do	
Remote Network IP	192.168.30.1	Route ▾	
Remote Network Mask	255.255.255.0	<input type="checkbox"/> IPsec VPN with the Same Subnets	
Local Network IP	192.168.1.1	<input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)	
Local Network Mask	255.255.255.0		
	<input type="button" value="More"/>		

VPN Tunnel Establishment

To initiate the VPN connection, go to **VPN and Remote Access >> Connection Management** on VPN Client. Select the profile to VPN Sever and click **Dial**.

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds : 10 ▾

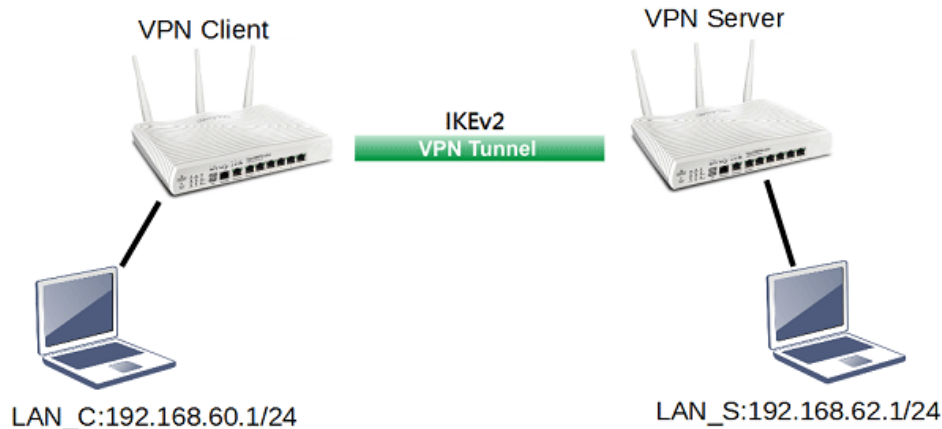
General Mode:	(Client) .39.141 ▾	<input type="button" value="Dial"/>
Backup Mode:	▾	<input type="button" value="Dial"/>
Load Balance Mode:	▾	<input type="button" value="Dial"/>

If all the settings are matched, the VPN will be established, and the statistics will be displayed on the same page.

A-2 How to Build a LAN-to-LAN VPN Between Vigor Routers via IKEv2

Modified from the previous version IKEv1, IKEv2 is a new VPN protocol and has lots of improvements then the former. It is more stable, more secure and faster connection establishing speed. Support newer and more complicated secure ciphers to make the connection more secure. Using new connection progress and discard the PPP, IKEv2 provides the faster establishing speed.

This application note demonstrates how to establish IKEv2 VPN connection between two Vigor Routers by the following topology.



VPN Server Settings

1. Go to VPN and Remote Access >> IPsec General Setup.

VPN and Remote Access >> IPsec General Setup

VPN IKE/IPsec General Setup

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

IKE Authentication Method	
Certificate for Dial-in	None ▼
Pre-Shared Key	
Pre-Shared Key
Confirm Pre-Shared Key
IPsec Security Method	
<input checked="" type="checkbox"/> Medium (AH)	Data will be authentic, but will not be encrypted.
High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES	Data will be encrypted and authentic.

OK Cancel

- (a) Input Pre-shared Key and Confirm Pre-Shared Key.
 - (b) Click OK.
2. Go to VPN and Remote Access >> LAN to LAN and click an available index.

Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="Server"/> <input checked="" type="checkbox"/> Enable this profile <hr/> VPN Dial-Out Through <input type="text" value="WAN1 First"/> Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	Call Direction <input type="radio"/> Both <input type="radio"/> Dial-Out <input checked="" type="radio"/> Dial-in Tunnel Mode <input type="radio"/> GRE Tunnel <input type="checkbox"/> Always on Idle Timeout <input type="text" value="0"/> second(s) <input type="checkbox"/> Enable PING to keep IPsec tunnel alive PING to the IP <input type="text"/>
--	--

- (a) Check Enable this profile.
- (b) Select Dial-in as Call Direction.
- (c) Allow IPsec Tunnel in Dial-In Settings.
- (d) Input the IP address of LAN_C as Remote Network IP and Remote Network Mask.
- (e) Click OK.

VPN Client Settings

1. Go to VPN and Remote Access >> LAN to LAN and click an available index.

1. Common Settings

Profile Name <input type="text" value="Client"/> <input checked="" type="checkbox"/> Enable this profile <hr/> VPN Dial-Out Through <input type="text" value="WAN1 First"/> Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	Call Direction <input type="radio"/> Both <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-in Tunnel Mode <input type="radio"/> GRE Tunnel <input type="checkbox"/> Always on Idle Timeout <input type="text" value="0"/> second(s) <input type="checkbox"/> Enable PING to keep IPsec tunnel alive PING to the IP <input type="text"/>
--	--

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> PPTP <input checked="" type="radio"/> IPsec Tunnel <input type="text" value="IKEv2"/> <input type="radio"/> L2TP with IPsec Policy <input type="text" value="None"/> <input type="radio"/> SSL Tunnel	Username <input type="text" value="???"/> Password(Max 15 char) <input type="text"/> PPP Authentication <input type="text" value="PAP/CHAP/MS-CHAP/MS-CHAPv2"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <input type="text" value="ikev2.server.net"/> Server Port (for SSL Tunnel): <input type="text" value="443"/>	IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key <input type="text" value="....."/> <input type="radio"/> Digital Signature(X.509) Peer ID <input type="text" value="None"/> Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First Local Certificate <input type="text" value="None"/>
IPsec Security Method <input type="radio"/> Medium(AH) <input checked="" type="radio"/> High(ESP) <input type="text" value="AES with Authentication"/> <input type="button" value="Advanced"/>	
Index(1-15) in <u>Schedule</u> Setup: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	

- (a) Give a Profile Name.
- (b) Check Enable this profile.
- (c) Select Dial-Out as Call Direction.
- (d) Select IPsec Tunnel with IKEv2 in Dial-Out Settings.

- (e) Input VPN server's WAN IP or domain name at Server IP/Host Name for VPN.
 - (f) Input Pre-Shared Key of VPN server.
2. In TCP/IP Network Settings, input the IP address of LAN_S as Remote Network IP and Remote Network Mask. Click OK to save the profile.

5. TCP/IP Network Settings

My WAN IP	0.0.0.0	RIP Direction	Disable
Remote Gateway IP	0.0.0.0	From first subnet to remote network, you have to do	
Remote Network IP	192.168.62.1	Route	
Remote Network Mask	255.255.255.0	<input type="checkbox"/> IPsec VPN with the Same Subnets	
Local Network IP	192.168.60.1	<input type="checkbox"/> Change default route to this VPN tunnel (Only active if one single WAN is up)	
Local Network Mask	255.255.255.0		
	More		

VPN Tunnel Establishment

To initiate the VPN connection, go to VPN and Remote Access >> Connection Management. Select the VPN profile and click Dial.

VPN and Remote Access >> Connection Management

Dial-out Tool

General Mode:	(Client) ikev2.server.net	Dial
Backup Mode:		Dial
Load Balance Mode:		Dial

After VPN is established successfully, the VPN connection status will be shown below.

VPN and Remote Access >> Connection Management

Dial-out Tool

General Mode:	(Client) ikev2.server.net	Dial
Backup Mode:		Dial
Load Balance Mode:		Dial

VPN Connection Status

LAN-to-LAN VPN Status			Remote Dial-in User Status					
VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Kbps)	Rx Pkts	Rx Rate(Kbps)	UpTime
1 (Client)	IKEv2 IPsec Tunnel AES-SHA1 Auth	192.168.29.29 via WAN2	192.168.62.1/24	8	35.26	9	35.26	0:0:59

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

IV-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.



Wireless LAN (5 GHz)
SSL VPN
General Setup
User Account
User Group
Online User Status
USB Application

Web User Interface

IV-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

Bind to WAN	<input checked="" type="checkbox"/> WAN1	<input checked="" type="checkbox"/> WAN2	<input checked="" type="checkbox"/> WAN3	<input checked="" type="checkbox"/> WAN4
Port	<input type="text" value="443"/>	(Default: 443)		
Server Certificate	<input type="text" value="self-signed"/>			<input type="button" value="v"/>

Note:

1. The settings will act on all SSL applications.
2. Please go to **System Maintenance >> Management** to enable SSLv3.0 .
3. Please go to **System Maintenance >> Self-Signed Certificate** to generate a new "self-signed" certificate.

Available settings are explained as follows:

Item	Description
Bind to WAN	Choose and check WAN interface(s) for SSL VPN tunnel establishment.
Port	Such port is set for SSL VPN server. It will not affect the HTTPS Port configuration set in System Maintenance>>Management . In general, the default setting is 443.
Server Certificate	When the client does not set any certificate, default certificate will be used for HTTPS and SSL VPN server. Choose any one of the user-defined certificates from the drop down list if users set several certificates previously. Otherwise, choose Self-signed to use the router's built-in default certificate. The default certificate can be used in SSL VPN server and HTTPS Web Proxy.

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

IV-2-2 User Account

With SSL VPN, Vigor2862 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, Vigor2862 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

Remote Access User Accounts:

[Set to Factory Default](#)

Index	User	Active	Status	Index	User	Active	Status
<u>1.</u>	???	<input type="checkbox"/>	---	<u>17.</u>	???	<input type="checkbox"/>	---
<u>2.</u>	???	<input type="checkbox"/>	---	<u>18.</u>	???	<input type="checkbox"/>	---
<u>3.</u>	???	<input type="checkbox"/>	---	<u>19.</u>	???	<input type="checkbox"/>	---
<u>4.</u>	???	<input type="checkbox"/>	---	<u>20.</u>	???	<input type="checkbox"/>	---
<u>5.</u>	???	<input type="checkbox"/>	---	<u>21.</u>	???	<input type="checkbox"/>	---
<u>6.</u>	???	<input type="checkbox"/>	---	<u>22.</u>	???	<input type="checkbox"/>	---
<u>7.</u>	???	<input type="checkbox"/>	---	<u>23.</u>	???	<input type="checkbox"/>	---
<u>8.</u>	???	<input type="checkbox"/>	---	<u>24.</u>	???	<input type="checkbox"/>	---
<u>9.</u>	???	<input type="checkbox"/>	---	<u>25.</u>	???	<input type="checkbox"/>	---
<u>10.</u>	???	<input type="checkbox"/>	---	<u>26.</u>	???	<input type="checkbox"/>	---
<u>11.</u>	???	<input type="checkbox"/>	---	<u>27.</u>	???	<input type="checkbox"/>	---
<u>12.</u>	???	<input type="checkbox"/>	---	<u>28.</u>	???	<input type="checkbox"/>	---
<u>13.</u>	???	<input type="checkbox"/>	---	<u>29.</u>	???	<input type="checkbox"/>	---
<u>14.</u>	???	<input type="checkbox"/>	---	<u>30.</u>	???	<input type="checkbox"/>	---
<u>15.</u>	???	<input type="checkbox"/>	---	<u>31.</u>	???	<input type="checkbox"/>	---
<u>16.</u>	???	<input type="checkbox"/>	---	<u>32.</u>	???	<input type="checkbox"/>	---

Note:

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

OK

Cancel

Click each index to edit one remote user profile.

SSL VPN >> Remote Dial-in User

Index No. 1

<p>User account and Authentication</p> <p><input type="checkbox"/> Enable this account</p> <p>Idle Timeout <input type="text" value="300"/> second(s)</p> <hr/> <p>Allowed Dial-In Type</p> <p><input checked="" type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> IPsec Tunnel</p> <p><input checked="" type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/></p> <p><input checked="" type="checkbox"/> SSL Tunnel</p> <p><input type="checkbox"/> Specify Remote Node</p> <p>Remote Client IP <input type="text"/></p> <p>or Peer ID <input type="text"/></p> <p>Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block</p> <p>Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block</p> <p>(for some IGMP,IP-Camera,DHCP Relay..etc.)</p> <hr/> <p>Subnet</p> <p><input type="text" value="LAN 1"/></p> <p><input type="checkbox"/> Assign Static IP Address</p> <p><input type="text" value="0.0.0.0"/></p>	<p>Username <input style="width: 100px;" type="text" value="???"/></p> <p>Password(Max 19 char) <input style="width: 100px;" type="text"/></p> <p><input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP)</p> <p>PIN Code <input style="width: 100px;" type="text"/></p> <p>Secret <input style="width: 100px;" type="text"/></p> <hr/> <p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p>IKE Pre-Shared Key <input style="width: 100px;" type="text"/></p> <p><input type="checkbox"/> Digital Signature(X.509)</p> <p><input type="text" value="None"/></p> <hr/> <p>IPsec Security Method</p> <p><input checked="" type="checkbox"/> Medium(AH)</p> <p>High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p> <p>Local ID (optional) <input style="width: 100px;" type="text"/></p>
---	--

Available settings are explained as follows:

Item	Description
<p>User account and Authentication</p>	<p>Enable this account - Check the box to enable this function.</p> <p>Idle Timeout- If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.</p> <p>User Name - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the name/password is limited to 23 characters.</p> <p>Password - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the name/password is limited to 19 characters.</p> <p>Enable Mobile One-Time Passwords (mOTP) - Check this box to make the authentication with mOTP function.</p> <p>PIN Code - Type the code for authentication (e.g, 1234).</p> <p>Secret - Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).</p>
<p>Allowed Dial-In Type</p>	<p>PPTP - Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.</p> <p>IPSec Tunnel - Allow the remote dial-in user to make an IPsec VPN connection through Internet.</p> <p>L2TP with IPsec Policy - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can</p>

Item	Description
	<p>select to use L2TP alone or with IPSec. Select from below:</p> <ul style="list-style-type: none"> ● None - Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. ● Nice to Have - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. ● Must -Specify the IPSec policy to be definitely applied on the L2TP connection. <p>SSL Tunnel - It allows the remote dial-in user to make an SSL VPN Tunnel connection through Internet, suitable for the application through network accessing (e.g., PPTP/L2TP/IPSec)</p> <p>If you check this box, the function of SSL Tunnel for this account will be activated immediately.</p> <p>Specify Remote Node - Check the checkbox to specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode). If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings.</p> <p>Netbios Naming Packet</p> <ul style="list-style-type: none"> ● Pass - Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. ● Block - When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel. <p>Multicast via VPN - Some programs might send multicast packets via VPN connection.</p> <ul style="list-style-type: none"> ● Pass - Click this button to let multicast packets pass through the router. ● Block - This is default setting. Click this button to let multicast packets be blocked by the router.
Subnet	<p>Chose one of the subnet selections for such VPN profile.</p> <p>Assign Static IP Address - Please type a static IP address for the subnet you specified.</p>
IKE Authentication Method	<p>This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node.</p> <p>Pre-Shared Key - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key.</p> <p>Digital Signature (X.509) - Check the box of Digital Signature to invoke this function and Select one predefined Profiles set in the VPN and Remote Access >>IPSec Peer Identity.</p>
IPSec Security Method	<p>This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method.</p> <p>Medium-Authentication Header (AH) means data will be</p>

Item	Description
	<p>authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it.</p> <p>High-Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.</p> <p>Local ID - Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.</p>

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

IV-2-3 User Group

There are 10 user group profiles which can be created for authentication by LDAP server. Such profiles will be used by applications such as User Management, VPN and etc.

SSL VPN >> User Group

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

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

Each item is explained as follows:

Item	Description
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. 1

Enable

Group Name

Authentication Methods

Local User DataBase

Available User Accounts	Selected User Accounts
<input type="text"/>	<input type="text"/>

RADIUS
 TACACS+
 LDAP / Active Directory

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable such profile.
Group Name	Type a name for such profile. The length of the name is limited to 23 characters.
Authentication Methods	<p>It can determine the authentication method used for such profile.</p> <p>Local User DataBase - The system will do the authentication by using the user defined account profiles (in VPN and Remote Access>>Remote Dial-In User). The enabled profiles will be listed in the Available User Account on the left box. To add a profile into a group, simply choose the one from the left box and click the >> button. It will be displayed in the Selected User Account on the right box. For detailed information about configuring the profile setting, refer to Objects Setting>>IP Group.</p> <p>RADIUS - The RADIUS server will do the authentication by using the username and password</p> <p>TACACS+ - The TACACS+ will do the authentication by using the username and password.</p> <p>LDAP / Active Directory - If it is checked, the LDAP / AD server will do the authentication by using the username, password, information stated on the selected profiles.</p> <p>If the above three options are enabled, the system will do the authentication based on them in sequence.</p>

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

IV-2-4 Online User Status

If you have finished the configuration of SSL Web Proxy (server), users can find out corresponding settings when they access into DrayTek SSL VPN portal interface.

The screenshot shows the DrayTek SSL VPN portal interface. At the top left is the DrayTek logo. Below it, the text "Provide SSL VPN" is visible. The interface has a navigation bar with "Home", "SSL Web Proxy", and "SSL Tunnel" tabs, and a "[logout]" link. On the left, an "INFO" box displays the user name "mike", IP address "(172.17.1.42)", and a welcome message. Below the info box, it says "Timeout after 5 minutes." with a "[Reset]" link. The main content area, titled "Main Page:", contains a message: "You have successfully logged in! You are given the following privileges:" followed by a list of two items: "SSL Web Proxy" and "SSL Tunnel". At the bottom right, there is a copyright notice: "Copyright © 2006, DrayTek Corp. All Rights Reserved."

Next, users can open **SSL VPN >> Online Status** to view logging status of SSL VPN.

SSL VPN >> Online User Status

Refresh Seconds :

Active User	Host IP	Time out(seconds)	Action
Kate	192.168.30.14	299	<input type="button" value="Drop"/>

Available settings are explained as follows:

Item	Description
Active User	Display current user who visits SSL VPN server.
Host IP	Display the IP address for the host.
Time out	Display the time remaining for logging out.
Action	You can click Drop to drop certain login user from the router's SSL Portal UI.

IV-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.



Web User Interface

IV-3-1 Local Certificate

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

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

Note:

1. Please setup the "System Maintenance >> **Time and Date**" correctly before signing the local certificate.
2. The Time Zone MUST be setup correctly!!

Available settings are explained as follows:

Item	Description
Generate	Click this button to open Generate Certificate Request window. Type in all the information that the window requests. Then click Generate again.
Import	Click this button to import a saved file as the certification information.
Refresh	Click this button to refresh the information listed below.
View	Click this button to view the detailed settings for certificate request.
Delete	Click this button to delete selected name with certification information.

GENERATE

Click this button to open **Generate Certificate Signing Request** window. Type in all the information that the window request such as certificate name (used for identifying different certificate), subject alternative name type and relational settings for subject name. Then click **GENERATE** again.

Generate Certificate Signing Request

Certificate Name	<input type="text"/>
Subject Alternative Name	
Type	IP Address <input type="button" value="v"/>
IP	<input type="text"/>
Subject Name	
Country (C)	<input type="text"/>
State (ST)	<input type="text"/>
Location (L)	<input type="text"/>
Organization (O)	<input type="text"/>
Organization Unit (OU)	<input type="text"/>
Common Name (CN)	<input type="text"/>
Email (E)	<input type="text"/>
Key Type	RSA <input type="button" value="v"/>
Key Size	1024 Bit <input type="button" value="v"/>
Algorithm	SHA-256 <input type="button" value="v"/>



Info

Please be noted that "Common Name" must be configured with router's WAN IP or domain name.

After clicking **GENERATE**, the generated information will be displayed on the window below:

X509 Local Certificate Configuration

Name	Subject	Status	Modify	
server	/C=TW/ST=Hsinchu/L=Hsinchu/O...	Requesting	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>

IMPORT

Vigor router allows you to generate a certificate request and submit it the CA server, then import it as "Local Certificate". If you have already gotten a certificate from a third party, you may import it directly. The supported types are PKCS12 Certificate and Certificate with a private key.

Click this button to import a saved file as the certification information. There are three types of local certificate supported by Vigor router.

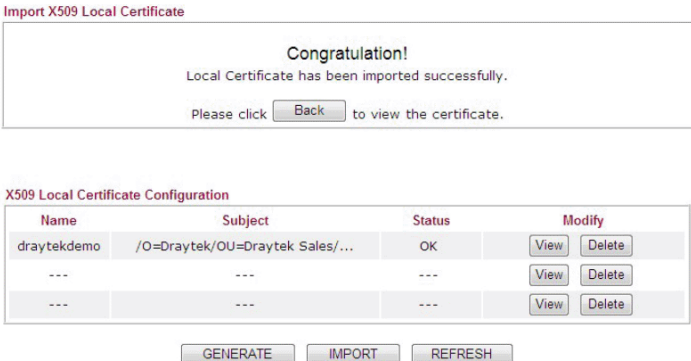
Import X509 Local Certificate

Upload Local Certificate
 Select a local certificate file.
 Certificate file:
 Click **Import** to upload the local certificate.

Upload PKCS12 Certificate
 Select a PKCS12 file.
 PKCS12 file:
 Password:
 Click **Import** to upload the PKCS12 file.

Upload Certificate and Private Key
 Select a certificate file and a matchable Private Key.
 Certificate file:
 Key file:
 Password:
 Click **Import** to upload the local certificate and private key.

Available settings are explained as follows:

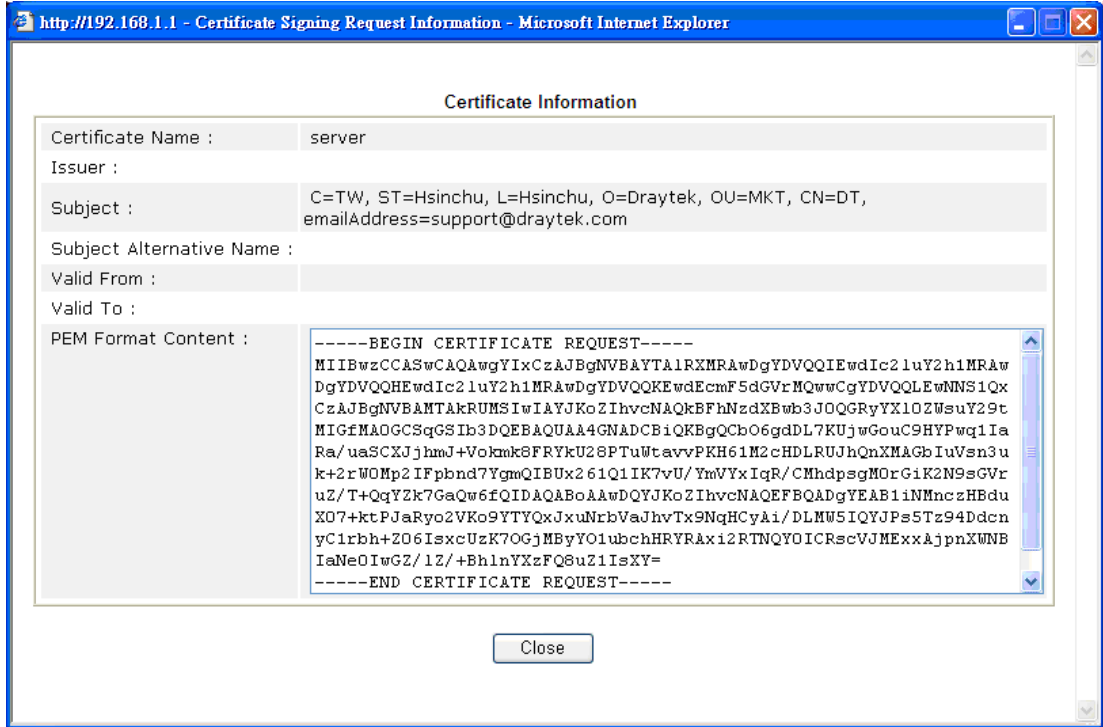
Item	Description																				
Upload Local Certificate	<p>It allows users to import the certificate which is generated by Vigor router and signed by CA server.</p> <p>If you have done well in certificate generation, the Status of the certificate will be shown as "OK".</p>  <p>The screenshot shows a 'Congratulations!' message: 'Local Certificate has been imported successfully. Please click <input type="button" value="Back"/> to view the certificate.'</p> <p>Below is the 'X509 Local Certificate Configuration' table:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Subject</th> <th>Status</th> <th colspan="2">Modify</th> </tr> </thead> <tbody> <tr> <td>draytekdemo</td> <td>/O=Draytek/OU=Draytek Sales/...</td> <td>OK</td> <td><input type="button" value="View"/></td> <td><input type="button" value="Delete"/></td> </tr> <tr> <td>---</td> <td>---</td> <td>---</td> <td><input type="button" value="View"/></td> <td><input type="button" value="Delete"/></td> </tr> <tr> <td>---</td> <td>---</td> <td>---</td> <td><input type="button" value="View"/></td> <td><input type="button" value="Delete"/></td> </tr> </tbody> </table> <p>Buttons: <input type="button" value="GENERATE"/> <input type="button" value="IMPORT"/> <input type="button" value="REFRESH"/></p>	Name	Subject	Status	Modify		draytekdemo	/O=Draytek/OU=Draytek Sales/...	OK	<input type="button" value="View"/>	<input type="button" value="Delete"/>	---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>	---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
Name	Subject	Status	Modify																		
draytekdemo	/O=Draytek/OU=Draytek Sales/...	OK	<input type="button" value="View"/>	<input type="button" value="Delete"/>																	
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>																	
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>																	
Upload PKCS12 Certificate	<p>It allows users to import the certificate whose extensions are usually .pfx or .p12. And these certificates usually need passwords.</p> <p>Note that PKCS12 is a standard for storing private keys and certificates securely. It is used in (among other things) Netscape and Microsoft Internet Explorer with their import and export options.</p>																				
Upload Certificate and Private Key	<p>It is useful when users have separated certificates and private keys. And the password is needed if the private key is encrypted.</p>																				

REFRESH

Click this button to refresh the information listed below.

View

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



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.

IV-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	---	---	<input type="button" value="Create"/>
Trusted CA-1	---	---	<input type="button" value="View"/> <input type="button" value="Delete"/>
Trusted CA-2	---	---	<input type="button" value="View"/> <input type="button" value="Delete"/>
Trusted CA-3	---	---	<input type="button" value="View"/> <input type="button" value="Delete"/>

Note:

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

Creating a Root CA

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

Certificate Name	Root CA
Subject Alternative Name	
Type	IP Address ▾
IP	<input type="text"/>
Subject Name	
Country (C)	<input type="text"/>
State (ST)	<input type="text"/>
Location (L)	<input type="text"/>
Organization (O)	<input type="text"/>
Organization Unit (OU)	<input type="text"/>
Common Name (CN)	<input type="text"/>
Email (E)	<input type="text"/>
Key Type	RSA ▾
Key Size	1024 Bit ▾
Algorithm	SHA-256 ▾

Importing a Trusted CA

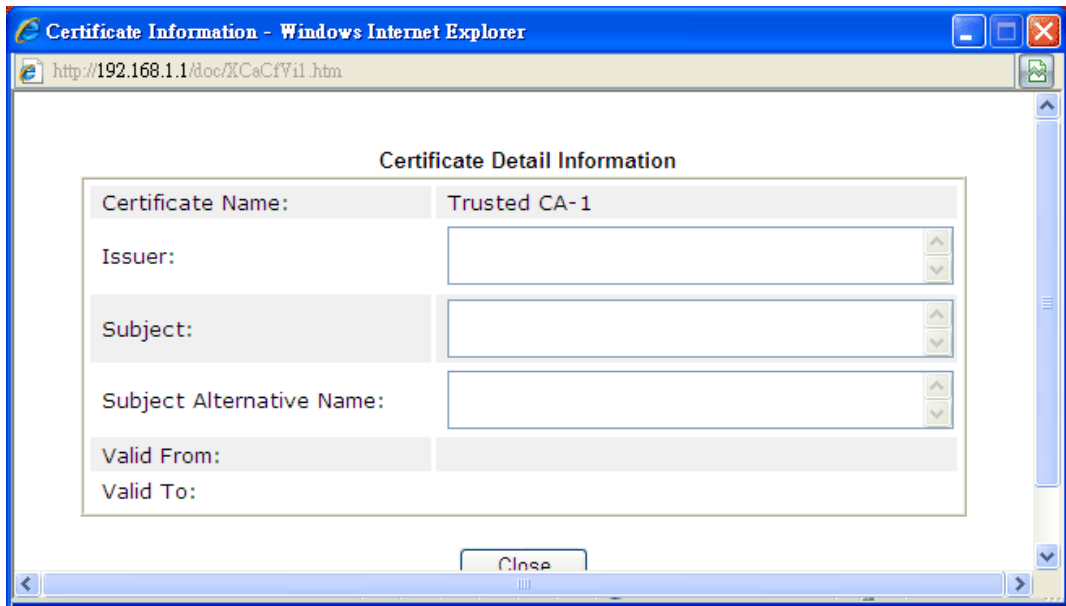
To import a pre-saved trusted CA certificate, please click **IMPORT** to open the following window. Use **Browse...** to find out the saved text file. Then click **Import**. The one you imported will be listed on the Trusted CA Certificate window.

Import X509 Trusted CA Certificate

Select a trusted CA certificate file.

Click **Import** to upload the certification.

For viewing each trusted CA certificate, click **View** to open the certificate detail information window. If you want to delete a CA certificate, choose the one and click **Delete** to remove all the certificate information.



IV-3-3 Certificate Backup

Local certificate and Trusted CA certificate for this router can be saved within one file. Please click **Backup** on the following screen to save them. If you want to set encryption password for these certificates, please type characters in both fields of **Encrypt password** and **Confirm password**.

Also, you can use **Restore** to retrieve these two settings to the router whenever you want.

Certificate Management >> Certificate Backup

Certificate Backup / Restoration

Backup

Encrypt password:

Confirm password:

Click to download certificates to your local PC as a file.

Restoration

Select a backup file to restore.

Decrypt password:

Click to upload the file.

Part V Security



Firewall



CSM

While the broadband users demand more bandwidth for multimedia, interactive applications, or distance learning, security has been always the most concerned. The firewall of the Vigor router helps to protect your local network against attack from unauthorized outsiders. It also restricts users in the local network from accessing the Internet.

CSM is an abbreviation of Central Security Management which is used to control IM/P2P usage, filter the web content and URL content to reach a goal of security management.

V-1 Firewall

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

Firewall Facilities

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

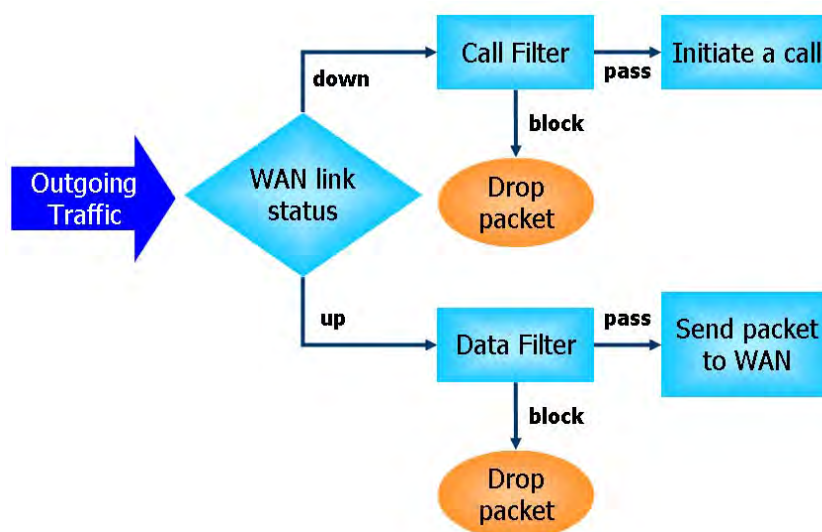
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

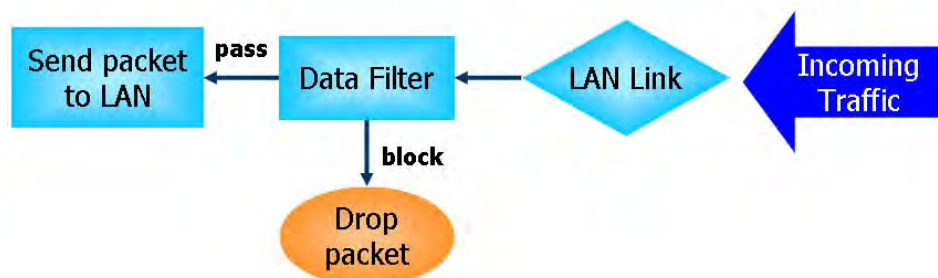
IP Filters

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

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

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





Stateful Packet Inspection (SPI)

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

Denial of Service (DoS) Defense

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

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

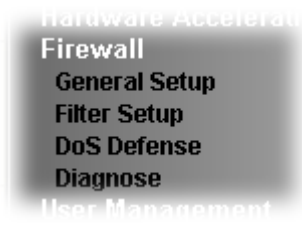
Also the Vigor router monitors the traffic. Any abnormal traffic flow violating the pre-defined parameter, such as the number of thresholds, is identified as an attack and the Vigor router will activate its defense mechanism to mitigate in a real-time manner.

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

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

Web User Interface

Below shows the menu items for Firewall.



V-1-1 General Setup

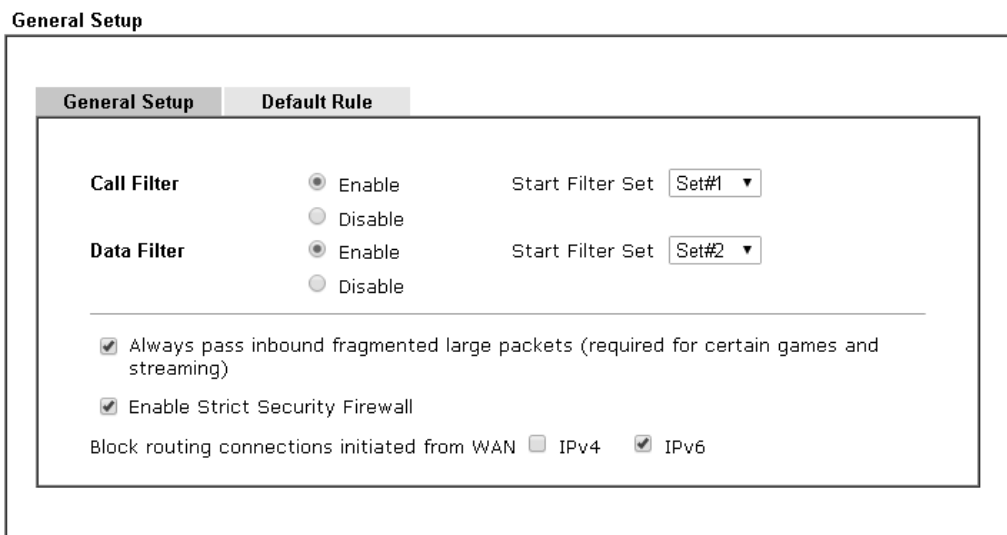
General Setup allows you to adjust settings of IP Filter and common options. Here you can enable or disable the **Call Filter** or **Data Filter**. Under some circumstance, your filter set can be linked to work in a serial manner. So here you assign the **Start Filter Set** only. Also you can configure the **Log Flag** settings, **Apply IP filter to VPN incoming packets**, and **Accept incoming fragmented UDP packets**.

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

General Setup Page

Such page allows you to enable / disable Call Filter and Data Filter, determine general rule for filtering the incoming and outgoing data.

Firewall >> General Setup



Note:

Packets are filtered by firewall functions in the following order:
1.Data Filter Sets and Rules 2.Block routing connections initiated from WAN 3.Default Rule

OK Cancel



Note:

This will not backup the detail setting of Quality of Service and Schedule.

Available settings are explained as follows:

Item	Description
Call Filter	Check Enable to activate the Call Filter function. Assign a start filter set for the Call Filter.
Data Filter	Check Enable to activate the Data Filter function. Assign a start filter set for the Data Filter.
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 connections initiated from WAN	Usually, IPv6 network sessions/traffic from WAN to LAN will be accepted by IPv6 firewall in default. IPv6 - To prevent remote client accessing into the PCs on LAN, check the box to make the packets (routed from WAN to LAN) via IPv6 being blocked by such router. It is effective only for the packets routed but not for packets translated by NAT. IPv4 - To prevent remote client accessing into the PCs on LAN, check the box to make the incoming packets via IPv4 being blocked by such router. It is effective only for the packets routed but not for packets translated by NAT.
Backup Firewall	Click Backup to save the firewall configuration.
Restore Firewall	Click Select to choose a firewall configuration file. Then click Restore to apply the file.

Default Rule Page

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

Firewall >> General Setup

General Setup

General Setup
Default Rule

Actions for default rule:

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

Advance Setting Edit

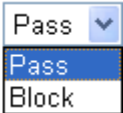
OK Cancel

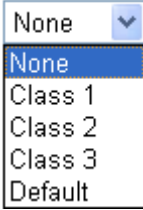
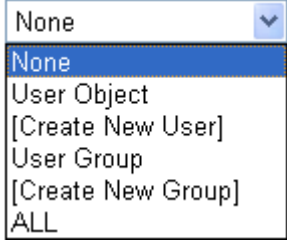
Backup Firewall : Backup Restore Firewall: 選擇檔案 未選擇任何檔案 Restore

Note:

This will not backup the detail setting of Quality of Service and Schedule.

Available settings are explained as follows:

Item	Description
Filter	<p>Select Pass or Block for the packets that do not match with the filter rules.</p> <p>Filter </p>
Sessions Control	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 70000.
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.

	
User Management	<p>Such item is available only when Rule-Based is selected in User Management>>General Setup. The general firewall rule will be applied to the user/user group/all users specified here.</p>  <p>When there is no user profile or group profile existed, Create New User or Create New Group item will appear for you to click to create a new one.</p>
APP Enforcement	<p>Select an APP Enforcement profile for global IM/P2P application blocking. If there is no profile for you to select, please choose [Create New] from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the APP Enforcement profile selected here. For detailed information, refer to the section of APP Enforcement profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p>
URL Content Filter	<p>Select one of the URL Content Filter profile settings (created in CSM>> URL Content Filter) for applying with this router. Please set at least one profile for choosing in CSM>> URL Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for URL Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p>
Web Content Filter	<p>Select one of the Web Content Filter profile settings (created in CSM>> Web Content Filter) for applying with this router. Please set at least one profile for anti-virus in CSM>> Web Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for Web Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p>
DNS Filter	<p>Select one of the DNS Filter profile settings (created in CSM>>DNS Filter) for applying with this router. Please set at least one profile in CSM>> Web Content Filter web page first. Or click the DNS Filter link in this page to create a new profile.</p>
Advance Setting	<p>Click Edit to open the following window. However, it is</p>

strongly recommended to use the default settings here.

Firewall >> General Setup

Advance Setting

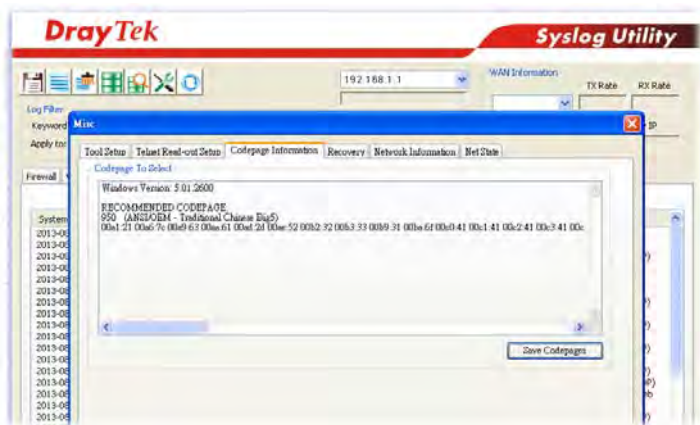
Codepage:

Window size:

Session timeout: Minute

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.

Backup Firewall	Click Backup to save the firewall configuration.
Restore Firewall	Click Select to choose a firewall configuration file. Then click Restore to apply the file.

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

V-1-2 Filter Setup

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

Firewall >> Filter Setup

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

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

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1

Comments :

Rule	Active	Comments	Direction	Src IP	Dst IP	Service Type	Action	CSM	Move Up	Move Down
1	<input checked="" type="checkbox"/>	Block NetBios	LAN/DMZ/RT/VPN -> WAN	Any	Any	TCP/UDP, Port: from 137~139 to any	Block Immediately			Down
2	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
3	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
4	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
5	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
6	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
7	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	

Filter Set [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#)

Next Filter Set

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

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.
Direction	Display the direction of packet.
Src IP / Dst IP	Display the IP address of source /destination.
Service Type	Display the type and port number of the packet.

Action	Display the packets to be passed /blocked.
CSM	Display the content security managed
Move Up/Down	Use Up or Down link to move the order of the filter rules.
Next Filter Set	Set the link to the next filter set to be executed after the current filter run. Do not make a loop with many filter sets.
Wizard Mode	Allow to configure frequently used settings for filter rule via several setting pages.
Advance Mode	Allow to configure detailed settings of filter rule.

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:

Firewall >> Edit Filter Set >> Edit Filter Rule Wizard

Filter Set 1 Rule 1

Firewall Rule applies to packets that meet the following criteria

Comments:

Direction:

Source IP:

Start IP Address:

End IP Address:

Subnet Mask:

Destination IP:

Start IP Address:

End IP Address:

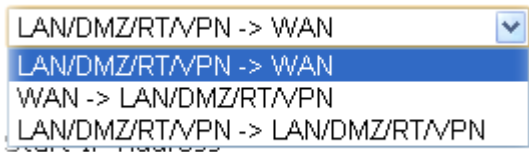
Subnet Mask:

Protocol:

Source Port:

Destination Port:

Available settings are explained as follows:

Item	Description
Comments	Enter filter set comments/description. Maximum length is 14- character long.
Direction	Set the direction of packet flow. It is for Data Filter only. For the Call Filter , this setting is not available since Call Filter is only applied to outgoing traffic.  Note: RT means routing domain for 2nd subnet or other LAN.
Source/Destination IP	To set the IP address manually, please choose Any Address/Single Address/Range Address/Subnet Address as the Address Type and type them in this dialog.

Protocol	Specify the protocol(s) which this filter rule will apply to.
Source Port / Destination Port	<p>(=) - when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type.</p> <p>(!=) - when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.</p> <p>(>) - the port number greater than this value is available.</p> <p>(<) - the port number less than this value is available for this profile.</p>

- Click Next to get the following page.

Firewall >> Edit Filter Set >> Edit Filter Rule Wizard

Filter Set 1 Rule 1

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

Pass

The current setting is :

Pass Immediately

APP Enforcement:

URL Content Filter:

Web Content Filter:

DNS Filter:

Block Immediately

Available settings are explained as follows:

Item	Description
Pass Immediately	<p>Packets matching the rule will be passed immediately.</p> <p>APP Enforcement - Select an APP Enforcement profile for global IM/P2P application blocking. If there is no profile for you to select, please choose [Create New] from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the APP Enforcement profile selected here. For detailed information, refer to the section of APP Enforcement profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p> <p>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.</p> <p>Web Content Filter - Select one of the Web Content Filter profile settings (created in CSM>> Web Content Filter) for</p>

	<p>applying with this router. Please set at least one profile for anti-virus in CSM>> Web Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for Web Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p> <p>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.</p>
Block Immediately	Packets matching the rule will be dropped immediately.

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

Firewall >> Edit Filter Set >> Edit Filter Rule Wizard

Filter Set 1 Rule 1 Configuration Summary

Comments :	Block NetBios
Direction	
LAN/DMZ/RT/VPN -> WAN	
Criteria	
Source IP	Any
Destination IP	Any
Protocol	TCP/UDP, Port: from 137 ~ 139 to any
More options	
Pass Immediately	APP Enforcement : None URL Content Filter : None Web Content Filter : 1 - Default DNS Filter : None

- 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.

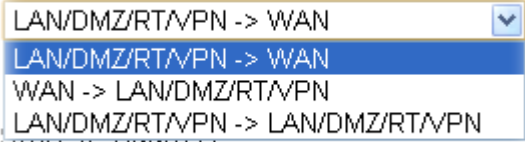
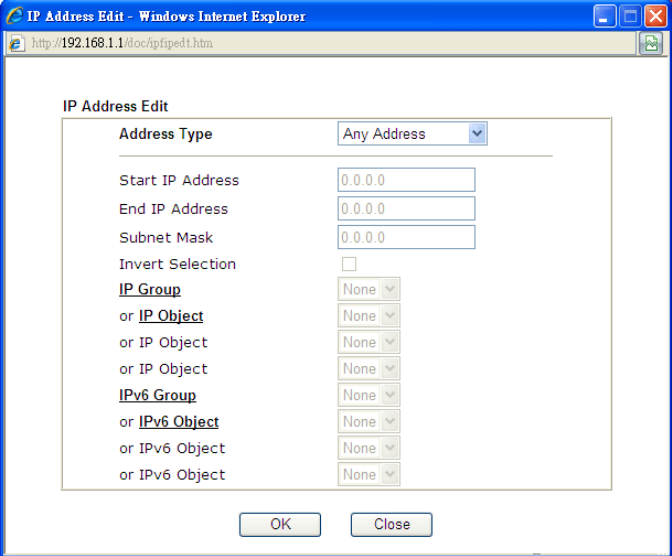
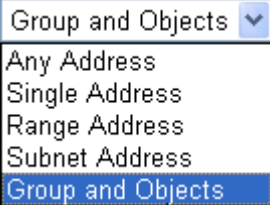
Firewall >> Edit Filter Set >> Edit Filter Rule

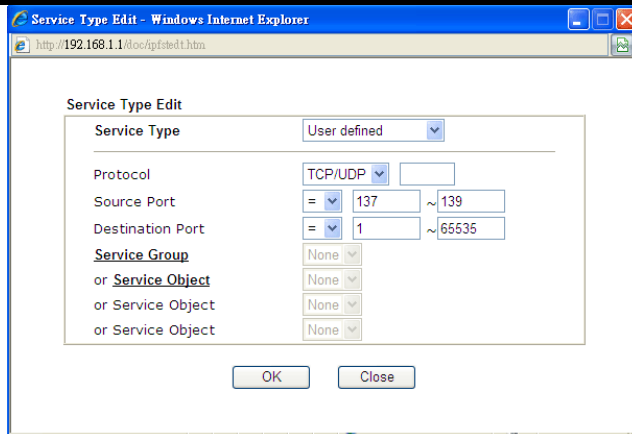
Filter Set 1 Rule 1

<input checked="" type="checkbox"/> Check to enable the Filter Rule		
Comments:	Block NetBios	
Index(1-15) in Schedule Setup:	, , ,	
Clear sessions when schedule ON:	<input type="checkbox"/> Enable	
<hr/>		
Direction:	LAN/DMZ/RT/WPN -> WAN	
Source IP:	Any	<input type="button" value="Edit"/>
Destination IP:	Any	<input type="button" value="Edit"/>
Service Type:	TCP/UDP, Port: from 137~139 to any	<input type="button" value="Edit"/>
Fragments:	Don't Care	
<hr/>		
Application	Action/Profile	Syslog
Filter:	Block Immediately	<input type="checkbox"/>
Branch to Other Filter Set:	None	
Sessions Control	0 / 60000	<input type="checkbox"/>
MAC Bind IP	Non-Strict	<input type="checkbox"/>
Quality of Service	None	<input type="checkbox"/>
User Management	None	<input type="checkbox"/>
APP Enforcement:	None	<input type="checkbox"/>
URL Content Filter:	None	<input type="checkbox"/>
Web Content Filter:	None	<input type="checkbox"/>
DNS Filter	None	<input type="checkbox"/>
<hr/>		
Advance Setting	<input type="button" value="Edit"/>	

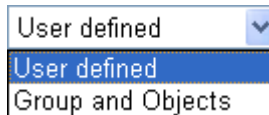
Available settings are explained as follows:

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.

	 <p>Note: RT means routing domain for 2nd subnet or other LAN.</p>
Source/Destination IP	<p>Click Edit to access into the following dialog to choose the source/destination IP or IP ranges.</p>  <p>To set the IP address manually, please choose Any Address/Single Address/Range Address/Subnet Address as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose Group and Objects as the Address Type.</p>  <p>From the IP Group drop down list, choose the one that you want to apply. Or use the IP Object drop down list to choose the object that you want.</p>
Service Type	<p>Click Edit to access into the following dialog to choose a suitable service type.</p>



To set the service type manually, please choose **User defined** as the Service Type and type them in this dialog. In addition, if you want to use the service type from defined groups or objects, please choose **Group and Objects** as the Service Type.



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

Source/Destination Port -

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

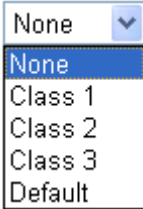
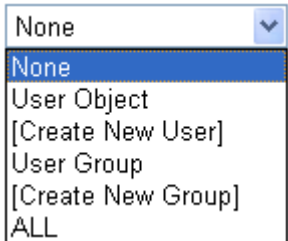
(!=) - when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.

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

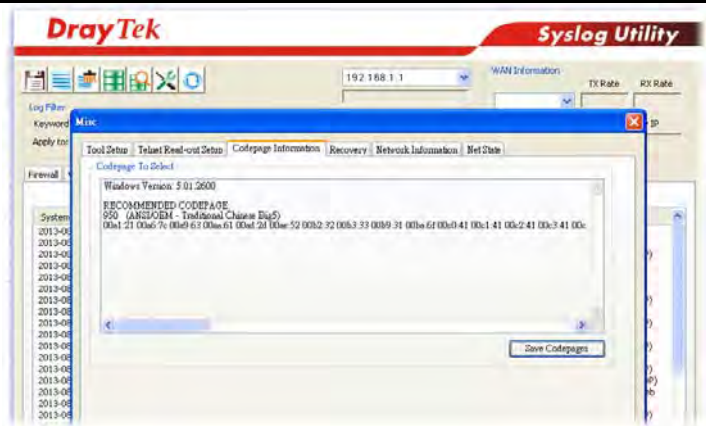
(<) - the port number less than this value is available for this profile.

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

<p>Fragments</p>	<p>Specify the action for fragmented packets. And it is used for Data Filter only.</p> <p>Don't care -No action will be taken towards fragmented packets.</p> <p>Unfragmented -Apply the rule to unfragmented packets.</p> <p>Fragmented - Apply the rule to fragmented packets.</p> <p>Too Short - Apply the rule only to packets that are too short to contain a complete header.</p>
<p>Filter</p>	<p>Specifies the action to be taken when packets match the rule.</p> <p>Block Immediately - Packets matching the rule will be dropped immediately.</p> <p>Pass Immediately - Packets matching the rule will be passed immediately.</p> <p>Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped.</p>

	<p>Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through.</p>
Branch to other Filter Set	<p>If the packet matches the filter rule, the next filter rule will branch to the specified filter set. Select next filter rule to branch from the drop-down menu. Be aware that the router will apply the specified filter rule for ever and will not return to previous filter rule any more.</p>
Sessions Control	<p>The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.</p>
MAC Bind IP	<p>Strict - Make the MAC address and IP address settings configured in IP Object for Source IP and Destination IP are bound for applying such filter rule.</p> <p>No-Strict - no limitation.</p>
Quality of Service	<p>Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later.</p> 
User Management	<p>Such item is available only when Rule-Based is selected in User Management>>General Setup. The general firewall rule will be applied to the user/user group/all users specified here.</p>  <p>Note: When there is no user profile or group profile existed, Create New User or Create New Group item will appear for you to click to create a new one.</p>
APP Enforcement	<p>Select an APP Enforcement profile for global IM/P2P application blocking. If there is no profile for you to select, please choose [Create New] from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the APP Enforcement profile selected here. For detailed information, refer to the section of APP Enforcement profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p>
URL Content Filter	<p>Select one of the URL Content Filter profile settings (created in CSM>> URL Content Filter) for applying with this router. Please set at least one profile for choosing in CSM>> URL Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to</p>

	<p>record information for URL Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p>
<p>Web Content Filter</p>	<p>Select one of the Web Content Filter profile settings (created in CSM>> Web Content Filter) for applying with this router. Please set at least one profile for anti-virus in CSM>> Web Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for Web Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p>
<p>DNS Filter</p>	<p>Select one of the DNS Filter profile settings (created in CSM>> DNS Filter) for applying with this router. Please set at least one profile in CSM>> Web Content Filter web page first. Or click the DNS Filter link from the drop down list in this page to create a new profile.</p>
<p>Advance Setting</p>	<p>Click Edit to open the following window. However, it is strongly recommended to use the default settings here.</p> <p>Firewall >> Edit Filter Set >> Edit Filter Rule</p> <hr/> <p>Filter Set 1 Rule 1</p> <div data-bbox="715 936 1385 1198" style="border: 1px solid gray; padding: 5px;"> <p>Advance Setting</p> <p>Codepage: ANSI(1252)-Latin I ▼</p> <p>Window size: 65535</p> <p>Session timeout: 1440 Minute</p> <p>DrayTek Banner: <input checked="" type="checkbox"/></p> <hr/> <p>Strict Security Checking</p> <p><input type="checkbox"/> APP Enforcement</p> </div> <p style="text-align: center;"> OK Close </p> <p>Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage.</p> <p>If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.</p>



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

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

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



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

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

V-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

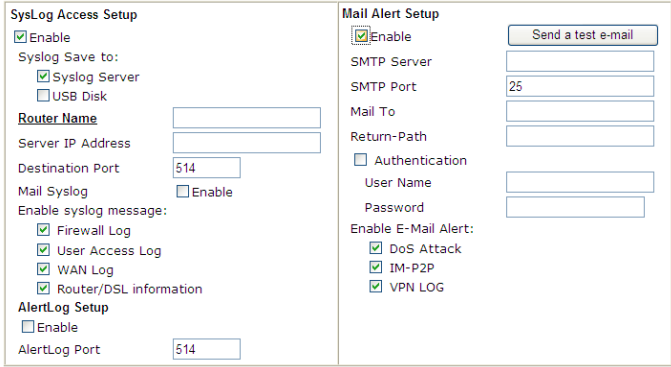
Enable DoS Defense

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

Available settings are explained as follows:

Item	Description
Enable Dos Defense	Check the box to activate the DoS Defense Functionality.
Select All	Click this button to select all the items listed below.
Enable SYN flood defense	<p>Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent TCP SYN packets for a period defined in Timeout. The goal for this is prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor router.</p> <p>By default, the threshold and timeout values are set to 2000 packets per second and 10 seconds, respectively. That means, when 2000 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.</p>
Enable UDP flood defense	<p>Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent UDP packets for a period defined in Timeout.</p> <p>The default setting for threshold and timeout are 2000</p>

	<p>packets per second and 10 seconds, respectively. That means, when 2000 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.</p>
Enable ICMP flood defense	<p>Check the box to activate the ICMP flood defense function. Similar to the UDP flood defense function, once if the Threshold of ICMP packets from Internet has exceeded the defined value, the router will discard the ICMP echo requests coming from the Internet.</p> <p>The default setting for threshold and timeout are 250 packets per second and 10 seconds, respectively. That means, when 250 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.</p>
Enable Port Scan detection	<p>Port Scan attacks the Vigor router by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the port-scanning Threshold rate, the Vigor router will send out a warning.</p> <p>By default, the Vigor router sets the threshold as 2000 packets per second. That means, when 2000 packets per second received, they will be regarded as "attack event".</p>
Block IP options	<p>Check the box to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messages...etc. An eavesdropper outside might learn the details of your private networks.</p>
Block Land	<p>Check the box to enforce the Vigor router to defend the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.</p>
Block Smurf	<p>Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.</p>
Block trace route	<p>Check the box to enforce the Vigor router not to forward any trace route packets.</p>
Block SYN fragment	<p>Check the box to activate the Block SYN fragment function. The Vigor router will drop any packets having SYN flag and more fragment bit set.</p>
Block Fraggle Attack	<p>Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked.</p> <p>Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.</p>

Block TCP flag scan	Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include <i>no flag scan</i> , <i>FIN without ACK scan</i> , <i>SYN FINscan</i> , <i>Xmas scan</i> and <i>full Xmas scan</i> .
Block Tear Drop	Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.
Block Ping of Death	Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.
Block ICMP Fragment	Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.
Block Unassigned Numbers	Check the box to activate the Block Unknown Protocol function. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and reject this kind of packets.
Warning Messages	<p>We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client.</p> <p>All the warning messages related to DoS Defense will be sent to user and user can review it through Syslog daemon. Look for the keyword DoS in the message, followed by a name to indicate what kind of attacks is detected.</p> <p>System Maintenance >> SysLog / Mail Alert Setup</p>  <p>Note: 1. Mail Syslog cannot be activated unless USB Disk is ticked for "Syslog Save to". 2. Mail Syslog feature sends a Syslog file when its size reaches 1M Bytes.</p>

DrayTek Syslog 4.5.3

DrayTek Syslog Utility

Log Filter

Keyword:

Apply to: Refresh

WAN Information: 172.16.3.130 TX Rate RX Rate

LAN Information: TX Packets RX Packets WAN IP Gateway IP

Show Syslog List Show Defense Alert TOP10

IP Filter Log CSR Log Defense Log Pause

System Time	Router Time	Host	Message
2013-08-20 11:53:47	Aug 20 03:53:05	vigor-router	[DOS][StoC][fraggle_attack][0.0.0.0:68->255.255.255.255:67][UDP][Len=20, Tlen=576]
2013-08-20 11:53:47	Aug 20 03:53:05	vigor-router	[DOS][StoC][fraggle_attack][0.0.0.0:68->255.255.255.255:67][UDP][Len=20, Tlen=576]
2013-08-20 11:53:46	Aug 20 03:53:03	vigor-router	[DOS][StoC][fraggle_attack][192.168.1.10:4744->255.255.255.255:9999][UDP][Len=20, Tlen=576]
2013-08-20 11:53:14	Aug 20 03:53:02	vigor-router	[DOS][StoC][fraggle_attack][0.0.0.0:68->255.255.255.255:67][UDP][Len=20, Tlen=576]
2013-08-28 11:53:14	Aug 28 03:53:02	vigor-router	[DOS][StoC][fraggle_attack][0.0.0.0:68->255.255.255.255:67][UDP][Len=20, Tlen=576]

System Time: Time tag from the computer which runs the syslog application Router Time: Time tag from router

V-1-4 Diagnose

The purpose of this function is to test when the router receiving incoming packet, which firewall rule will be applied to that packet. The test result, including firewall rule profile, IP address translation in packet transmission, state of the firewall functions and etc., also will be shown on this page.



Info

The result obtained by using Diagnose is offered for RD debug. It will be different according to actual state such as network connection, LAN/WAN settings and so on.

Firewall >> Diagnose

Mode

ICMP UDP TCP IPv4 ▾

Direction

From LAN ▾

Test View



Packet & Payload

Packet	Enable	Direction	Protocol
1	<input checked="" type="checkbox"/>	A->B ▾	UDP:Customize
2	<input checked="" type="checkbox"/>	B->A ▾	UDP:Customize

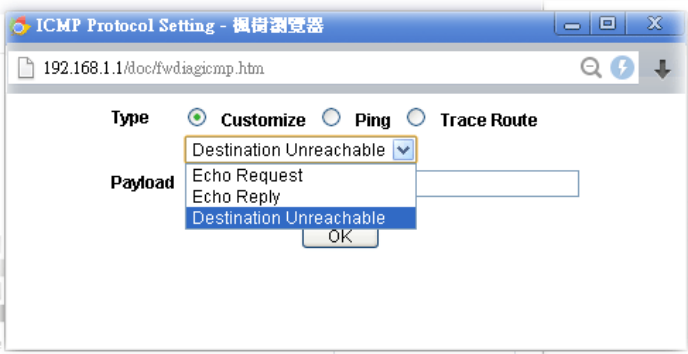
Note:

This is firewall live test which need setup WAN and plug cable in.

Analyze

Available settings are explained as follows:

Item	Description
Mode	To have a firewall rule test, specify the service type (ICMP, UDP, TCP) of the packet and type of the IP address (IPv4/IPv6).
Direction	Set the way (from WAN or from LAN) that Vigor router receives the first packet for test. Different way means the firewall will process the connection initiated from LAN or from WAN.
Test View	This is a dynamic display page. According to the direction specified, test view will display the figure to guide you typing IP address, port number, and MAC address. Later, after clicking the Analyze button, the information for the firewall rule profile and address translation will be shown on this page.
Src IP	Type the IPv4/IPv6 address of the packet's source.
Src Port	Type the port number of the packet's source.
Src MAC	Type the MAC address of the packet's source.

Dst IP	Type the IPv4/IPv6 address of the packet's destination.
Dst Port	Type the port number of the packet's destination.
Packet & Payload	<p>In firewall diagnose, two packets belong to one connection. In general, two packets are enough for Vigor router to perform this test.</p> <p>Enable - Check the box to send out the test packet.</p> <p>Direction - The first packet of the firewall test will follow the direction specified above. However, the direction for the second packet might be different. Simply choose the direction (from Computer A to B or from the B to A) for the second packet.</p> <p>Protocol - It displays the mode selected above and the sate. If required, click the mode link to configure advanced setting. The common service type (Customize, Ping, Trace Route / Customize, DNS, Trace Route / Customize, Http(GET) related to that mode (ICMP / UDP / TCP) will be shown on the following dialog box.</p>  <ul style="list-style-type: none"> ● Type - Choose Customize, Ping, Trace Route / Customize, DNS, Trace Route / Customize, Http (GET). ● Payload - It is available when Customzie is selected. Simply type 16 HEX characters which represent certain packet (e.g., DNS packet) if you want to set the data transfered with protocol (ICMP/UDP/TCP) which is different to Type setting.
Analyze	Execute the test and analyze the result.

The following figure shows the test result after clicking **Analyze**. Processing state for the functions (MAC Filter, QoS, User management, etc.) related to the firewall will be displayed by green or red LED.

Firewall >> Diagnose

Mode
 ICMP UDP TCP

Direction

Test View

A

192.168.1.111:22222
->7.7.7.7:51348

LAN

Firewall

WAN1

<<REPLY

7.7.7.7:51348
172.16.2.234:62094<-

B

Status	Packet	Set	Rule	UCF/WCF
Pass	2	default	default	n/a

Packet & Payload

Packet	Enable	Direction	Protocol			
1	<input checked="" type="checkbox"/>	A->B	UDP:Customize			
Acceleration						
2	<input checked="" type="checkbox"/>	B->A	UDP:Customize			
Acceleration						
<input checked="" type="checkbox"/> SESS CTL	<input checked="" type="checkbox"/> MAC FILTER	<input checked="" type="checkbox"/> PCAP	<input checked="" type="checkbox"/> USER MGT	<input checked="" type="checkbox"/> APPE	<input checked="" type="checkbox"/> UCF	<input checked="" type="checkbox"/> WCE
<input checked="" type="checkbox"/> DNSF	<input checked="" type="checkbox"/> SESS LMT	<input checked="" type="checkbox"/> BW LMT	<input checked="" type="checkbox"/> QOS	<input checked="" type="checkbox"/> APP_QOS	<input checked="" type="checkbox"/> HW ACC	

APP: The APP need to check. ●: The APP is completed.
 APP: The APP doesn't need to check. ●: The APP is processing.

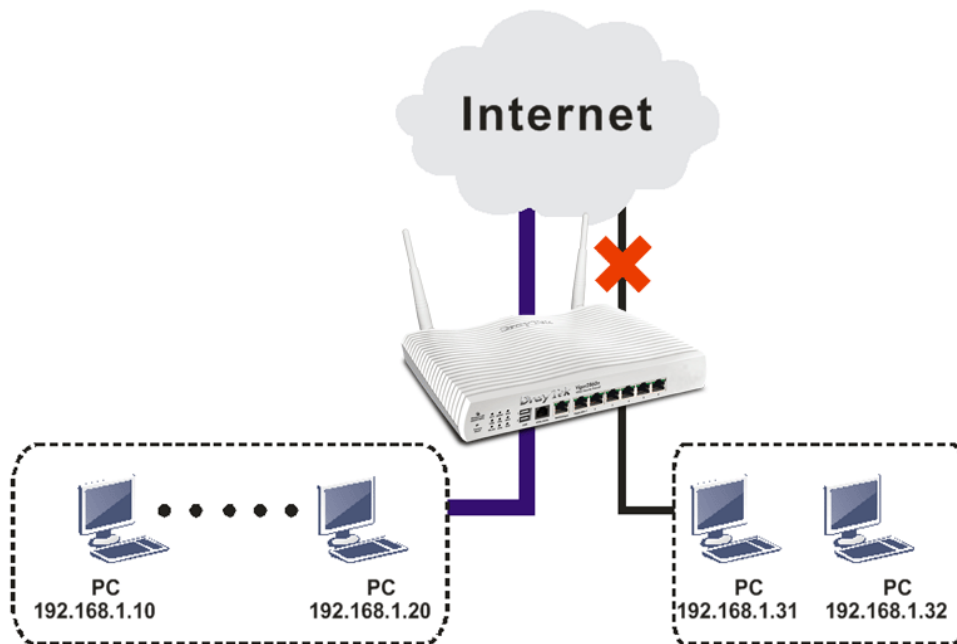
Note:
 PCAP is "ip pcap" in telnet command.

<<Back Reset

Application Notes

A-1 How to Configure Certain Computers Accessing to Internet

We can specify certain computers (e.g., 192.168.1.10 ~ 192.168.1.20) accessing to Internet through Vigor router. Others (e.g., 192.168.1.31 and 192.168.1.32) outside the range can get the source from LAN only.



The way we can use is to set two rules under Firewall. For Rule 1 of Set 2 under Firewall>>Filter Setup is used as the default setting, we have to create a new rule starting from Filter Rule 2 of Set 2.

1. Access into the web user interface of Vigor router.
2. Open Firewall>>Filter Setup. Click the Set 2 link, choose Advance Mode and choose the Filter Rule 2 button.

Firewall >> Filter Setup

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

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 2

Comments: Default Data Filter

Rule	Active	Comments	Direction	Src IP	Dst IP	Service Type	Action	CSM	Move Up	Move Down
1	<input checked="" type="checkbox"/>	xNetBios -> DNS	LAN/DMZ/RT/VPN -> WAN	Any	Any	TCP/UDP, Port: from 137~139 to 53	Block Immediately			Down
2	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
3	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down

3. 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**.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 2

Check to enable the Filter Rule

Comments:

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

Clear sessions when schedule ON: Enable

Direction: LAN/RT/VPN -> WAN

Source IP:

Destination IP:

Service Type:

Fragments:

Application

Filter:

Branch to Other Filter Set:

Sessions Control:

Syslog:



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**.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 3

Check to enable the Filter Rule

Comments:

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

Clear sessions when schedule ON: Enable

Direction: LAN/RT/VPN -> WAN

Source IP:

Destination IP:

Service Type:

Fragments:

Application

Filter:

Branch to Other Filter Set:

Syslog:

- A dialog box will be popped up. Choose **Range Address** as **Address Type** by using the drop down list. Type 192.168.1.10 in the field of **Start IP**, and type 192.168.1.20 in the field of **End IP**. Then, click **OK** to save the settings. The computers within the range can access into the Internet.

IP Address Edit

Address Type	Range Address
Start IP Address	192.168.1.10
End IP Address	192.168.1.20
Subnet Mask	0.0.0.0
Invert Selection	<input type="checkbox"/>
IP Group	None
or IP Object	None
or IP Object	None
or IP Object	None
IPv6 Group	None
or IPv6 Object	None
or IPv6 Object	None
or IPv6 Object	None

OK Close

- Now, check the content of **Source IP** is correct or not. The action for **Filter** shall be set with **Pass Immediately**. Then, click **OK** to save the settings.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 3

<input checked="" type="checkbox"/> Check to enable the Filter Rule	
Comments:	open_ip
Index(1-15) in Schedule Setup:	
Clear sessions when schedule ON:	<input type="checkbox"/> Enable
Direction:	LAN/RT/VPN -> WAN
Source IP:	192.168.1.10~192.168.1.20
Destination IP:	Any
Service Type:	Any
Fragments:	Don't Care
Application	Action/Profile
Filter:	Pass Immediately
Branch to Other Filter Set:	None
	Syslog <input type="checkbox"/>

8. Both filter rules have been created. Click OK.

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 2

Comments :

Rule	Active	Comments	Direction	Src IP	Dst IP	Service Type
1	<input checked="" type="checkbox"/>	xNetBios -> DNS	LAN/RT/VPN -> WAN	Any	Any	TCP/UDP, Port: from 137~139 to 53
2	<input checked="" type="checkbox"/>	block_all	LAN/RT/VPN -> WAN	Any	Any	Any
3	<input checked="" type="checkbox"/>	open_ip	LAN/RT/VPN -> WAN	192.168.1.10 ~ 192.168.1.20	Any	Any
4	<input type="checkbox"/>		LAN/RT/VPN -> WAN	Any	Any	Any

Now, all the settings are configured well. Only the computers with the IP addresses within 192.168.1.10 ~ 192.168.1.20 can access to Internet.

V-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 misuse during office hour or prevent unknown security leak. It is similar situation for corporation towards peer-to-peer applications since file-sharing can be convenient but insecure at the same time. To address these needs, we provide CSM functionality.

URL Content Filter

To provide an appropriate cyberspace to users, Vigor router equips with **URL Content Filter** not only to limit illegal traffic from/to the inappropriate web sites but also prohibit other web feature where malicious code may conceal.

Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines to teenagers. At office, **URL Content Filter** can also provide a job-related only environment hence to increase the employee work efficiency. How can URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.

On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from websites, you may risk bringing threat to your system. For example, an ActiveX control object is usually used for providing interactive web feature. If malicious code hides inside, it may occupy user's system.

Web Content Filter

We all know that the content on the Internet just like other types of media may be inappropriate sometimes. As a responsible parent or employer, you should protect those in your trust against the hazards. With Web filtering service of the Vigor router, you can protect your business from common primary threats, such as productivity, legal liability, network and security threats. For parents, you can protect your children from viewing adult websites or chat rooms.

Once you have activated your Web Filtering service in Vigor router and chosen the categories of website you wish to restrict, each URL address requested (e.g. www.bbc.co.uk) will be checked against our server database. This database is updated as frequent as daily by a global team of Internet researchers. The server will look up the URL and return a category to your router. Your Vigor router will then decide whether to allow access to this site according to the categories you have selected. Please note that this action will not introduce any delay in your Web surfing because each of multiple load balanced database servers can handle millions of requests for categorization.



Info

The priority of URL Content Filter is higher than Web Content Filter.

Web User Interface

Objects Setting
CSM
APP Enforcement Profile
APPE Signature Upgrade
URL Content Filter Profile
Web Content Filter Profile
DNS Filter Profile

V-2-1 APP Enforcement Profile

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

CSM >> APP Enforcement Profile

APP Enforcement Profile Table: | [Set to Factory Default](#) |

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

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.

CSM >> APP Enforcement Profile

Profile Index : 1 Profile Name:

IM		P2P	Protocol	OTHERS
<input type="button" value="Select All"/>		<input type="button" value="Clear All"/>		
IM				
Enable	APP Name	Version	Note	
<input type="checkbox"/>	AIM	5.9		
<input type="checkbox"/>	AIM	8	Only block Login. If users have already logged in, AIM services can not be blocked.	
<input type="checkbox"/>	AliWWW	2008		
<input type="checkbox"/>	Ares	2.0.9		
<input type="checkbox"/>	BaiduHi	37378		
<input type="checkbox"/>	Facebook	97.0.0.18.69	To block Facebook for PC and mobile phone(97.0.0.18.69).	
<input type="checkbox"/>	Fetion	2010		
<input type="checkbox"/>	GaduGadu Protocol			
<input type="checkbox"/>	Google Chat			
<input type="checkbox"/>	Google Hangouts	18.0	Block PC user's login and Android user's chat/phone service.	
<input type="checkbox"/>	ICQ	7	In ICQ6, if Videos are blocked, Voices will be blocked at the same time. In ICQ5 or former versions, Videos and Voices can be blocked separately.	
<input type="checkbox"/>	ICU2	8.0.6		

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

The items categorized under P2P -----

CSM >> APP Enforcement Profile

Profile Index : 1 Profile Name:

IM	P2P	Protocol	OTHERS
<input type="button" value="Select All"/>	<input type="button" value="Clear All"/>		
BitTorrent			
Enable	APP Name	Version	Note
<input type="checkbox"/>	BitTorrent		The encrypted connection can not be 100% blocked. To block BitComet (1.30), BitSpirit (3.2.1), BitTorrent (4.4.1) and UltraTorrent (2.0).
FastTrack			
Enable	APP Name	Version	Note
<input type="checkbox"/>	FASTTRACK		To block BareShare (6.2.0.45), iMesh (9.1), KazaA (1.0.0.3) and Shareaza (4.1.0).
Gnutella			
Enable	APP Name	Version	Note
<input type="checkbox"/>	GNUTELLA		To block BareShare (5.1.0.26), Foxy (1.9.9), LimeWireWin (4.18.3) and Shareaza (2.3.0.0).
OpenFT			
Enable	APP Name	Version	Note
<input type="checkbox"/>	OpenFT		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 "Connecting" status. KCeasy (0.19) also supports Ares

The items categorized under OTHERS-----

CSM >> APP Enforcement Profile

Profile Index : 1 Profile Name:

IM	P2P	Protocol	OTHERS
Select All	Clear All		
TUNNEL			
Enable	APP Name	Version	Note
<input type="checkbox"/>	DNSEncrypt	0.0.6	Only blocks DNSEncrypt login.
<input type="checkbox"/>	DynaPass	1.5	
<input type="checkbox"/>	FreeU	10	
<input type="checkbox"/>	HTTP Proxy		
<input type="checkbox"/>	HTTP Tunnel	4.4.4000	
<input type="checkbox"/>	Hamachi	1.0.2.5	
<input type="checkbox"/>	Hotspot Shield	4.15.3	Block Hotspot Shield from establishing VPN connections. Please note that the APP Enforcement needs to be enabled prior than the VPN connections, or the blocking may not be successful.
<input type="checkbox"/>	MS Teredo		
<input type="checkbox"/>	PGPNet	7.0.3	
<input type="checkbox"/>	Ping Tunnel	0.61	
<input type="checkbox"/>	RealTunnel	1.0.1	
<input type="checkbox"/>	Skyfire	1.5	
<input type="checkbox"/>	Socks 4/5		Please note that Radmin will also be blocked by this item. Please set the server port of Radmin within 5001~32767 to avoid being blocked.

V-2-2 APPE Signature Upgrade

The APPE Enforcement Profile adopted by Vigor router will be treated as the APPE signature. DrayTek will periodically upgrade versions for all of the APPs supported by Vigor router. However, it might be inconvenient for users to upgrade the APP version one by one. This feature is specially designed to offer a quick method to execute APP version upgrade. Users can perform the APPE signature upgrade manually or configure the settings on this page to make Vigor router performing the APPE signature automatically.

CSM >> APPE Signature Upgrade

APP Enforcement License

[Activate](#)

[Status: **Not Activated**]

Upgrade Setting

APPE Module Version: **10.11**

New version from the Internet: -- [Download](#)

Upgrade via interface: [auto-selected](#)

(Waiting for WAN connection...)

Setup Download Server	auto-selected	Find more
Signature authentication / download message		
<pre>[2000-01-01 00:00:02] Load APPE signature failed. System will use APPE default signature.</pre>		

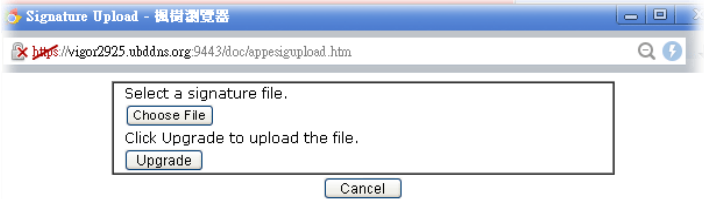
Upgrade Manually	Import
-------------------------	------------------------

Upgrade Automatically			
<input type="checkbox"/> Scheduled Update			
<input checked="" type="radio"/> Every:	1 (hour)	00 (minutes after the hour)	
<input type="radio"/> Daily:	0 (hour)	00 (minute)	
<input type="radio"/> Weekly:	Sunday (day)	0 (hour)	00 (minute)

[OK](#)

Available settings are explained as follows:

Item	Description
Upgrade Setting	<p>APPE Module Version - Display current version status of APPE signature.</p> <p>New version from the Internet - Download button is available only when Vigor router detects new APPE version. After clicking it, a dialog will appear with information added to such new version. Click OK to exit the dialog and start the signature upgrade.</p> <p>Upgrade via interface - Choose one of the WAN interfaces as a channel for APPE signature upgrade.</p>
Setup Download Server	<p>Specify the download server by typing the URL of the server located. Or you can click Find more link to search the one you want.</p> <p>Signature authentication/download message - Display the status of APPE Signature Upgrade.</p>

<p>Upgrade Manually</p>	<p>Import - Click this button to open the following page. Press Choose File to locate the signature file which downloaded from MyVigor portal or FTP server previously. Then, click Upgrade and wait for the system completing the process.</p> 
<p>Upgrade Automatically</p>	<p>Scheduled Update - Check the box to make Vigor router upgrading the APPE signature based on the schedule configured here.</p>

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

V-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.

CSM >> URL Content Filter Profile



URL Content Filter Profile Table:

[Set to Factory Default](#)

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

Administration Message (Max 255 characters)

[Preview](#)

Default Message

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

OK

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Profile	Display the number of the profile which allows you to click to set different policy.
Name	Display the name of the URL Content Filter Profile.
Administration Message	You can 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

Profile Index: 1

Profile Name:

Priority: **Log:**

1.URL Access Control

Enable URL Access Control Prevent web access from IP address

Action: Group/Object Selections:

Exception List

2.Web Feature

Enable Web Feature Restriction

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

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
Priority	<p>It determines the action that this router will apply.</p> <p>Both: Pass - The router will let all the packages that match with the conditions specified in URL Access Control and Web Feature below passing through. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.</p> <p>Both:Block -The router will block all the packages that match with the conditions specified in URL Access Control and Web Feature below. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.</p> <p>Either: URL Access Control First - When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for URL first, then Web feature second.</p> <p>Either: Web Feature First -When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for web feature first, then URL second.</p>

	<div data-bbox="707 203 1150 376"> <p>Both : Pass</p> <ul style="list-style-type: none"> Both : Pass Both : Block Either : URL Access Control First Either : Web Feature First </div>
<p>Log</p>	<p>None - There is no log file will be recorded for this profile. Pass - Only the log about Pass will be recorded in Syslog. Block - Only the log about Block will be recorded in Syslog. All - All the actions (Pass and Block) will be recorded in Syslog.</p> <div data-bbox="707 600 826 770"> <p>None</p> <ul style="list-style-type: none"> None Pass Block All </div>
<p>URL Access Control</p>	<p>Enable URL Access Control - Check the box to activate URL Access Control. Note that the priority for URL Access Control is higher than Restrict Web Feature. If the web content match the setting set in URL Access Control, the router will execute the action specified in this field and ignore the action specified under Restrict Web Feature.</p> <p>Prevent web access from IP address - Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control. You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.</p> <p>Action - This setting is available only when Either : URL Access Control First or Either : Web Feature First is selected.</p> <ul style="list-style-type: none"> ● <i>Pass</i> - Allow accessing into the corresponding webpage with the keywords listed on the box below. ● <i>Block</i> - Restrict accessing into the corresponding webpage with the keywords listed on the box below. If the web pages do not match with the keyword set here, it will be processed with reverse action. <p>Exception List - Specify the object profile(s) as the exception list which will be processed in an opposite manner to the action selected above.</p> <p>Group/Object Selections - The Vigor router provides several frames for users to define keywords and each frame supports multiple keywords. The keyword could be a noun, a partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or semicolon. In addition, the maximal length of each frame is 32-character long. After specifying keywords, the Vigor 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.</p>

Object/Group Edit

<u>Keyword Object</u>	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or <u>Keyword Group</u>	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None

OK Close

Web Feature

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

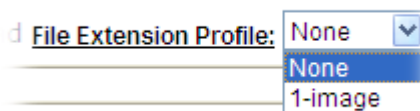
Action - This setting is available only when Either: URL Access Control First or Either: Web Feature First is selected.

Pass - Allow accessing into the corresponding webpage with the keywords listed on the box below.

Block - Restrict accessing into the corresponding webpage with the keywords listed on the box below.

If the web pages do not match with the specified feature set here, it will be processed with reverse action.

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



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

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

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

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

V-2-4 Web Content Filter Profile

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

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

However, if you use the **Web Content Filter Profile** page to activate WCF feature, it is necessary for you to access into the server (**MyVigor**) located on <http://myvigor.draytek.com>. Therefore, you need to register an account on <http://myvigor.draytek.com> for using corresponding service. Please refer to section of creating MyVigor account.

WCF adopts the mechanism developed and offered by certain service provider (e.g., DrayTek). No matter activating WCF feature or getting a new license for web content filter, you have to click **Activate** to satisfy your request. Be aware that service provider matching with Vigor router currently offers a period of time for trial version for users to experiment. If you want to purchase a formal edition, simply contact with the channel partner or your dealer.

Click **CSM** and click **Web Content Filter Profile** to open the profile setting page. The default setting for Setup Query Server /Setup Test Server is **auto-selected**. You can choose another server for your necessity by clicking **Find more** to open <http://myvigor.draytek.com> for searching another qualified and suitable one.



Info 1

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

Info 2

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



Web-Filter License

[Activate](#)

[Status: **Not Activated**]

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

Web Content Filter Profile Table:

[Set to Factory Default](#)

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

Cache :

Administration Message (Max 255 characters)

[Default Message](#)

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

Legend:

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

[OK](#)

Available settings are explained as follows:

Item	Description
Activate	Click it to access into MyVigor for activating WCF service.
Setup Query Server	It is recommended for you to use the default setting, auto-selected. You need to specify a server for categorize searching when you type URL in browser based on the web content filter profile.
Setup Test Server	It is recommended for you to use the default setting, auto-selected.
Find more	Click it to open http://myvigor.draytek.com for searching another qualified and suitable server.
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 .
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.

CSM >> Web Content Filter Profile

Profile Index: 1
 Profile Name: Log:

Black/White List

Enable

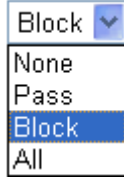
Action:

Action:

Groups	Categories		
Child Protection <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input checked="" type="checkbox"/> Alcohol & Tobacco <input checked="" type="checkbox"/> Hate & Intolerance <input checked="" type="checkbox"/> Porn & Sexually <input checked="" type="checkbox"/> School Cheating	<input checked="" type="checkbox"/> Criminal Activity <input checked="" type="checkbox"/> Illegal Drug <input checked="" type="checkbox"/> Violence <input checked="" type="checkbox"/> Sex Education	<input checked="" type="checkbox"/> Gambling <input checked="" type="checkbox"/> Nudity <input checked="" type="checkbox"/> Weapons <input checked="" type="checkbox"/> Tasteless
	<input type="checkbox"/> News <input type="checkbox"/> Politics <input type="checkbox"/> Restaurants & Dining <input type="checkbox"/> General <input type="checkbox"/> Image Sharing <input type="checkbox"/> Private IP Addresses	<input type="checkbox"/> Non-profits & NGOs <input type="checkbox"/> Real Estate <input type="checkbox"/> Shopping <input type="checkbox"/> Cults <input type="checkbox"/> Network Errors <input type="checkbox"/> Uncategorized Sites	<input type="checkbox"/> Personal Sites <input type="checkbox"/> Religion <input type="checkbox"/> Translators <input type="checkbox"/> Greeting cards <input type="checkbox"/> Parked Domains

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.
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.

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

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

V-2-5 DNS Filter Profile

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

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



Info

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

CSM >> DNS Filter

DNS Filter Profile Table

[Set to Factory Default](#)

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

DNS Filter Local Setting

DNS Filter	<input checked="" type="checkbox"/> Enable	
Syslog	Pass	
WCF	WCF-1 Default	
UCF	None	
Black/White List	<input type="checkbox"/> Enable	Blacklist
	Address Type	Any Address
	Start IP Address	0.0.0.0
	End IP Address	0.0.0.0
	Subnet Mask	0.0.0.0
	IP Group	None
	or IP Group	None
	or IP Object	None
	or IP Object	None

Administration Message (Max 255 characters)

[Default Message](#)

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

Legend:

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

OK Cancel

Available settings are explained as follows:

Item	Description
<p>DNS Filter Profile Table</p>	<p>It displays a list of different DNS filter profiles (with specified WCF and UCF).</p> <p>Click the profile link to open the following page. Then, type the name of the profile and specify WCF/UCF based on your requirement.</p> <p>CSM >> DNS Filter</p> <hr/> <p>Index No. 1</p> <div style="border: 1px solid black; padding: 5px;"> <p>Profile Name <input type="text"/></p> <p>Syslog <input type="button" value="None"/> ▾</p> <p>WCF <input type="button" value="None"/> ▾</p> <p>UCF <input type="button" value="None"/> ▾</p> </div> <p style="text-align: center;"> <input type="button" value="OK"/> <input type="button" value="Clear"/> <input type="button" value="Cancel"/> </p>
<p>DNS Filter Local Setting</p>	<p>DNS Filter Local Setting will be applied to DNS query from clients on LAN when router's DNS server is used.</p> <p>DNS Filter - Check Enable to enable such feature.</p> <p>Syslog - The filtering result can be recorded according to the setting selected for Syslog.</p> <ul style="list-style-type: none"> ● None - There is no log file will be recorded for this profile. ● Pass - Only the log about Pass will be recorded in Syslog. ● Block - Only the log about Block will be recorded in Syslog. ● All - All the actions (Pass and Block) will be recorded in Syslog. <p>WCF- Set the filtering conditions.</p> <p>UCF - Set the filtering conditions.</p> <p>Black/White List - Specify IP address, subnet mask, IP object, or IP group as a black list or white list for DNS packets passing through or blocked by Vigor router.</p>
<p>Administration Message</p>	<p>When DNS packets are blocked by DNS filter, a web page containing the description listed on Administration Message will be shown on the screen.</p> <p>Type the words or sentences which will be displayed when a web page is blocked by Vigor router. 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.</p>

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.

CSM >> Web Content Filter Profile



Web-Filter License
[Status:Not Activated]

Activate

Setup Query Server	auto-selected	Find more
Setup Test Server	auto-selected	Find more

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

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

Administration Message (Max 255)

[Preview!](#)

Cache :

Or

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

System Maintenance >> Activation

Activate via interface : auto-selected ▼

Web-Filter License
[Status:Not Activated]

Activate

Authentication Message

Note: If you want to use email alert or syslog, please configure the [SysLog/Mail Alert Setup](#) page.

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



LOGIN

UserName :

Password :

Auth Code : t xxhdd

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

[Forgotten password?](#)

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

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

3. Click the link of **Create an account now**.
4. Check to confirm that you accept the **Agreement** and click **Accept**.

Register

Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 Completion

===== MyVigor Agreement =====

1. Agreement

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

2. Registration

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

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

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

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

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

Register

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

1 Agreement

2 Personal Information

3 Preferences

4 Completion

Account Information

UserName:*
(3 - 20 characters)

Password:*
(4 - 20 characters : Do not set the same as the username.)

Confirm Password:*

Personal Information

First Name:*

Last Name:*

Company Name:

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

Tel: -

Country:*

Career:*

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

Register

Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 Completion

How did you find out about this website?

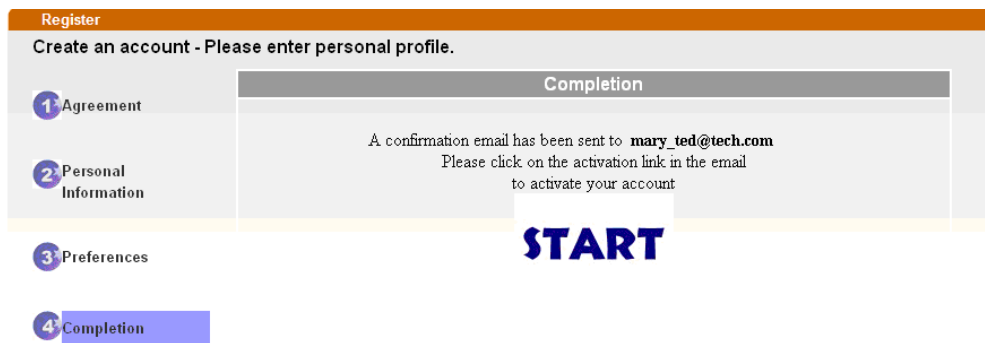
What kind of anti-virus do you use?

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

I would like to receive DrayTek product news.

Please select the mail server for receiving the verification mail.

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



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

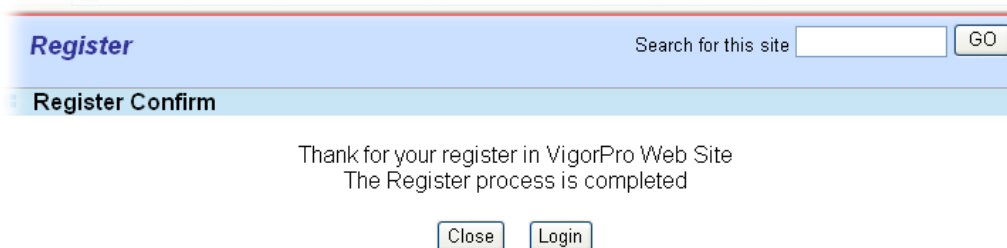
***** This is an automated message from myvigor.draytek.com.*****

Thank you (**Mary**) for creating an account.

Please click on the activation link below to activate your account

Link : [Activate my Account](#)

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



- When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**.



LOGIN

UserName :

Password :

Auth Code : **T4he1C**

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

[Forgotten password?](#)

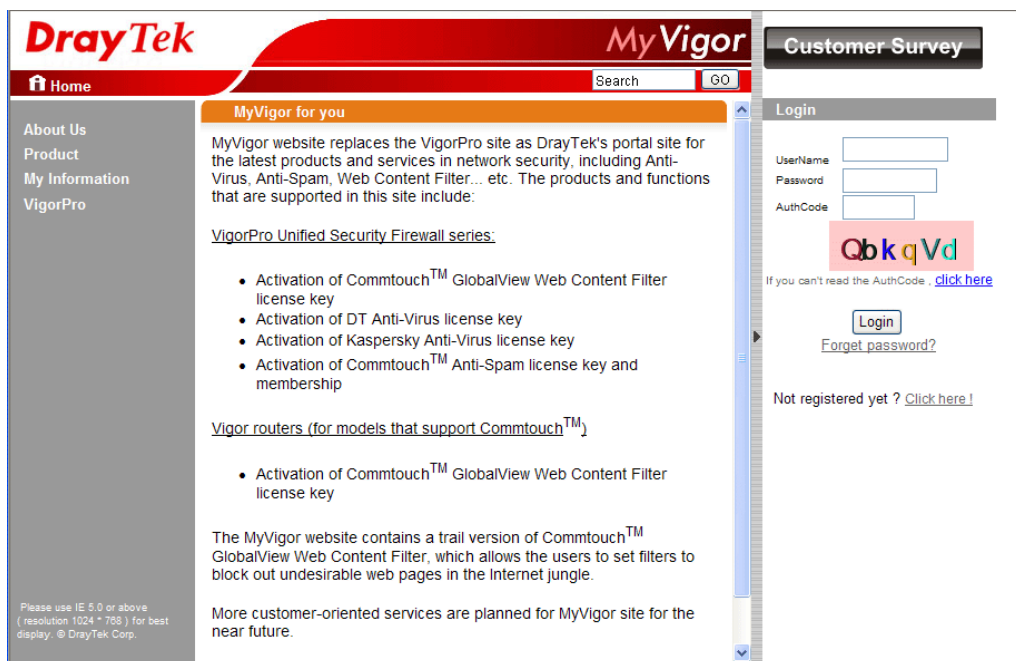
Don't have a MyVigor Account ? [Create an account now](#)

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

- 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

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



The screenshot shows the MyVigor website interface. At the top, there is a navigation bar with the DrayTek logo, a search bar, and a 'Customer Survey' button. Below the navigation bar, there is a 'MyVigor for you' section with a list of services and a 'Login' form. The login form includes fields for 'UserName', 'Password', and 'AuthCode', along with a 'Login' button and a 'Forget password?' link. A CAPTCHA image with the code 'QbkqVd' is displayed above the login form. The 'AuthCode' field in the login form contains the value 'T4he1C'. The website also features a sidebar with navigation links and a footer with technical information.

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

Register

Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 Completion

MyVigor Agreement

1. Agreement

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

2. Registration

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

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

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

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

<< Back Accept >>

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

Register

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

1 Agreement

2 Personal Information

3 Preferences

4 Completion

Account Information

UserName:* Mary Check Account

(3 - 20 characters)

Password:* ●●●●

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

Confirm Password:* ●●●●

Personal Information

First Name:* Mary

Last Name:* Ted

Company Name: Tech Ltd.

Email Address:* mary_ted@tech.com

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

Tel: 0 -

Country:* SWITZERLAND

Career:* Supervisor

<< Back Continue >>

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

Register

Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 Completion

How did you find out about this website? Internet

What kind of anti-virus do you use? AntiVir

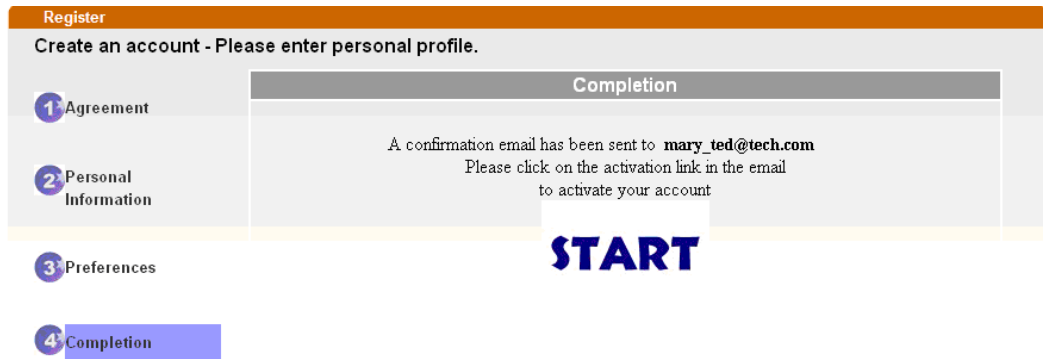
I would like to subscribe to the MyVigor e-letter.

I would like to receive DrayTek product news.

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

<< Back Continue >>

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



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

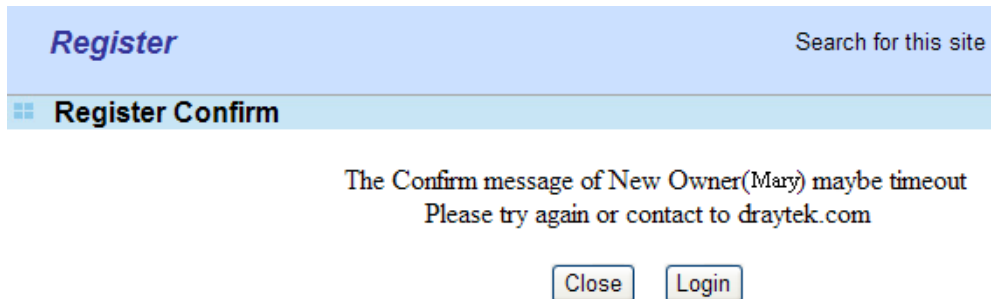
***** This is an automated message from myvigor.draytek.com.*****

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**.



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.



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!

LOGIN

UserName :

Password :

Auth Code : **T4he1C**

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

[Forgotten password?](#)

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

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

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

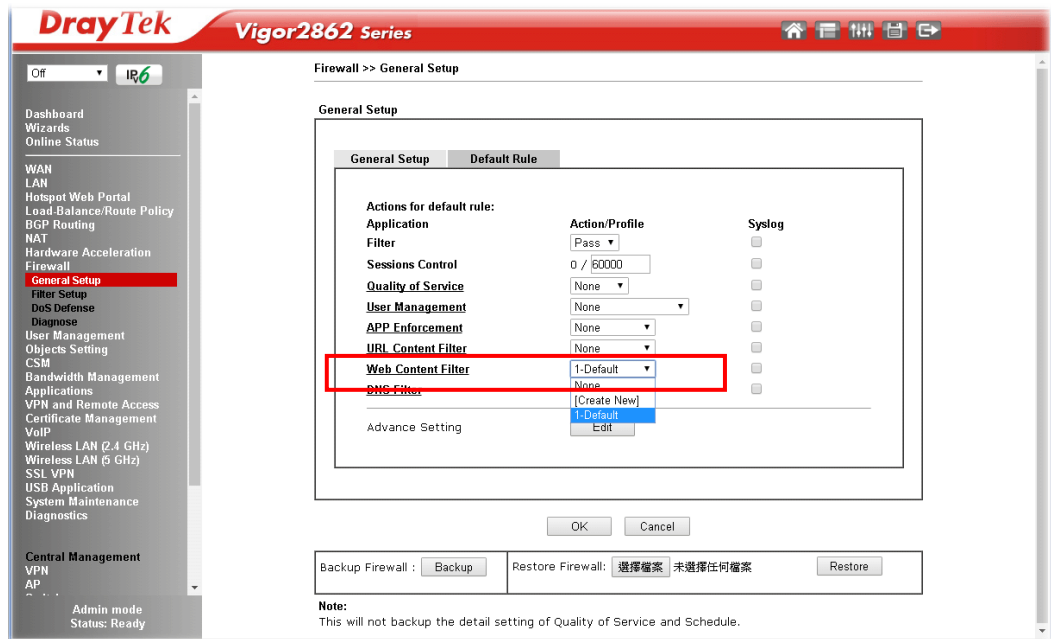
1. Make sure the Web Content Filter (powered by Commtouch) license is valid.



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.

Objects Setting >> Keyword Object Setup

Profile Index : 1

Name	Facebook
Contents	facebook

Limit of Contents: Max 3 Words and 63 Characters.
Each word should be separated by a single space.

You can replace a character with %HEX.
Example:
Contents: backdoo%72 virus keep%20out

Result:
1. backdoor
2. virus
3. keep out

OK Clear Cancel

3. Open CSM>>URL Content Filter Profile. Click an index number to open the setting page.
4. Configure the settings as the following figure.

CSM >> URL Content Filter Profile

Profile Index: 1

Profile Name: Facebook

Priority: Either : URL Access Control First Log: None

1.URL Access Control

Enable URL Access Control Prevent web access from IP address

Action: Block Group/Object Selections: Facebook Edit

2.Web Feature

Enable Restrict Web Feature

Action: Pass Cookie Proxy Upload File Extension Profile: None

OK Clear Cancel

5. When you finished the above steps, click OK. Then, open Firewall>>General Setup.

- Click the **Default Rule** tab. Choose the profile just configured from the drop down list in the field of **URL Content Filter**. Now, users cannot open any web page with the word "facebook" inside.

Firewall >> General Setup

General Setup

General Setup Default Rule

Actions for default rule:	Action/Profile	Syslog
Application	Pass	<input type="checkbox"/>
Filter	0 / 60000	<input type="checkbox"/>
Sessions Control	None	<input type="checkbox"/>
Quality of Service	Auto-Select	<input type="checkbox"/>
Load-Balance policy	None	<input type="checkbox"/>
User Management	None	<input type="checkbox"/>
APP Enforcement	None	<input type="checkbox"/>
URL Content Filter	1-Facebook	<input type="checkbox"/>
Web Content Filter	None	<input type="checkbox"/>

Advance Setting Edit

B. Disallow users to play games on Facebook

- Open **Object Settings>>Keyword Object**. Click an index number to open the setting page.
- In the field of **Contents**, please type *apps.facebook*. Configure the settings as the following figure.

Objects Setting >> Keyword Object Setup

Profile Index : 2

Name	facebook-apps
Contents	apps.facebook

Limit of Contents: Max 3 Words and 63 Characters.
Each word should be separated by a single space.

You can replace a character with %HEX.
Example:
Contents: backdoo%72 virus keep%20out

Result:

- backdoor
- virus
- keep out

OK Clear Cancel

- Open CSM>>URL Content Filter Profile. Click an index number to open the setting page.
- Configure the settings as the following figure.

CSM >> URL Content Filter Profile

Profile Index: 2

Profile Name:

Priority: Log:

1.URL Access Control

Enable URL Access Control Prevent web access from IP address

Action: Group/Object Selections:

2.Web Feature

Enable Restrict Web Feature

Action: Cookie Proxy Upload File Extension Profile:

- When you finished the above steps, please open Firewall>>General Setup.
- Click the **Default Rule** tab. Choose the profile just configured from the drop down list in the field of URL Content Filter. Now, users cannot open any web page with the word "facebook" inside.

Firewall >> General Setup

General Setup

Actions for default rule:	Action/Profile	Syslog
Application	<input type="text" value="Pass"/>	<input type="checkbox"/>
Filter	<input type="text" value="0 / 60000"/>	<input type="checkbox"/>
Sessions Control	<input type="text" value="None"/>	<input type="checkbox"/>
Quality of Service	<input type="text" value="Auto-Select"/>	<input type="checkbox"/>
Load-Balance policy	<input type="text" value="None"/>	<input type="checkbox"/>
User Management	<input type="text" value="None"/>	<input type="checkbox"/>
APP Enforcement	<input type="text" value="None"/>	<input type="checkbox"/>
URL Content Filter	<input type="text" value="2-face.apps"/>	<input type="checkbox"/>
Web Content Filter	<input type="text" value="None"/>	<input type="checkbox"/>

Advance Setting

This page is left blank.

Part VI Management



System
Maintenance



Bandwidth
Management



User
Management

There are several items offered for the Vigor router system setup: System Status, TR-069, Administrator Password, User Password, Login Page Greeting, Configuration Backup, Syslog /Mail Alert, Time and Date, Management, Reboot System, Firmware Upgrade and Activation.

It is used to control the bandwidth of data transmission through configuration of Sessions Limit, Bandwidth Limit, and Quality of Service (QoS).

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.

VI-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, Activation, Internal Service User List and Dashboard Control.

Below shows the menu items for System Maintenance.



Web User Interface

VI-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 : Vigor2862ac
Firmware Version : 3.8.7_RC3_STD
Build Date/Time : Sep 29 2017 14:06:14

LAN					
	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-1D-AA-5D-C9-E0	192.168.1.1	255.255.255.0	OFF	8.8.8.8
LAN2	00-1D-AA-5D-C9-E0	192.168.2.1	255.255.255.0	ON	8.8.8.8
LAN3	00-1D-AA-5D-C9-E0	192.168.3.1	255.255.255.0	ON	8.8.8.8
LAN4	00-1D-AA-5D-C9-E0	192.168.4.1	255.255.255.0	ON	8.8.8.8
LAN5	00-1D-AA-5D-C9-E0	192.168.5.1	255.255.255.0	ON	8.8.8.8
LAN6	00-1D-AA-5D-C9-E0	192.168.6.1	255.255.255.0	ON	8.8.8.8
LAN7	00-1D-AA-5D-C9-E0	192.168.7.1	255.255.255.0	ON	8.8.8.8
LAN8	00-1D-AA-5D-C9-E0	192.168.8.1	255.255.255.0	ON	8.8.8.8
DMZ PORT	00-1D-AA-5D-C9-E0	192.168.17.1	255.255.255.0	ON	8.8.8.8
IP Routed Subnet	00-1D-AA-5D-C9-E0	192.168.0.1	255.255.255.0	ON	8.8.8.8

Wireless LAN(2.4GHz)			
MAC Address	Frequency Domain	Firmware Version	SSID
00-1D-AA-5D-C9-E0	Europe	3.3	DrayTek

Wireless LAN(5GHz)			
MAC Address	Frequency Domain	Firmware Version	SSID
00-1D-AA-5D-C9-E2	Europe	10.4-2.4.3.1008	DrayTek_5G

WAN					
	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Disconnected	00-1D-AA-5D-C9-E1	PPPoE	---	---
WAN2	Disconnected	00-1D-AA-5D-C9-E2	DHCP Client	---	---
WAN3	Disconnected	00-1D-AA-5D-C9-E3	---	---	---
WAN4	Disconnected	00-1D-AA-5D-C9-E4	---	---	---

IPv6		
Address	Scope	Internet Access Mode
LAN FE80::21D:AFF:FE5D:C9E0/64	Link	---

Available settings are explained as follows:

Item	Description
Model Name	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
Build Date/Time	Display the date and time of the current firmware build.
LAN	MAC Address - Display the MAC address of the LAN Interface. IP Address - Display the IP address of the LAN interface. Subnet Mask - Display the subnet mask address of the LAN interface. DHCP Server

	<ul style="list-style-type: none"> - Display the current status of DHCP server of the LAN interface <p>DNS</p> <ul style="list-style-type: none"> - Display the assigned IP address of the primary DNS.
WAN	<p>Link Status</p> <ul style="list-style-type: none"> - Display current connection status. <p>MAC Address</p> <ul style="list-style-type: none"> - Display the MAC address of the WAN Interface. <p>Connection</p> <ul style="list-style-type: none"> - Display the connection type. <p>IP Address</p> <ul style="list-style-type: none"> - Display the IP address of the WAN interface. <p>Default Gateway</p> <ul style="list-style-type: none"> - Display the assigned IP address of the default gateway.
IPv6	<p>Address - Display the IPv6 address for LAN.</p> <p>Scope - Display the scope of IPv6 address. For example, IPv6 Link Local could only be used for direct IPv6 link. It can't be used for IPv6 internet.</p> <p>Internet Access Mode - Display the connection mode chosen for accessing into Internet.</p>

VI-1-2 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through an Auto Configuration Server, e.g., VigorACS.

System Maintenance >> TR-069 Setting

ACS and CPE Settings	Export Parameters																
Tr069 <input checked="" type="radio"/> Disable <input type="radio"/> Enable ACS Server On <input type="text" value="Internet"/>																	
ACS Server URL <input type="text"/> <input type="button" value="Wizard"/> <input type="checkbox"/> Acquire URL from DHCP option 43 Username <input type="text"/> Password <input type="text"/> <input type="button" value="Test With Inform"/> Event Code <input type="text" value="PERIODIC"/>																	
Last Inform Response Time :(NA) ●																	
CPE Client <input checked="" type="radio"/> Http <input type="radio"/> Https URL <input type="text"/> Port <input type="text" value="8069"/> Username <input type="text" value="vigor"/> Password <input type="text" value="*****"/>																	
Periodic Inform Settings <input checked="" type="radio"/> Disable <input type="radio"/> Enable Interval Time <input type="text" value="900"/> second(s)																	
STUN Settings <input checked="" type="radio"/> Disable <input type="radio"/> Enable Server Address <input type="text"/> Server Port <input type="text" value="3478"/> Minimum Keep Alive Period <input type="text" value="60"/> second(s) Maximum Keep Alive Period <input type="text" value="-1"/> second(s)																	
Apply Settings to APs <input checked="" type="radio"/> Disable <input type="radio"/> Enable AP Password <input type="text"/> <input type="checkbox"/> Apply Specific STUN Settings to APs																	
Bandwidth Utilisation Notification Settings <input checked="" type="radio"/> Disable <input type="radio"/> Enable Time Period <input type="text" value="15 mins"/>																	
<p>Note: Please turn off Hardware Acceleration in the router to receive Alerts Notifications, and accuracy of Bandwidth data.</p> <table border="1"> <thead> <tr> <th></th> <th>WAN</th> <th>Threshold Level</th> <th>Line Speed</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>WAN1</td> <td>Medium <input type="text" value="0"/> % High <input type="text" value="0"/> % of TX: <input type="text" value="N/A"/> Mbps RX: <input type="text" value="N/A"/> Mbps</td> <td></td> </tr> <tr> <td><input type="checkbox"/></td> <td>WAN2</td> <td>Medium <input type="text" value="0"/> % High <input type="text" value="0"/> % of TX: <input type="text" value="0"/> Mbps RX: <input type="text" value="0"/> Mbps</td> <td></td> </tr> <tr> <td><input type="checkbox"/></td> <td>WAN3</td> <td>Medium <input type="text" value="0"/> % High <input type="text" value="0"/> % of TX: <input type="text" value="0"/> Mbps RX: <input type="text" value="0"/> Mbps</td> <td></td> </tr> </tbody> </table>			WAN	Threshold Level	Line Speed	<input type="checkbox"/>	WAN1	Medium <input type="text" value="0"/> % High <input type="text" value="0"/> % of TX: <input type="text" value="N/A"/> Mbps RX: <input type="text" value="N/A"/> Mbps		<input type="checkbox"/>	WAN2	Medium <input type="text" value="0"/> % High <input type="text" value="0"/> % of TX: <input type="text" value="0"/> Mbps RX: <input type="text" value="0"/> Mbps		<input type="checkbox"/>	WAN3	Medium <input type="text" value="0"/> % High <input type="text" value="0"/> % of TX: <input type="text" value="0"/> Mbps RX: <input type="text" value="0"/> Mbps	
	WAN	Threshold Level	Line Speed														
<input type="checkbox"/>	WAN1	Medium <input type="text" value="0"/> % High <input type="text" value="0"/> % of TX: <input type="text" value="N/A"/> Mbps RX: <input type="text" value="N/A"/> Mbps															
<input type="checkbox"/>	WAN2	Medium <input type="text" value="0"/> % High <input type="text" value="0"/> % of TX: <input type="text" value="0"/> Mbps RX: <input type="text" value="0"/> Mbps															
<input type="checkbox"/>	WAN3	Medium <input type="text" value="0"/> % High <input type="text" value="0"/> % of TX: <input type="text" value="0"/> Mbps RX: <input type="text" value="0"/> Mbps															

Note: If "Apply Specific STUN Settings to APs" is enabled, router STUN Settings would be discarded.

Available settings are explained as follows:

Item	Description
Tr069	Click Enable to activate the settings on this page.
ACS Server On	Choose the interface for the router connecting to ACS server.
ACS Server	<p>URL/Username/Password - Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information.</p> <p>Wizard - Click it to enter the IP address of VigorACS server, port number and the handler.</p> <p>Test With Inform - Click it to send a message based on the event code selection to test if such CPE is able to communicate with VigorACS SI server.</p> <p>Event Code - Use the drop down menu to specify an event to perform the test.</p> <p>Last Inform Response Time - Display the time that VigorACS server made a response while receiving Inform message from CPE last time.</p>
CPE Client	<p>Such information is useful for Auto Configuration Server.</p> <p>Enable/Disable - Allow/Deny the CPE Client to connect with Auto Configuration Server.</p> <p>Port - Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE.</p> <p>Username and Password - Type the username and password that VigorACS can use to access into such CPE.</p>
Periodic Inform Settings	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	<p>The default is Disable. If you click Enable, please type the relational settings listed below:</p> <p>Server IP - Type the IP address of the STUN server.</p> <p>Server Port - Type the port number of the STUN server.</p> <p>Minimum Keep Alive Period - If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds".</p> <p>Maximum Keep Alive Period - If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.</p>
Apply Settings to APs	<p>This feature is able to apply TR-069 settings (including STUN and ACS server settings) to all of APs managed by Vigor2862 at the same time.</p> <p>Disable - Related settings will not be applied to VigorAP.</p> <p>Enable - Above STUN settings will be applied to VigorAP after clicking OK. If such feature is enabled, you have to type the password for accessing VigorAP.</p> <ul style="list-style-type: none"> ● AP Password - Type the password of the VigorAP that you want to apply Vigor2862's TR-069 settings. <p>Apply Specific STUN Settings to APs - After clicking the Enable radio button for Apply Settings to APs, if you want to</p>

	<p>apply specific STUN settings (not the STUN Settings configured for Vigor2862) to VigorAPs to meet specific requirements, simply check this box. Then, type the server IP address, server port, minimum keep alive period and maximum keep alive period respectively.</p>
<p>Bandwidth Utilisation Notification Settings</p>	<p>To administrator, this feature is useful to monitor the bandwidth utilization of CPE(s). When the bandwidth used is over the threshold level (percentage defined in medium and high fields), a notification will be sent to VigorACS. After a long time observation, the administrator can determine if it is necessary to increase the bandwidth setting for that CPE or not.</p> <p>Enable - Click it to enable such feature.</p> <p>Time Period - Choose the time interval (15 mins, 30 mins, 1hour, 3 hours, or 6 hours) for CPE to send a notification of bandwidth utilization to VigorACS.</p> <p>WAN - Choose the WAN interface for applying the bandwidth utilization notification mechanism.</p> <p>Threshold Level - Set the percentage of bandwidth in transmission and receiving data as threshold values for CPE to detect bandwidth utilization.</p> <p>Line Speed - Set the transmission rate and receiving rate for specified WAN interface.</p>

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

VI-1-3 Administrator Password

This page allows you to set new password.

System Maintenance >> Administrator Password Setup

Administrator Password

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

Note:

Password can contain only a-z A-Z 0-9 , ; : . " < > * + = | ? @ # ^ ! ()

Administrator Local User

<input type="checkbox"/> Local User				
Local User List				
<table border="1"> <thead> <tr> <th>Index</th> <th>User Name</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Index	User Name		
Index	User Name			
Specific User				
User Name: <input type="text"/>				
Password: <input type="text"/> Confirm Password: <input type="text"/>				
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				
<input checked="" type="checkbox"/> Enable 'admin' account log into Web UI from the Internet				

Administrator LDAP Setting

<input type="checkbox"/> Enable LDAP/AD login for admin users
<input checked="" type="checkbox"/> Enable 'admin' account log in from the Internet
LDAP Server Profiles Setup

Note:

If Local User is enabled, you will need to select 'admin' group when log into Web UI.

Available settings are explained as follows:

Item	Description
Administrator Password	<p>Old Password - Type in the old password. The factory default setting for password is "admin".</p> <p>New Password - Type in new password in this field. The length of the password is limited to 23 characters.</p> <p>Confirm Password - Type in the new password again.</p>
Administrator Local User	<p>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.</p> <p>Local User - Check the box to enable the local user configuration.</p>

	<p>Local User List - It displays the username of the local user.</p> <p>User Name - Give a user name for the local user.</p> <p>Password - Type the password for the local user.</p> <p>Confirm Password - Type the password again for confirmation.</p> <p>Add - After typing the user name and password above, simply click it to create a new local user. The new one will be shown on the Local User List immediately.</p> <p>Edit - If the username listed on the box above is not satisfied, simply click the username and modify it on the field of User Name. Later, click Edit to update the information.</p> <p>Delete - If the local user listed on the box above is not satisfied, simply click the username and click Delete to remove it.</p>
<p>Administrator LDAP Setting</p>	<p>Enable LDAP/AD login for Admin users - If it is enabled, any user can access into the web user interface of Vigor router through the LDAP server authentication.</p> <p>Enable 'admin' account login to Web UI from the Internet - The default setting is enabled. It can ensure any user accessing into web user interface of Vigor router through Internet by username/password of "admin/admin".</p> <p>LDAP Server Profiles - Available profiles will be displayed here under the link of LDAP Profile Setup.</p> <p>LDAP Profile Setup - It allows you to create a new LDAP profile.</p>

When you click OK, the login window will appear. Please use the new password to access into the web user interface again.

VI-1-4 User Password

This page allows you to set new password for user operation.

System Maintenance >> User Password

Enable User Mode for simple web configuration

User Password

| [Set to Factory Default](#) |

Password	<input type="text"/>
Confirm Password	<input type="text"/> (Max. 23 characters allowed)
Password Strength:	<input type="button" value="Weak"/> <input type="button" value="Medium"/> <input type="button" value="Strong"/>
Strong password requirements:	
1. Have at least one upper-case letter and one lower-case letter.	
2. Including non-alphanumeric characters is a plus.	

Note:

1. Password can contain a-z A-Z 0-9 , ; : . " < > * + = | ? @ # ^ ! ()
2. Password can't be all asterisks(*). For example, '*' or '****' is illegal, but '123*' or '*45' is OK.

Available settings are explained as follows:

Item	Description
Enable User Mode for simple web configuration	After checking this box, you can access into the web user interface with the password typed here for simple web configuration. The settings on simple web user interface will be different with full web user interface accessed by using the administrator password.
Password	Type in new password in this field. The length of the password is limited to 31 characters.
Confirm Password	Type in the new password again.
Password Strength	Display the security strength of the password specified above.
Set to Factory Default	Click to return to the factory default setting.

When you click OK, the login window will appear. Please use the new password to access into the web user interface again. Below shows an example for accessing into User Operation with User Password.

1. Open System Maintenance>>User Password.
2. Check the box of **Enable User Mode for simple web configuration** to enable user mode operation. Type a new password in the field of New Password and click **OK**.

System Maintenance >> User Password

Enable User Mode for simple web configuration

User Password

[Set to Factory Default](#)

Password	<input type="password"/>	
Confirm Password	<input type="password"/>	(Max. 23 characters allowed)
Password Strength:	Weak Medium Strong	
Strong password requirements:		
1. Have at least one upper-case letter and one lower-case letter.		
2. Including non-alphanumeric characters is a plus.		

Note:

1. Password can contain a-z A-Z 0-9 , ; : . " < > * + = | ? @ # ^ ! ()
2. Password can't be all asterisks(*). For example, '*' or '****' is illegal, but '123*' or '*45' is OK.

OK

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 field of Password and click Login.

6. The main screen with User Mode will be shown as follows.

The screenshot displays the DrayTek Vigor2862 Series User Mode main screen. The interface is divided into several sections:

- System Information:**

Model Name	Vigor2862ac	System Up Time	170:35:19
Router Name	DrayTek	Current Time	2000 Jan 8 Sat 2:34:26
Firmware Version	3.8.5_RC5a	Build Date/Time	Jan 20 2017 05:48:56
DSL Version	07-07-02-08-00-01	LAN MAC Address	00-1D-AA-F7-C0-F0
- IPv4 LAN Information:**

LAN	IP Address	DHCP	IP Address	DHCP
LAN1	192.168.1.1/24	v	192.168.2.1/24	v
LAN3	192.168.3.1/24	v	192.168.4.1/24	v
LAN5	192.168.5.1/24	v	192.168.6.1/24	v
LAN7	192.168.7.1/24	v	192.168.8.1/24	v
DMZ PORT	192.168.17.1/24	v	IP Routed Subnet	192.168.0.1/24
- IPv4 Internet Access:**

WAN	Line / Mode	IP Address	MAC Address	Up Time
WAN1	ADSL / PPPoA	Disconnected	00-1D-AA-F7-C0-F1	00:00:00
WAN2	Ethernet / DHCP Client	Disconnected	00-1D-AA-F7-C0-F2	00:00:00
WAN3	USB / ---	Disconnected	00-1D-AA-F7-C0-F3	00:00:00
WAN4	USB / ---	Disconnected	00-1D-AA-F7-C0-F4	00:00:00
- Interface:**

DSL	Connected : Down Stream : 0Kbps / Up Stream : 0Kbps
WAN	Connected : 0, <input type="radio"/> WAN1 <input type="radio"/> WAN2 <input type="radio"/> WAN3 <input type="radio"/> WAN4
LAN	Connected : 0, <input type="radio"/> Port1 <input checked="" type="radio"/> Port2 <input type="radio"/> Port3 <input type="radio"/> Port4
WLAN	Connected : 0
WLAN5G	Connected : 0

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.

VI-1-5 Login Page Greeting

When you want to access into the web user interface of Vigor router, the system will ask you to offer username and password first. At that moment, the background of the web page is blank and no heading will be displayed on the Login window. This page allows you to specify login URL and the heading on the Login window if you have such requirement.

System Maintenance >> Login Page Greeting

Login Page Greeting

Enable

Login Page Title (31 char max.)

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

```
<h1><b><font color=red>Welcome Message</font></b></h1><p>This welcome message is displayed in the Login page of the router. Replace this text with your own message. </p><ol><li>The welcome message can be written in HTML so lists such as this one can be created </li><li>Other markup tags such as p, font or img can be used</li></ol>
```

Examples of Welcome Message and Bulletin:
<h1>Welcome Message</h1>
<p>Message</p>

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable the login customization function.
Login Page Title	Type a brief description (e.g., Welcome to DrayTek) which will be shown on the heading of the login dialog.
Welcome Message and Bulletin	Type words or sentences here. It will be displayed for bulletin message. In addition, it can be displayed on the login dialog at the bottom. Note that do not type URL redirect link here.
Preview	Click it to display the preview of the login window based on the settings on this web page.
Set to Factory Default	Click to return to the factory default setting.

Below shows an example of login customization with the information typed in Login Description and Bulletin.



The screenshot displays the login interface for the DrayTek Vigor2862 Series. At the top, the DrayTek logo is on the left and 'Vigor2862 Series' is on the right, both in white text on a red background. Below this, a black bar contains the word 'Login' in white. Underneath, the text 'Just for Carrie' is centered. The login form includes two input fields: 'Username' and 'Password', each with a corresponding label to its left. A 'Login' button is positioned below the password field. At the bottom of the form area, the copyright notice 'Copyright © 2000-2017 DrayTek Corp. All Rights Reserved.' is visible.

Welcome Message

This welcome message is displayed in the Login page of the router. Replace this text with your own message.

1. The welcome message can be written in HTML, so lists such as this one can be created
2. Other markup tags such as p, font or img can be used

VI-1-6 Configuration Backup

Such function can be used to apply the router settings configured by Vigor2820/ Vigor2830/ Vigor2850 to Vigor2862.

Backup the Configuration

Follow the steps below to backup your configuration.

1. Go to **System Maintenance >> Configuration Backup**. The following page will be popped-up, as shown below.

System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restore
Restore settings from a configuration file.

選擇檔案 未選擇檔案

USB Storage

Restore configuration except the login password.

Note:
This will work only if the selected configuration file was created from this device.

Backup
Back up the current settings into a configuration file.

Protect with password

Auto Backup to USB storage

Enable

Backup folder

Periodicity backup
Cycle duration: days and hours

Backup after change configuration

Note:

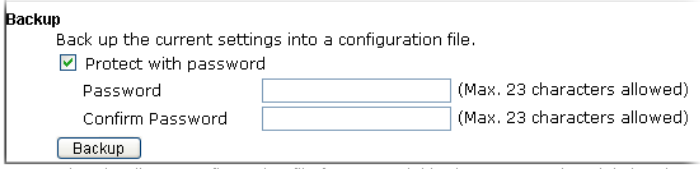
1. When loading a configuration file from a model in the Supported Model List please note that features and functionality can vary between models so please manually verify the settings after the restoration.
2. Auto backup to USB: if settings do not change, configuration doesn't backup.
3. Auto backup to USB: if configuration backup multiple times in one hour, the old file will be overwritten with the same filename.

Supported Model List

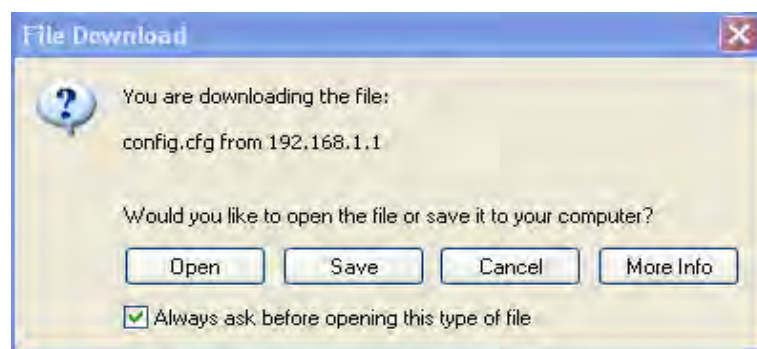
Model	Firmware Version
Vigor2860	3.8.5, or later

Available settings are explained as follows:

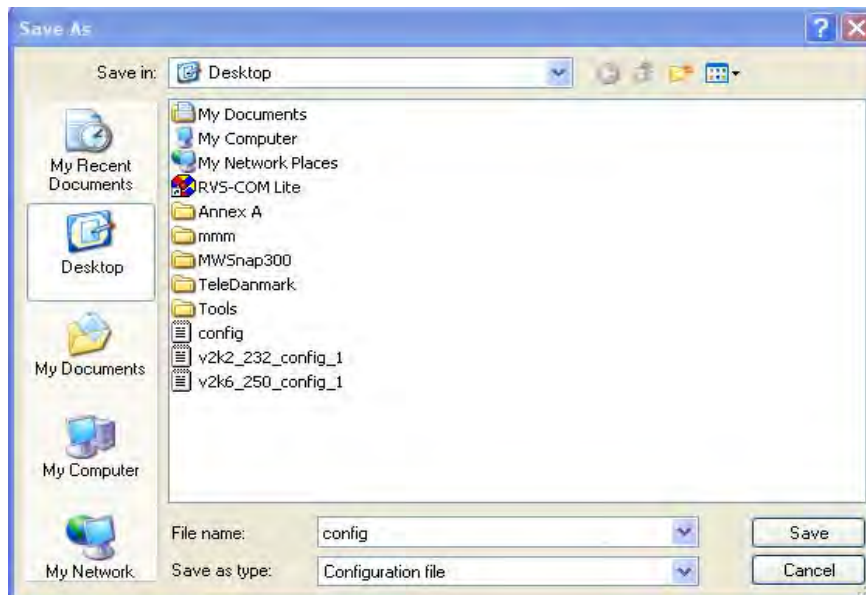
Item	Description
Restore	<p>Choose File /USB Storage - Click it to specify a file to be restored.</p> <p>Restore configuration except the login password - If the password settings shall not be restored and applied to Vigor2862, simply check this box to get rid of password settings.</p> <p>Click Restore to restore the configuration. If the file is</p>

	encrypted, the system will ask you to type the password to decrypt the configuration file.
Backup	<p>Click it to perform the configuration backup of this router.</p> <p>Protect with password- For the sake of security, the configuration file for the router can be encrypted.</p>  <p><small>Note: When loading a configuration file from a model in the Supported Model List please</small></p> <ul style="list-style-type: none"> ● Password - Type several characters as the password for encrypting the configuration file. ● Confirm Password - Type the password again for confirmation.
Auto Backup to USB storage	<p>The configuration can be stored to a USB connecting to Vigor router as a backup.</p> <p>Backup folder - Set the path for downloading.</p> <p>Periodicity backup - Set the circle duration for backup.</p> <p>Backup after change configuration - Backup will be executed whenever the configuration is changed.</p>
Support Model List	<p>Web configuration file from <i>other</i> Vigor router can be applied to Vigor2862 series. At present, the configuration file of Vigor2860 is accepted for Vigor 2862.</p> <p>This field displays model name(s) and firmware which web configuration file saved can be used by such router.</p>

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.

Configuration Backup / Restoration

Restore

Restore settings from a configuration file.

選擇檔案 未選擇檔案

USB Storage 📁

Restore configuration except the login password.

Note:
This will work only if the selected configuration file was created from this device.

Backup

Back up the current settings into a configuration file.

Protect with password

Auto Backup to USB storage

Enable

Backup folder 📁

Periodicity backup

Cycle duration: days and hours

Backup after change configuration

Note:

1. When loading a configuration file from a model in the Supported Model List please note that features and functionality can vary between models so please manually verify the settings after the restoration.
2. Auto backup to USB: if settings do not change, configuration doesn't backup.
3. Auto backup to USB: if configuration backup multiple times in one hour, the old file will be overwritten with the same filename.

Supported Model List

Model	Firmware Version
Vigor2860	3.8.5, or later

2. Click **Choose File** button to choose the correct configuration file for uploading to the router.
3. Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

VI-1-7 Syslog/Mail Alert

SysLog function is provided for users to monitor router.

System Maintenance >> SysLog / Mail Alert Setup

SysLog / Mail Alert Setup	
<p>SysLog Access Setup</p> <p><input checked="" type="checkbox"/> Enable</p> <p>Syslog Save to:</p> <p><input checked="" type="checkbox"/> Syslog Server</p> <p><input type="checkbox"/> USB Disk</p> <p>Router Name <input type="text" value="DrayTek"/></p> <p>Server IP Address <input type="text"/></p> <p>Destination Port <input type="text" value="514"/></p> <p>Mail Syslog <input type="checkbox"/> Enable</p> <p>Enable syslog message:</p> <p><input checked="" type="checkbox"/> Firewall Log</p> <p><input checked="" type="checkbox"/> VPN Log</p> <p><input checked="" type="checkbox"/> User Access Log</p> <p><input checked="" type="checkbox"/> Call Log</p> <p><input checked="" type="checkbox"/> WAN Log</p> <p><input checked="" type="checkbox"/> Router/DSL information</p> <p><input checked="" type="checkbox"/> WLAN Log</p>	<p>Mail Alert Setup</p> <p><input checked="" type="checkbox"/> Enable <input type="button" value="Send a test e-mail"/></p> <p>SMTP Server <input type="text"/></p> <p>SMTP Port <input type="text" value="25"/></p> <p>Mail To <input type="text"/></p> <p>Return-Path <input type="text"/></p> <p><input type="checkbox"/> Use SSL</p> <p><input type="checkbox"/> Authentication</p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>Enable E-Mail Alert:</p> <p><input checked="" type="checkbox"/> DoS Attack</p> <p><input checked="" type="checkbox"/> APPE</p> <p><input checked="" type="checkbox"/> VPN LOG</p> <p><input type="checkbox"/> APPE Signature</p> <p><input type="checkbox"/> Debug Log</p>

Note:

1. Mail Syslog cannot be activated unless USB Disk is ticked for "Syslog Save to".
2. Mail Syslog feature sends a Syslog file when its size reaches 1M Bytes.
3. We only support secured SMTP connection on port 465.

Available settings are explained as follows:

Item	Description
SysLog Access Setup	<p>Enable - Check Enable to activate function of syslog.</p> <p>Syslog Save to - Check Syslog Server to save the log to Syslog server.</p> <p>Check USB Disk to save the log to the attached USB storage disk.</p>
Router Name	<p>Display the name for such router configured in System Maintenance>>Management.</p> <p>If there is no name here, simply lick the link to access into System Maintenance>>Management to set the router name.</p> <p>Server IP Address -The IP address of the Syslog server.</p> <p>Destination Port - Assign a port for the Syslog protocol.</p> <p>Mail Syslog - Check the box to recode the mail event on Syslog.</p> <p>Enable syslog message - Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to Syslog.</p>
Mail Alert Setup	<p>Check Enable to activate function of mail alert.</p> <p>Send a test e-mail - Make a simple test for the e-mail address specified in this page. Please assign the mail address first and click this button to execute a test for verify the mail</p>

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.

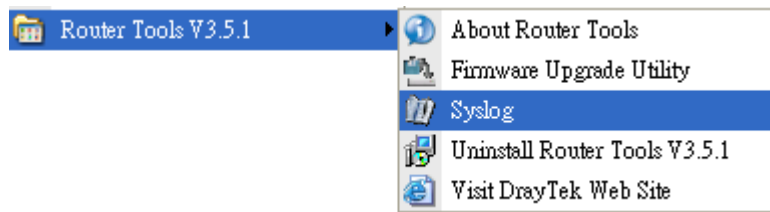
Password - Type the password for authentication.

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.

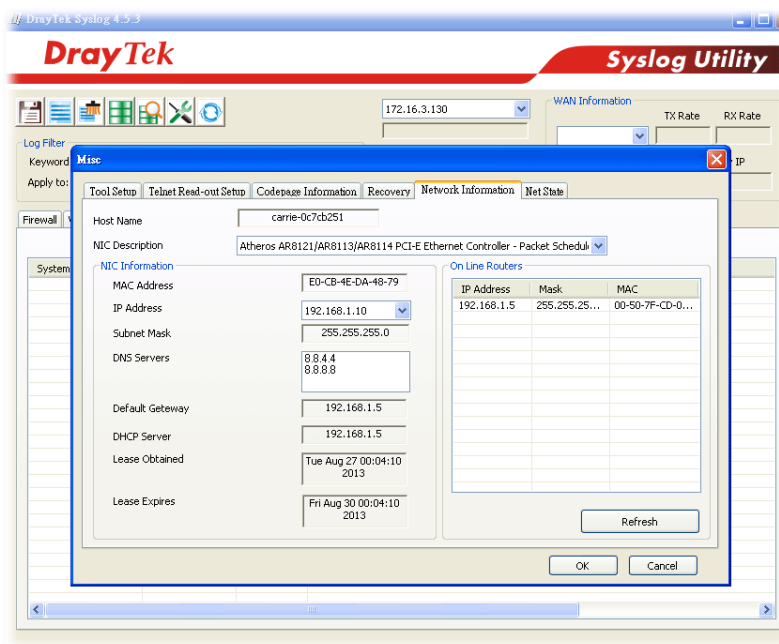
Click **OK** to save these settings.

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.



VI-1-8 Time and Date

It allows you to specify where the time of the router should be inquired from.

System Maintenance >> Time and Date

Time Information

Current System Time: 2000 Jan 2 Sun 19 : 14 : 53 Inquire Time

Time Setup

Use Browser Time
 Use Internet Time

Time Server: pool.ntp.org

Priority: Auto

Time Zone: (GMT) Greenwich Mean Time : Dublin

Enable Daylight Saving: Advanced

Automatically Update Interval: 30 min

Send NTP Request Through: Auto

OK Cancel

Available settings are explained as follows:

Item	Description
Current System Time	Click Inquire Time to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.
Time Server	Type the 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. <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Daylight Saving Advanced</p> <p> <input checked="" type="radio"/> Default Start: No Daylight Saving End: No Daylight Saving </p> <p> <input type="radio"/> Date Range Start: Year Month Day 00:00 End: Year Month Day 00:00 </p> <p> <input type="radio"/> Yearly Start: Yearly On Januai First Sunda 00:00 End: Yearly On Januai First Sunda 00:00 </p> <p style="text-align: center;"> OK Close </p> </div> 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.

Send NTP Request Through	Specify a WAN interface to send NTP request for time synchronization.
--------------------------	---

Click OK to save these settings.

VI-1-9 SNMP

This page allows you to configure settings for SNMP and SNMPV3 services.

The SNMPv3 is more secure than SNMP through the encryption method (support AES and DES) and authentication method (support MD5 and SHA) for the management needs.

System Maintenance >> SNMP

SNMP Setup

Enable SNMP Agent

Get Community:

Set Community:

Manager Host IP(IPv4)	Index	IP	Subnet Mask
	1	<input type="text"/>	<input type="text" value=""/>
	2	<input type="text"/>	<input type="text" value=""/>
	3	<input type="text"/>	<input type="text" value=""/>

Manager Host IP(IPv6)	Index	IPv6 Address	/ Prefix Length
	1	<input type="text"/>	<input type="text" value="/0"/>
	2	<input type="text"/>	<input type="text" value="/0"/>
	3	<input type="text"/>	<input type="text" value="/0"/>

Trap Community:

Notification Host IP(IPv4)	Index	IP
	1	<input type="text"/>
	2	<input type="text"/>

Notification Host IP(IPv6)	Index	IPv6 Address
	1	<input type="text"/>
	2	<input type="text"/>

Trap Timeout:

Enable SNMPV3 Agent

USM User:

Auth Algorithm:

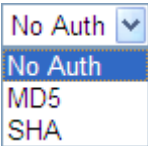
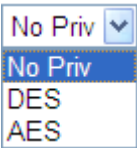
Auth Password:

Privacy Algorithm:

Privacy Password:

Available settings are explained as follows:

Item	Description
Enable SNMP Agent	Check it to enable this function.
Get Community	Set the name for getting community by typing a proper

	<p>character. The default setting is public.</p> <p>The maximum length of the text is limited to 23 characters.</p>
Set Community	<p>Set community by typing a proper name. The default setting is private.</p> <p>The maximum length of the text is limited to 23 characters.</p>
Manager Host IP (IPv4)	<p>Set one host as the manager to execute SNMP function. Please type in IPv4 address to specify certain host.</p>
Manager Host IP (IPv6)	<p>Set one host as the manager to execute SNMP function. Please type in IPv6 address to specify certain host.</p>
Trap Community	<p>Set trap community by typing a proper name. The default setting is public.</p> <p>The maximum length of the text is limited to 23 characters.</p>
Notification Host IP (IPv4)	<p>Set the IPv4 address of the host that will receive the trap community.</p>
Notification Host IP (IPv6)	<p>Set the IPv6 address of the host that will receive the trap community.</p>
Trap Timeout	<p>The default setting is 10 seconds.</p>
Enable SNMPV3 Agent	<p>Check it to enable this function.</p>
USM User	<p>USM means user-based security mode.</p> <p>Type a username which will be used for authentication. The maximum length of the text is limited to 23 characters.</p>
Auth Algorithm	<p>Choose one of the encryption methods listed below as the authentication algorithm.</p> 
Auth Password	<p>Type a password for authentication. The maximum length of the text is limited to 23 characters.</p>
Privacy Algorithm	<p>Choose one of the methods listed below as the privacy algorithm.</p> 
Privacy Password	<p>Type a password for privacy. The maximum length of the text is limited to 23 characters.</p>

Click OK to save these settings.

VI-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

System Maintenance >> Management

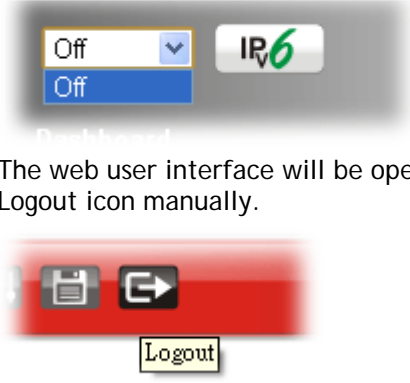


IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup
Router Name <input type="text" value="DrayTek"/>		
<input type="checkbox"/> Default: Disable Auto-Logout <input type="checkbox"/> Enable Validation Code in Internet/LAN Access		
Internet Access Control <input type="checkbox"/> Allow management from the Internet Domain name allowed <input type="text"/>		
<input type="checkbox"/> FTP Server <input type="checkbox"/> HTTP Server <input type="checkbox"/> Enforce HTTPS Access <input checked="" type="checkbox"/> HTTPS Server <input type="checkbox"/> Telnet Server <input type="checkbox"/> TR069 Server <input type="checkbox"/> SSH Server <input type="checkbox"/> SNMP Server <input checked="" type="checkbox"/> Disable PING from the Internet		
Access List from the Internet		
List	index in IP Object	IP / Mask
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>
Management Port Setup <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports		
Telnet Port <input type="text" value="23"/> (Default: 23)		
HTTP Port <input type="text" value="80"/> (Default: 80)		
HTTPS Port <input type="text" value="443"/> (Default: 443)		
FTP Port <input type="text" value="21"/> (Default: 21)		
TR069 Port <input type="text" value="8069"/> (Default: 8069)		
SSH Port <input type="text" value="22"/> (Default: 22)		
Brute Force Protection <input type="checkbox"/> Enable brute force login protection		
<input type="checkbox"/> FTP Server <input type="checkbox"/> HTTP Server <input type="checkbox"/> HTTPS Server <input type="checkbox"/> Telnet Server <input type="checkbox"/> TR069 Server <input type="checkbox"/> SSH Server		
Maximum login failures <input type="text" value="0"/> times		
Penalty period <input type="text" value="0"/> seconds		
Blocked IP List		
TLS/SSL Encryption Setup <input checked="" type="checkbox"/> Enable TLS 1.2 <input checked="" type="checkbox"/> Enable TLS 1.1 <input checked="" type="checkbox"/> Enable TLS 1.0 <input type="checkbox"/> Enable SSL 3.0		
CVM Access Control <input type="checkbox"/> CVM Port <input type="text" value="8000"/> (Default: 8000) <input type="checkbox"/> CVM SSL Port <input type="text" value="8443"/> (Default: 8443)		
AP Management <input checked="" type="checkbox"/> Enable AP Management		
<input checked="" type="checkbox"/> Device Management <input type="checkbox"/> Respond to external device		

OK

Available settings are explained as follows:

Item	Description
Router Name	Type in the router name provided by ISP.
Default: Disable Auto-Logout	If it is enabled, the function of auto-logout for web user interface will be disabled.

	 <p>The web user interface will be open until you click the Logout icon manually.</p>
Enable Validation Code in Internet/LAN Access	<p>If it is enabled, the mechanism of validation code will be offered by Vigor router. That is, the client must type validation code while accessing into Internet or web user interface of Vigor router.</p>
Internet Access Control	<p>Allow management from the Internet - Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.</p> <p>Disable PING from the Internet - Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.</p>
Access List from the Internet	<p>You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.</p> <p>index in IP Object- Type the index number of the IP object profile. Related IP with Subnet Mask will appear automatically.</p>
Management Port Setup	<p>User Define Ports - Check to specify user-defined port numbers for the Telnet, HTTP, HTTPS, FTP, TR-069 and SSH servers.</p> <p>Default Ports - Check to use standard port numbers for the Telnet and HTTP servers.</p>
Brute Force Protection	<p>Any client trying to access into Internet via Vigor router will be asked for passing through user authentication. Such feature can prevent Vigor router from attacks when a hacker tries every possible combination of letters, numbers and symbols until find out the correct combination of password.</p> <p>Enable brute force login protection - Enable the protection mechanism.</p> <p>Maximum login failure - Specify the maximum number of wrong password that client can try for logging to Vigor router.</p> <p>Penalty period - Set a period of time to block the IP address which is used (by user or hacker) for passing through the user authentication again and again but failed always. When the time is up, Vigor system will unblock that IP and allow it to access into Vigor router again.</p> <p>Blocked IP List - Open another web page which displays current blocked IPs.</p>
TLS/SSL Encryption Setup	<p>Enable SSL 3.0/1.0/1.1/1.2 - Check the box to enable the</p>

	<p>function of SSL 3.0/1.0/1.1/1.2 if required.</p> <p>Due to security consideration, the built-in HTTPS and SSL VPN server of the router had upgraded to TLS1.x protocol. If you are using old browser(eg. IE6.0) or old SmartVPN Client, you may still need to enable SSL 3.0 to make sure you can connect, however, it's not recommended.</p>
CVM Access Control	<p>CVM Port - Check the box to enable such port setting.</p> <p>CVM SSL Port - Check the box to enable such port setting.</p>
AP Management	<p>Enable AP Management - Check it to enable the function of Central Management>>AP. If unchecked, menu items related to Central Management>>AP will be hidden.</p>
Device Management	<p>Check the box to enable the device management function for Vigor2862.</p> <p>Respond to external device - If it is enabled, Vigor2862 will be regarded as slave device. When the external device (master device) sends request packet to Vigor2862, Vigor2862 would send back information to respond the request coming from the external device which is able to manage Vigor2862.</p>

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

For IPv6

System Maintenance >> Management



IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup																																	
<p>Management Access Control</p> <p><input type="checkbox"/> Allow management from the Internet</p> <ul style="list-style-type: none"> <input type="checkbox"/> Telnet Server (Port : 23) <input type="checkbox"/> HTTP Server (Port : 80) <input type="checkbox"/> HTTPS Server (Port : 443) <input type="checkbox"/> SSH Server (Port : 22) <input type="checkbox"/> SNMP Server (Port : 161) <p><input checked="" type="checkbox"/> Disable PING from the Internet</p> <hr/> <p>Access List from the Internet</p> <table border="1"> <thead> <tr> <th>List</th> <th>index in IPv6 Object</th> <th>IPv6 / Prefix</th> </tr> </thead> <tbody> <tr><td>1</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>2</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>3</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>4</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>5</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>6</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>7</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>8</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>9</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>10</td><td><input type="text"/></td><td><input type="text"/></td></tr> </tbody> </table> <p>Note: Telnet / Http server port is the same as IPv4.</p>			List	index in IPv6 Object	IPv6 / Prefix	1	<input type="text"/>	<input type="text"/>	2	<input type="text"/>	<input type="text"/>	3	<input type="text"/>	<input type="text"/>	4	<input type="text"/>	<input type="text"/>	5	<input type="text"/>	<input type="text"/>	6	<input type="text"/>	<input type="text"/>	7	<input type="text"/>	<input type="text"/>	8	<input type="text"/>	<input type="text"/>	9	<input type="text"/>	<input type="text"/>	10	<input type="text"/>	<input type="text"/>
List	index in IPv6 Object	IPv6 / Prefix																																	
1	<input type="text"/>	<input type="text"/>																																	
2	<input type="text"/>	<input type="text"/>																																	
3	<input type="text"/>	<input type="text"/>																																	
4	<input type="text"/>	<input type="text"/>																																	
5	<input type="text"/>	<input type="text"/>																																	
6	<input type="text"/>	<input type="text"/>																																	
7	<input type="text"/>	<input type="text"/>																																	
8	<input type="text"/>	<input type="text"/>																																	
9	<input type="text"/>	<input type="text"/>																																	
10	<input type="text"/>	<input type="text"/>																																	

OK

Available settings are explained as follows:

Item	Description
Management Access Control	<p>Allow management from the Internet - Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.</p> <p>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.</p>
Access List from the Internet	<p>You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.</p> <p>Index in IPv6 Object- Type the index number of the IPv6 object profile. Related IP address will appear automatically.</p>

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

For LAN

System Maintenance >> Management



IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup
<input checked="" type="checkbox"/> Allow management from LAN		
<input checked="" type="checkbox"/> FTP Server		
<input checked="" type="checkbox"/> HTTP Server <input type="checkbox"/> Enforce HTTPS Access		
<input checked="" type="checkbox"/> HTTPS Server		
<input checked="" type="checkbox"/> Telnet Server		
<input checked="" type="checkbox"/> TR069 Server		
<input checked="" type="checkbox"/> SSH Server		
Apply To Subnet		Index in IP Object
<input checked="" type="checkbox"/> LAN1	<input type="checkbox"/>	<input type="text"/>
<input checked="" type="checkbox"/> LAN2	<input type="checkbox"/>	<input type="text"/>
<input checked="" type="checkbox"/> LAN3	<input type="checkbox"/>	<input type="text"/>
<input checked="" type="checkbox"/> LAN4	<input type="checkbox"/>	<input type="text"/>
<input checked="" type="checkbox"/> LAN5	<input type="checkbox"/>	<input type="text"/>
<input checked="" type="checkbox"/> LAN6	<input type="checkbox"/>	<input type="text"/>
<input checked="" type="checkbox"/> LAN7	<input type="checkbox"/>	<input type="text"/>
<input checked="" type="checkbox"/> LAN8	<input type="checkbox"/>	<input type="text"/>
<input checked="" type="checkbox"/> DMZ	<input type="checkbox"/>	<input type="text"/>
<input checked="" type="checkbox"/> IP Routed Subnet	<input type="checkbox"/>	<input type="text"/>

Note:

If an IP Object is specified in a LAN Subnet, the setting will be applied to the selected IP only.

OK

Available settings are explained as follows:

Item	Description
Allow management from LAN	Enable the checkbox to allow system administrators to login from LAN interface. There are several servers provided by the system which allow you to manage the router from LAN interface. Check the box(es) to specify.
Apply To Subnet	Check the LAN interface for the administrator to use for accessing into web user interface of Vigor router. Index in IP Object - Type the index number of the IP object profile. Related IP address will appear automatically.

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

VI-1-11 Self-Signed Certificate

A self-signed certificate is a *unique* identification for the device (e.g., Vigor router) which generates the certificate by itself to ensure the router security. Such self-signed certificate is signed with its own private key.

The self-signed certificate will be applied in SSL VPN, HTTPS, and so on. In addition, it can be created for free by using a wide variety of tools.

System Maintenance >> Self-Signed Certificate

Self-Signed Certificate Information

Certificate Name :	self-signed
Issuer :	C=TW, ST=HsinChu, L=HuKou, O=DrayTek Corp., OU=DrayTek Support, CN=Vigor Router
Subject :	C=TW, ST=HsinChu, L=HuKou, O=DrayTek Corp., OU=DrayTek Support, CN=Vigor Router
Subject Alternative Name :	
Valid From :	Jun 2 13:05:46 2016 GMT
Valid To :	Jun 2 13:05:46 2046 GMT
PEM Format Content :	<pre>-----BEGIN CERTIFICATE----- MIIDcTCCAImgAwIBAgIJAP67J8my6NLIMA0GCSqGSIb3DQEBCwUAMHgx CzA3BgNV BAYTA1R0MRFAwDgYD VQIEwdIc2luQ2h1MQ4wDAYD VQHEwVIDUctvdTEWMBQGA1UE ChMNRHJheVR1ayBDb3JwLjEYMBYGA1UECxMFRHJheVR1ayBDb3JwLjEYMBYGA1UE VQDEwWwWdvc1B5b3V0ZiX1wHcNMTYwNjAyMTMwNTQ2WncNNDYwNjAyMTMwNTQ2 WjB4MQswCQYD VQGEwJUVzE QMA4GA1UECBMHSHpkkModTEOMA wGA1UEBxMFSHVL b3Ux FjAUBGNVBAcT DURyYX1UZWsgQ29ycC4xGDAWBgNVBAstD0RyYX1UZWsgU3Vl cG9ydEVMBGMA1UEAxMMVmlnb3JgUm91dGVyMIIIBIjANBgkqhkiG9w0BAQEFAAOC AQ8AMIIBCgKCAQEAYyy8jGcJhUfPcMBODHvq/jtSemVlMXJxPBd0mv780PyPvQ3QH mWLRNfLteu9Y7Y7p8AdK8yOp1vxUW30hjQI6WbuKcndYzdgTx6aV6gtT09XriRU zjFcXxhLNNi dtS1GYt6GiysFJR219BSudCeaAlMoeHWiVq34/juIuEcV8XqVlHeH cJGvpVEAAAjDM3sWNsYCu1K51FuCRZpPcXaj aS5fx9Hz0TbMy2T1oE0zudD219eX lbkqdkjX56VQ1z9G6/wQKYNBw9B015MFmIk3/moLkjm8E5HbaESSJorhyFNQF9TJ bvgN1DNQH8f0Wic5tqZkIXE0gm0vyKdYaccstwidAQABMA0GCSqGSIb3DQEBCwUA A4IBAQBZ+Jb8UxgMmipmSu3Yai0JPrboigtD3fE3SULkGGqkd04jtWlJq0+KtUz Ma0uU4zxEg13tmYY5nqPTs/EGnzJI/vWxxtG1cB0vcC3EcbTj+g0Y9VnB8Y0vE B8QiJgIW+coPjsFCb2kzf+Rb16LAAETw7718S/qkHgFmydaqa5L945yKgwNaNaijk jg6J+piagGhx6t/1Y2WB3Tezb/UH5iD8SfII1C1F/yiz3v4Sg2godJscck1q2xcB LbRCK1+X0TzM5gd7W5gS2eRc0z3u0+iRFKqi0bJOYNZDz4Kyx1WoprNG4iF7cLcR /HAPsHelogs0Ttlx3M2yLICmrzzi -----END CERTIFICATE-----</pre>

Note:

1. Please setup the **System Maintenance >> Time and Date** correctly before you try to regenerate a self-signed certificate!!
2. The Time Zone MUST be setup correctly!!

Regenerate

Click Regeneration to open Regenerate Self-Signed Certificate window. Type in all the information that the window request such as certificate name (used for identifying different certificate), subject alternative name type and relational settings for subject name. Then click GENERATE.

Regenerate Self-Signed Certificate

Certificate Name	self-signed
Subject Alternative Name	
Type	IP Address ▾
IP	<input type="text"/>
Subject Name	
Country (C)	<input type="text"/>
State (ST)	<input type="text"/>
Location (L)	<input type="text"/>
Organization (O)	<input type="text"/>
Organization Unit (OU)	<input type="text"/>
Common Name (CN)	<input type="text"/>
Email (E)	<input type="text"/>
Key Type	RSA ▾
Key Size	2048 Bit ▾

Generate

VI-1-12 Reboot System

The Web user interface may be used to restart your router. Click **Reboot System** from **System Maintenance** to open the following page.

System Maintenance >> Reboot System

Reboot System

Do you want to reboot your router ?

Using current configuration
 Using factory default configuration

Auto Reboot Time Schedule

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

Note:
Action and Idle Timeout settings will be ignored.

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.

VI-1-13 Firmware Upgrade

Click **System Maintenance >> Firmware Upgrade** to proceed to firmware upgrade.

System Maintenance >> Firmware Upgrade



Firmware Version Status

Current Firmware Version: 3.8.7_RC3_STD

[Check The Latest Firmware](#)

Web Firmware Upgrade

Select a firmware file.

[選擇檔案](#) [未選擇檔案](#)

Click Upgrade to upload the file.

[Upgrade](#)

TFTP Firmware Upgrade from LAN

Firmware Upgrade Procedures:

1. Click "OK" to start the TFTP server.
2. Open the Firmware Upgrade Utility or other 3-party TFTP client software.
3. Check that the firmware filename is correct.
4. Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade.
5. After the upgrade is complete, the TFTP server will automatically stop running.

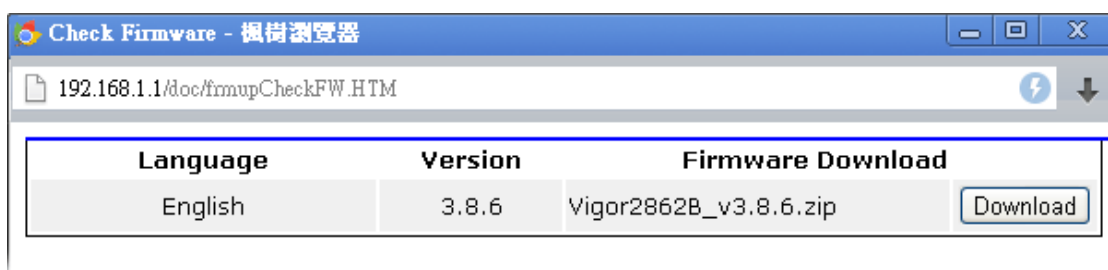
Do you want to upgrade firmware ?

[OK](#)

Note:

Upgrade using the ALL file will retain existing router configuration, whereas using the RST file will reset the configuration to factory defaults.

Click the button of **Check The Latest Firmware** to open a pop up window displaying the newest firmware version released for such Vigor router.



Choose the one you need and click **Download**. After that, click **Select** to specify the one you just download. Then, click **Upgrade**. The system will upgrade the firmware of the router automatically.

VI-1-14 Firmware Backup

The firmware for Vigor router can be saved on the host as a backup firmware. After that, if the router crashes due to the firmware error, the backup firmware will be applied to make the router run normally.

System Maintenance >> Firmware Backup

Firmware Backup Setting

- Backup after reboot
- Backup after system running day hour (max. 7 days)
- Manually backup

Last backup time: 2017/10/13 02:54:22

Simply specify the condition to run the firmware backup and click OK to save the settings.

VI-1-15 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.

Click Upgrade to upload the file.

VI-1-16 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>.

Web-Filter License**Activate**

[Status:Not Activated]

Authentication Message

Note:

1. If you want to use email alert or syslog, please configure the [SysLog/Mail Alert Setup](#) page.
2. If you change the service provider, the configuration of the function will be reset.

Available settings are explained as follows:

Item	Description
Activate via Interface	Choose WAN interface used by such device for activating Web Content Filter.
Activate	The Activate link brings you accessing into www.vigorpro.com to finish the activation of the account and the router.
Authentication Message	As for authentication information of web filter, the process of authenticating will be displayed on this field for your reference.

Below shows the successful activation of Web Content Filter:

Web-Filter License**Activate**

[Status:Commtouch] [Start Date:2011-03-28 Expire Date:2011-04-27]

Authentication Message

```
WebFilter, Activation authenticate fail, contact with support@draytek.com, 2011-03-28 01:00:24
```

Note: If you want to use email alert or syslog, please configure the [SysLog/Mail Alert Setup](#) page.

If you change the service provider, the configuration of the function will be reset.

VI-1-17 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 internal RADIUS and/or Local 802.1X) for each user profile without accessing into the User Management configuration page.

System Maintenance >> Internal Service User List

User Name	<input type="checkbox"/> Radius	<input type="checkbox"/> Local 802.1X	User Name	<input type="checkbox"/> Radius	<input type="checkbox"/> Local 802.1X
test_1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	test_sales	<input type="checkbox"/>	<input type="checkbox"/>

OK Cancel

Note:

1. Only the user profiles which is enabled in User **Management >> User Profile** will be listed here.
2. 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 **Management >> User Profile**.

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 security 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 security 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**.

VI-1-18 Dashboard Control

There are nine groups of setting information which can be displayed on Dashboard as a reference for administrator/user. Except for Front Panel and System Information, the settings information regarding to the groups listed on this page can be hidden if required.

System Maintenance >> Dashboard Control

<input type="checkbox"/> Front Panel
<input type="checkbox"/> System Information
<input checked="" type="checkbox"/> IPv4 LAN Information
<input checked="" type="checkbox"/> IPv4 Internet Access
<input checked="" type="checkbox"/> IPv6 Internet Access
<input checked="" type="checkbox"/> Interface
<input checked="" type="checkbox"/> Security
<input checked="" type="checkbox"/> System Resource
<input checked="" type="checkbox"/> Quick Access

OK

Cancel

VI-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?

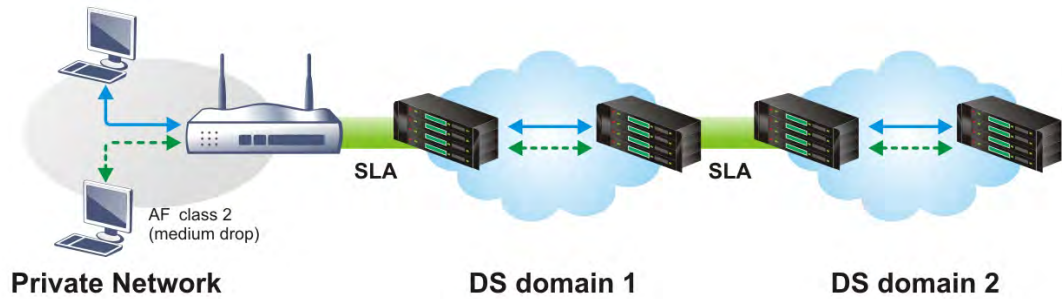
There are two components within Primary configuration of QoS deployment:

- 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.



VI-2-1 Sessions Limit

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

Bandwidth Management >> Sessions Limit

IPv4
IPv6

Enable Disable

Default Max Sessions:

Limitation List

Index	Start IP	End IP	Max Sessions

Specific Limitation

Start IP: End IP:

Maximum Sessions:

Administration Message (Max 255 characters)

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

Time Schedule

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

Note:
Action and Idle Timeout settings will be ignored.

To activate the function of limit session, simply click Enable and set the default session limit. Available settings are explained as follows:

Item	Description
Session Limit	<p>Enable - Click this button to activate the function of limit session.</p> <p>Disable - Click this button to close the function of limit session.</p> <p>Default Max Session - Defines the default maximum session</p>

	number used for each computer in LAN.
Limitation List	Displays a list of specific limitations that you set on this web page.
Specific Limitation	<p>Start IP- Defines the start IP address for limit session.</p> <p>End IP - Defines the end IP address for limit session.</p> <p>Maximum Sessions - Defines the available session number for each host in the specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index.</p> <p>Add - Adds the specific session limitation onto the list above.</p> <p>Edit - Allows you to edit the settings for the selected limitation.</p> <p>Delete - Remove the selected settings existing on the limitation list.</p>
Administration Message	<p>Type the words which will be displayed when reaches the maximum number of Internet sessions permitted.</p> <p>Default Message - Click this button to apply the default message offered by the router.</p>
Time Schedule	Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page.

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

VI-2-2 Bandwidth Limit

In the **Bandwidth Management** menu, click **Bandwidth Limit** to open the web page. To activate the function of limit bandwidth, simply click **Enable** and set the default upstream and downstream limit.

Bandwidth Management >> Bandwidth Limit

IPv4
IPv6

Enable IP Routed Subnet **Disable**

Default TX Limit Per User: Kbps
 Default RX Limit Per User: Kbps

Limitation List

Index	Start IP/Group	End IP/Object	TX limit	RX limit	Share

Specific Limitation IP Object

Start IP: End IP:

Each Shared
 TX Limit: Kbps
 RX Limit: Kbps

Allow auto adjustment to assign available bandwidth equally to active user.

Smart Bandwidth Limit

For any LAN IP Not in Limitation List, whose session number exceeds

TX Limit : Kbps
 RX Limit : Kbps

Note:

1. For TX/RX, a setting of "0" means unlimited bandwidth.
2. Available bandwidth is calculated according to the maximum bandwidth detected or the Line Speed defined in WAN >> **General Setup** when in "According to Line Speed" Load Balance mode.

Time Schedule

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

Note:
Action and Idle Timeout settings will be ignored.

Available settings are explained as follows:

Item	Description
Enable	Click this button to activate the function of limit bandwidth. IP Routed Subnet - Check this box to apply the bandwidth limit to the second subnet specified in LAN>>General Setup. It is available for IPv4 settings only. 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.
Disable	Click this button to close the function of limit bandwidth.
Limitation List	Display a list of specific limitations that you set on this web page.

<p>Specific Limitation</p>	<p>IP - All the IPs within the range defined will be restricted by bandwidth limit defined by TX Limit and RX Limit below.</p> <ul style="list-style-type: none"> ● Start IP - Define the start IP address for limit bandwidth. ● End IP - Define the end IP address for limit bandwidth. <p>Object - All the IPs specified by the selected IP object or IP group will be restricted by bandwidth limit defined by TX Limit and RX Limit below.</p> <ul style="list-style-type: none"> ● IP Group - Specify an IP group by using the drop down list. ● IP Object - Specify an IP object by using the drop down list. <p>Each / Shared - Select Each to make each IP within the range of Start IP and End IP having the same speed defined in TX limit and RX limit fields; select Shared to make all the IPs within the range of Start IP and End IP share the speed defined in TX limit and RX limit fields.</p> <p>TX limit - Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.</p> <p>RX limit - Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.</p> <p>Add - Add the specific speed limitation onto the list above.</p> <p>Edit - Allow you to edit the settings for the selected limitation.</p> <p>Delete - Remove the selected settings existing on the limitation list.</p>
<p>Allow auto adjustment to assign available ...</p>	<p>Check this box to make the best utilization of available bandwidth.</p>
<p>Smart Bandwidth Limit</p>	<p>Check this box to have the bandwidth limit determined by the system automatically.</p> <p>TX limit - Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.</p> <p>RX limit - Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.</p>
<p>Time Schedule</p>	<p>Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page.</p>

VI-2-3 Quality of Service

In the Bandwidth Management menu, click Quality of Service to open the web page.

Bandwidth Management >> Quality of Service

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

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	--Kbps/--Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN2	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN4	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setup

Class Rule

Index	Name	Rule	Service Type
Class 1		Edit	
Class 2		Edit	Edit
Class 3		Edit	

Enable the First Priority for VoIP SIP/RTP:

SIP UDP Port: (Default: 5060)

Available settings are explained as follows:

Item	Description
General Setup	<p>Index - Display the WAN/LTE interface number that you can edit.</p> <p>Status - Display if the WAN interface is available for such function or not.</p> <p>Bandwidth - Display the inbound and outbound bandwidth setting for the WAN interface.</p> <p>Direction - Display which direction that such function will influence.</p> <p>Class 1/Class2/Class 3/Others - Display the bandwidth percentage for each class.</p> <p>UDP Bandwidth Control - Display the UDP bandwidth control is enabled or not.</p> <p>Online Statistics - Display an online statistics for quality of service for your reference.</p> <p>Setup - Allow to configure general QoS setting for WAN interface.</p>
Class Rule	<p>Index - Display the class number that you can edit.</p> <p>Name - Display the name of the class.</p> <p>Rule - Allow to configure detailed settings for the selected Class.</p> <p>Service Type - Allow to configure detailed settings for the service type.</p>
Enable the First Priority for VoIP SIP/RTP	<p>When this feature is enabled, the VoIP SIP/UDP packets will be sent with highest priority.</p> <p>SIP UDP Port - Set a port number used for SIP.</p>

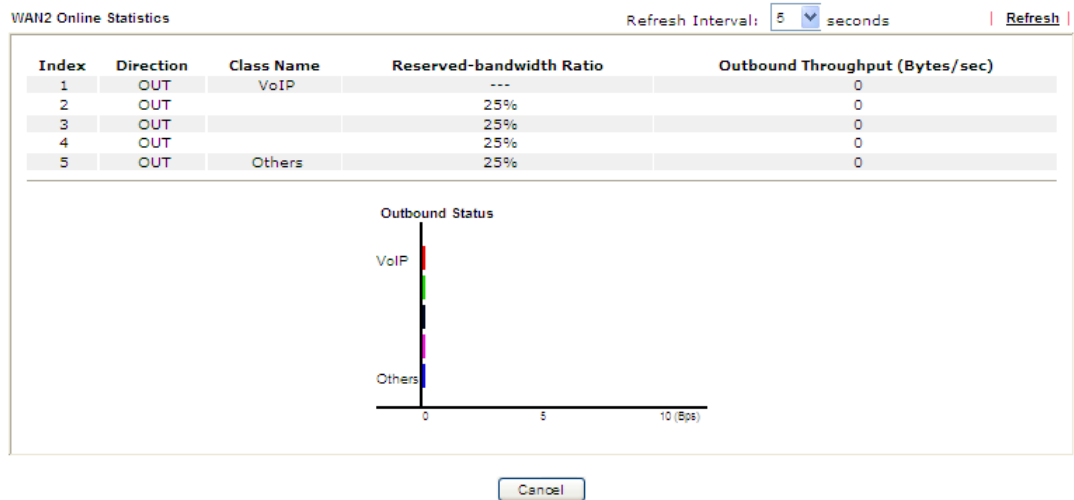
This page displays the QoS settings result of the WAN interface. Click the **Setup** link to access into next page for the general setup of WAN interface. As to class rule, simply click the **Edit** link to access into next for configuration.

You can configure general setup for the WAN interface, edit the Class Rule, and edit the Service Type for the Class Rule for your request.

Online Statistics

Display an online statistics for quality of service for your reference. This feature is available only when the Quality of Service for WAN interface is enabled.

Bandwidth Management >> Quality of Service



General Setup for WAN Interface

When you click **Setup**, you can configure the bandwidth ratio for QoS of the WAN interface. There are four queues allowed for QoS control. The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. Yet, the last one is reserved for the packets which are not suitable for the user-defined class rules.

Bandwidth Management >> Quality of Service

WAN3 General Setup

Enable the QoS Control BOTH ▾

WAN Inbound Bandwidth	<input type="text" value="100"/>	<input type="radio"/> Kbps	<input checked="" type="radio"/> Mbps	
WAN Outbound Bandwidth	<input type="text" value="100"/>	<input type="radio"/> Kbps	<input checked="" type="radio"/> Mbps	
Index	Class Name	Reserved bandwidth Ratio		
Class 1		<input type="text" value="25"/>	%	
Class 2		<input type="text" value="25"/>	%	
Class 3		<input type="text" value="25"/>	%	
	Others	<input type="text" value="25"/>	%	
<input type="checkbox"/> Enable UDP Bandwidth Control		Limited_bandwidth Ratio <input type="text" value="25"/> %		
<input type="checkbox"/> Outbound TCP ACK Prioritize				

Note:

1. Before enable QoS, you should test the real bandwidth first. QoS may not work properly if the bandwidth is not accurate.
2. You can do speed test by <http://speedtest.net> or contact with your ISP for speed test program.

Available settings are explained as follows:

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



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](#)

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics
WAN1	Disable	--Kbps/--Kbps		25%	25%	25%	25%	Inactive	Status Setup
WAN2	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status Setup
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status Setup
WAN4	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status Setup

Class Rule

Index	Name	Rule	Service Type
Class 1		Edit	
Class 2		Edit	Edit
Class 3		Edit	

Enable the First Priority for VoIP SIP/RTP:
 SIP UDP Port: (Default:5060)

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

Bandwidth Management >> Quality of Service

Class Index #1

Name Tag Outbound Packets as:

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

- For adding a new rule, click **Add** to open the following page.

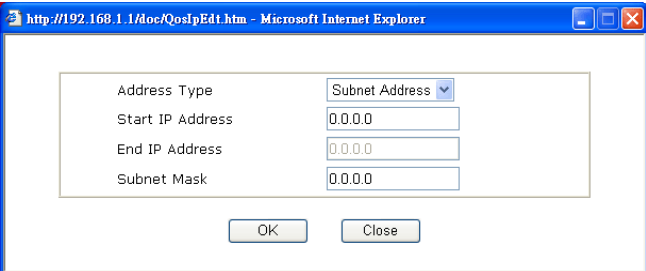
Bandwidth Management >> Quality of Service

Rule Edit

<input checked="" type="checkbox"/> ACT	<input type="checkbox"/> Hardware Acceleration
Ethernet Type	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Local Address	Any <input type="button" value="Edit"/>
Remote Address	Any <input type="button" value="Edit"/>
DiffServ CodePoint	ANY <input type="button" value="v"/>
Service Type	---Predefined--- <input type="button" value="v"/>

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

Available settings are explained as follows:

Item	Description
ACT	Check this box to invoke these settings.
Hardware Acceleration	Check this box to enable the hardware acceleration when such rule is applied.
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.  <p>Address Type - Determine the address type for the source address. For Single Address, you have to fill in Start IP address. For Range Address, you have to fill in Start IP address and End IP address. For Subnet Address, you have to fill in Start IP address and Subnet Mask.</p>
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.

Bandwidth Management >> Quality of Service

Class Index #1

Name Tag Outbound Packets as:

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

Edit the Service Type for Class Rule

1. To add a new service type, edit or delete an existed service type, please click the Edit link under Service Type field.

Bandwidth Management >> Quality of Service

General Setup [Set to Factory Default](#)

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics
WAN1	Disable	--Kbps/--Kbps	Both	25%	25%	25%	25%	Inactive	Status Setup
WAN2	Disable	100000Kbps/100000Kbps	Both	25%	25%	25%	25%	Inactive	Status Setup
WAN3	Disable	100000Kbps/100000Kbps	Both	25%	25%	25%	25%	Inactive	Status Setup
WAN4	Disable	100000Kbps/100000Kbps	Both	25%	25%	25%	25%	Inactive	Status Setup

Class Rule

Index	Name	Rule	Service Type
Class 1	Test	Edit	Edit
Class 2		Edit	
Class 3		Edit	

Enable the First Priority for VoIP SIP/RTP:

SIP UDP Port: (Default: 5060)

2. After you click the Edit link, you will see the following page.

Bandwidth Management >> Quality of Service

User Defined Service Type

NO	Name	Protocol	Port
1	Empty	-	-

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

Bandwidth Management >> Quality of Service

Service Type Edit

Service Name	<input type="text"/>
Service Type	TCP <input type="button" value="v"/> <input type="text" value="6"/>
Port Configuration	
Type	<input checked="" type="radio"/> Single <input type="radio"/> Range
Port Number	<input type="text" value="0"/> - <input type="text" value="0"/>

Available settings are explained as follows:

Item	Description
Service Name	Type in a new service for your request. 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	<p>Type - Click Single or Range as the Type. If you select Range, you have to type in the starting port number and the end porting number on the boxes below.</p> <p>Port Number - Type in the starting port number and the end porting number here if you choose Range as the type.</p>

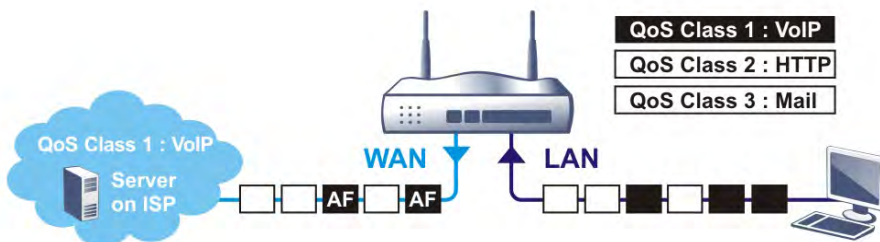
- After finishing all the settings here, please click **OK** to save the configuration.

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.



Bandwidth Management >> Quality of Service

Class Index #1

Name: Tag packets as:

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

VI-2-4 APP QoS

The QoS function is used to do bandwidth management for the services with certain IP or port number. However, there is no effect of bandwidth management on the service such as VNC or PPTV without fixed IP or port number.

APP QoS employs the function of APP Enforcement to detect the types of software in application layer. By combining the function of QoS (adjustment on Inbound/Outbound bandwidth and bandwidth ratio), Vigor router can perform the bandwidth management for the protocols, streaming, remote control, web HD and so on.

Click **Bandwidth Management >> APP QoS** to open the following page.

Bandwidth Management >> APP QoS

APP QoS

Enable
 Disable

Traceable
 Untraceable

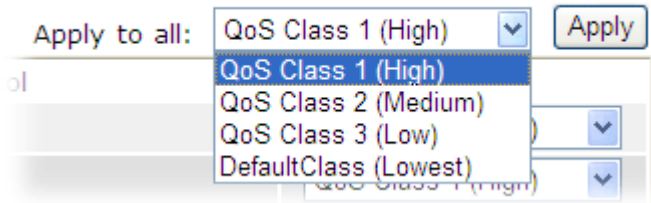
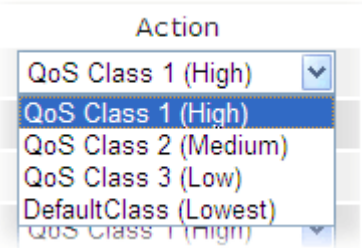
Apply to all: QoS Class 1 (High)

Enable	Protocol	Version	Action
<input type="checkbox"/>	DNS		QoS Class 1 (High) <input type="button" value="v"/>
<input type="checkbox"/>	FTP		QoS Class 1 (High) <input type="button" value="v"/>
<input type="checkbox"/>	HTTP	1.1	QoS Class 1 (High) <input type="button" value="v"/>
<input type="checkbox"/>	IMAP	4.1	QoS Class 1 (High) <input type="button" value="v"/>
<input type="checkbox"/>	IMAP STARTTLS	4.1	QoS Class 1 (High) <input type="button" value="v"/>
<input type="checkbox"/>	IRC	2.4.0	QoS Class 1 (High) <input type="button" value="v"/>
<input type="checkbox"/>	NNTP		QoS Class 1 (High) <input type="button" value="v"/>
<input type="checkbox"/>	POP3		QoS Class 1 (High) <input type="button" value="v"/>
<input type="checkbox"/>	POP3 STARTTLS		QoS Class 1 (High) <input type="button" value="v"/>
<input type="checkbox"/>	SMB	3.0	QoS Class 1 (High) <input type="button" value="v"/>
<input type="checkbox"/>	SMTP		QoS Class 1 (High) <input type="button" value="v"/>
<input type="checkbox"/>	SMTP STARTTLS		QoS Class 1 (High) <input type="button" value="v"/>
<input type="checkbox"/>	SNMP	2C	QoS Class 1 (High) <input type="button" value="v"/>
<input type="checkbox"/>	SSH	2	QoS Class 1 (High) <input type="button" value="v"/>
<input type="checkbox"/>	SSL/TLS	3.0/1.2	QoS Class 1 (High) <input type="button" value="v"/>
<input type="checkbox"/>	TELNET		QoS Class 1 (High) <input type="button" value="v"/>

Note: Please remember to adjust Inbound/Outbound bandwidth of your network in "Quality of Service".
This will help QoS to work more efficient.

Available settings are explained as follows:

Item	Description
Enable/Disable	Click Enable to activate APP QoS function. Click Disable to deactivate APP QoS function.
Traceable	The protocol listed below is traceable by Vigor router. Each tab offers different types of protocols to fit your request.
Untraceable	The protocol listed below is not easy to be traced by Vigor router. Each tab offers different types of protocols to fit your

	request.
Select All	Click it to select all of the protocols.
Clear All	Click it to de-select all of the protocols.
Apply to all	<p>Choose one of the actions from the drop down list. It is prepared for applying to all protocols.</p>  <p>Apply - Click it to make the selected action be applied all of the selected protocols immediately.</p>
Action	<p>There are many protocols which can be specified with different QoS Class.</p> 

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.


Bandwidth Management >> Quality of Service

General Setup | Set to Factory Default |

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics
WAN1	Disable	--Kbps/--Kbps		25%	25%	25%	25%	Inactive	Status Setup
WAN2	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status Setup
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status Setup
WAN4	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status Setup

Class Rule

Index	Name	Rule	Service Type
Class 1		Edit	
Class 2		Edit	Edit
Class 3		Edit	

Enable the First Priority for VoIP SIP/RTP:
SIP UDP Port: (Default:5060) 

- In the following page, type a name (e.g., VoIP) for such class and click **Add**.

Bandwidth Management >> Quality of Service

Class Index #1

Name: Tag Outbound Packets as:

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

- Check the box of **ACT**. Click **Edit** to specify the local address.

Bandwidth Management >> Quality of Service

Rule Edit

ACT Hardware Acceleration

Ethernet Type: IPv4 IPv6

Local Address:

Remote Address:

DiffServ CodePoint:

Service Type:

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

- 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.

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

Bandwidth Management >> Quality of Service

Rule Edit

ACT Hardware Acceleration

Ethernet Type: IPv4 IPv6

Local Address:

Remote Address:

DiffServ CodePoint:

Service Type:

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

7. The class rule for VoIP has been set. Click OK to return to previous page.

Bandwidth Management >> Quality of Service

Class Index #1
 Name Tag Outbound Packets as:

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 <input type="radio"/>	Active	172.16.1.240 ~ 172.16.1.241	Any	ANY	ANY

8. Do the same steps to add class rules for IPTV and Data/Email with IP addresses as shown below.

Bandwidth Management >> Quality of Service

Class Index #2
 Name Tag Outbound Packets as:

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 <input type="radio"/>	Active	172.16.1.242 ~ 172.16.1.249	Any	ANY	ANY

and

Bandwidth Management >> Quality of Service

Class Index #3
 Name Tag Outbound Packets as:

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 <input type="radio"/>	Active	Any	Any	ANY	NFS(UDP:2049)

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

[Set to Factory Default](#)

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	--Kbps/--Kbps	Both	25%	25%	25%	25%	Inactive	Status	Setup
WAN2	Disable	100000Kbps/100000Kbps	Both	25%	25%	25%	25%	Inactive	Status	Setup
WAN3	Disable	100000Kbps/100000Kbps	Both	25%	25%	25%	25%	Inactive	Status	Setup
WAN4	Disable	100000Kbps/100000Kbps	Both	25%	25%	25%	25%	Inactive	Status	Setup

- 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**.

Bandwidth Management >> Quality of Service

WAN1 General Setup

Enable the QoS Control BOTH ▾

Index	Class Name	Reserved Bandwidth Ratio
Class 1	VoIP	30 %
Class 2	IPTV	50 %
Class 3	Data/Email	15 %
	Others	5 %

Enable UDP Bandwidth Control Limited_bandwidth Ratio %
 Outbound TCP ACK Prioritize

Note:

- Before enable QoS, you should test the real bandwidth first. QoS may not work properly if the bandwidth is not accurate.
- You can do speed test by <http://speedtest.net> or contact with your ISP for speed test program.

OK Clear Cancel

- Click OK to save the settings. The class rules for WAN1 are defined as shown below.

Bandwidth Management >> Quality of Service

General Setup

| [Set to Factory Default](#) |

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Enable	--Kbps/--Kbps	Both	30%	50%	15%	5%	Active	Status	Setup
WAN2	Disable	100000Kbps/100000Kbps	Both	25%	25%	25%	25%	Inactive	Status	Setup
WAN3	Disable	100000Kbps/100000Kbps	Both	25%	25%	25%	25%	Inactive	Status	Setup
WAN4	Disable	100000Kbps/100000Kbps	Both	25%	25%	25%	25%	Inactive	Status	Setup

VI-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

- Firewall
- User Management**
- General Setup
- User Profile
- User Group
- User Online Status
- Object Settings

VI-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.

User Management >> General Setup

General Setup

Mode Selection:

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

Authentication page:

Web Authentication: HTTPS HTTP

Login Page Logo: Upload a file Default Blank 擇檔案 (Max 524 × 352 pixel) Upload

Login Page Greeting: Upload a file

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

Landing page:

(Max 255 characters) Preview Set to Factory Default

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

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Mode	<p>There are two modes offered here for you to choose. Each mode will bring different filtering effect to the users involved.</p> <p>User-Based - If you choose such mode, the router will apply the filter rules configured in User Management>>User Profile to the users.</p> <p>Rule-Based -If you choose such mode, the router will apply the filter rules configured in Firewall>>General Setup and</p>

	Filter Rule to the users.
Authentication page	<p>Web Authentication - Choose the protocol for web authentication.</p> <p>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.</p> <p>Login Page Greeting - Such link allows you to access into the setting page for login greeting. For detailed information, refer to System Maintenance>>Login Page Greeting.</p> <p>Display IP Address on tracking window - Check the box to display the IP address of the client on the tracking window.</p>
Landing Page	Type the information to be displayed on the first web page when the LAN user accessing into Internet via such router.

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

VI-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**.

User Management >> User Profile

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

Profile	Enable	Name	Profile	Enable	Name
1.	<input checked="" type="checkbox"/>	admin	17.	<input type="checkbox"/>	
2.	<input checked="" type="checkbox"/>	Dial-In User	18.	<input type="checkbox"/>	
3.	<input type="checkbox"/>		19.	<input type="checkbox"/>	
4.	<input type="checkbox"/>		20.	<input type="checkbox"/>	
5.	<input type="checkbox"/>		21.	<input type="checkbox"/>	
6.	<input type="checkbox"/>		22.	<input type="checkbox"/>	
7.	<input type="checkbox"/>		23.	<input type="checkbox"/>	
8.	<input type="checkbox"/>		24.	<input type="checkbox"/>	
9.	<input type="checkbox"/>		25.	<input type="checkbox"/>	
10.	<input type="checkbox"/>		26.	<input type="checkbox"/>	
11.	<input type="checkbox"/>		27.	<input type="checkbox"/>	
12.	<input type="checkbox"/>		28.	<input type="checkbox"/>	
13.	<input type="checkbox"/>		29.	<input type="checkbox"/>	
14.	<input type="checkbox"/>		30.	<input type="checkbox"/>	
15.	<input type="checkbox"/>		31.	<input type="checkbox"/>	
16.	<input type="checkbox"/>		32.	<input type="checkbox"/>	

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

Note:

- 1.admin: To change the administrator password,please go to System Maintenance >> Administrator Password.
- 2.Dial-In User Profile: Dial-In User Profile is reserved for VPN authentication.
- 3.During authentication,Router will check all the local user profiles first,and then the profiles in

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.

Profile Index 3

1. Common Settings

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

2. Web login Setting

Idle Timeout	<input type="text" value="10"/> min(s) 0:Unlimited
Max User Login	<input type="text" value="0"/> 0:Unlimited
External Server Authentication	<input type="text" value="None"/>
Log	<input type="text" value="None"/>
Pop Browser Tracking Window	<input checked="" type="checkbox"/>
Authentication	<input checked="" type="checkbox"/> Web <input checked="" type="checkbox"/> Alert Tool <input checked="" type="checkbox"/> Telnet
Landing Page	<input type="checkbox"/>
Login Permission Schedule (Index: 1-15):	<input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>
Auto Logout every <input type="text" value="0"/> minutes (0~65535) (0:Off)	
<input type="checkbox"/> Enable Time Quota 0 min.	<input type="text" value="0"/> min.
<input type="checkbox"/> Enable Data Quota 0 MB	<input type="text" value="0"/> MB
Reset quota automatically	
<input type="checkbox"/> Enable	Default Time Quota <input type="text" value="0"/> min. Default Data Quota <input type="text" value="0"/> MB
Quota reset	<input checked="" type="radio"/> when login permission schedule expired <input type="radio"/> at the start time of Schedule (Index: 1-15): <input type="text"/>

3. Internal Services

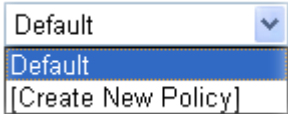
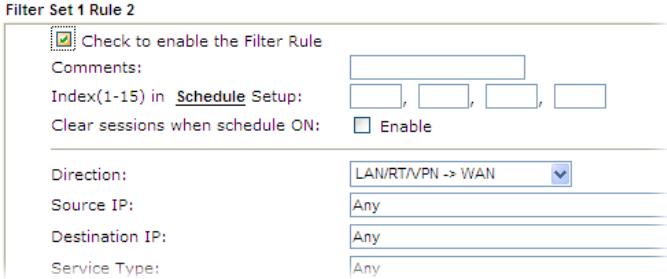
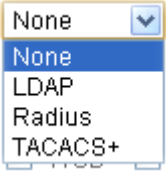
<input type="checkbox"/> Internal RADIUS	<input type="checkbox"/> Local 802.1X
--	---------------------------------------

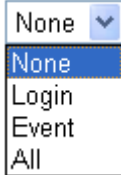


Note:

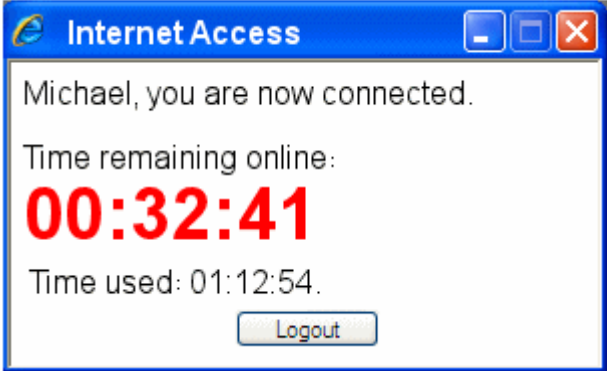
Internal Services means the account and password of this user profile can be used by other application.

Available settings are explained as follows:

Item	Description
Enable this account	Check this box to enable such user profile.
User Name	Type a name for such user profile (e.g., 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., lug123, wug123, wug456, 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

	<p>authentication, he/she can access Internet via this router with the limitation configured in this user profile.</p> <p>The maximum length of the password you can set is 24 characters.</p>
Confirm Password	Type the password again for confirmation.
Idle Timeout	If the user is idle over the limitation of the timer, the network connection will be stopped for such user . By default, the Idle Timeout is set to 10 minutes.
Max User Login	Such profile can be used by many users. You can set the limitation for the number of users accessing Internet with the conditions of such profile. The default setting is 0 which means no limitation in the number of users.
Policy	<p>It is available only when User-Based mode selected in User Management>>General Setup.</p>  <p>Default - If you choose such item, the filter rules pre-configured in Firewall can be adopted for such user profile.</p> <p>Create New Policy - If you choose such item, the following page will be popped up for you to define another filter rule as a new policy.</p> <p>Firewall >> Edit Filter Set >> Edit Filter Rule</p>  <p>For the detailed configuration, simply refer to Firewall>>Filter Rule. The firewall filter rules that are not selected in Firewall>>General>>Default rule can be available for use in User Management>>User Profile.</p>
External Service Authentication	<p>The router will authenticate the dial-in user by itself or by external service such as LDAP server or Radius server or TACACS+ server. If LDAP, Radius or TACACS+ is selected here, it is not necessary to configure the password setting above.</p> 
Log	Time of login/log out, block/unblock for the user(s) can be sent to and displayed in Syslog. Please choose any one of the log items to take down relational records for the user(s).

	
Pop Browser Tracking Window	If such function is enabled, a pop up window will be displayed on the screen with time remaining for connection if Idle Timeout is set. However, the system will update the time periodically to keep the connection always on. Thus, Idle Timeout will not interrupt the network connection.
Authentication	<p>Any user (from LAN side or WLAN side) tries to connect to Internet via Vigor router must be authenticated by the router first. There are three ways offered by the router for the user to choose for authentication.</p> <p>Web - If it is selected, the user can type the URL of the router from any browser. Then, a login window will be popped up and ask the user to type the user name and password for authentication. If succeed, a Welcome Message (configured in User Management >> General Setup) will be displayed. After authentication, the destination URL (if requested by the user) will be guided automatically by the router.</p> <p>Alert Tool - If it is selected, the user can open Alert Tool and type the user name and password for authentication. A window with remaining time of connection for such user will be displayed. Next, the user can access Internet through any browser on Windows. Note that Alert Tool can be downloaded from DrayTek web site.</p> <p>Telnet - If it is selected, the user can use Telnet command to perform the authentication job.</p>
Landing Page	<p>When a user tries to access into the web user interface of Vigor router series with the user name and password specified in this profile, he/she will be lead into the web page configured in Landing Page field in User Management>>General Setup.</p> <p>Check this box to enable such function.</p>
Login Permission Schedule (Index: 1-15)	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.
Auto Logout every...	Such account will be forced to logout after a certain time set here.
Enable Time Quota	<p>Time quota means the total connection time allowed by the router for the user with such profile. Check the box to enable the function of time quota. The first box displays the remaining time of the network connection. The second box allows to type the number of time (unit is minute) which is available for the user (using such profile) to access Internet.</p> <p> - Click this box to set and increase the time quota for such profile.</p> <p> - Click this box to decrease the time quota for such profile.</p> <p>Note: A dialog will be popped up to notify how many</p>

	<p>time remained when a user accesses into Internet through Vigor router successfully.</p>  <p>When the time is up, all the connection jobs including network, IM, social media, facebook, and etc. will be terminated.</p>
<p>Enable Data Quota</p>	<p>Data Quota means the total amount for data transmission allowed for the user. The unit is MB/GB.</p> <p><input type="checkbox"/> + - Click this box to set and increase the data quota for such profile.</p> <p><input type="checkbox"/> - - Click this box to decrease the data quota for such profile.</p>
<p>Reset quota automatically</p>	<p>Enable - Set default time quota and data quota for such profile. Vigor router will reset the quota automatically according to the factory quota settings.</p> <ul style="list-style-type: none"> ● Default Time Quota - Type the value for the time manually. ● Default Data Quota - Type the value for the data manually. <p>Quota reset - when login permission schedule expired - When the scheduling time is up, the router will reset the quota with user-defined time/data values automatically.</p> <p>Quota reset - at the start time of Schedule - The router will reset the quota with user-defined time/data values at the starting time configured in the selected schedule profile.</p>
<p>Internal RADIUS</p>	<p>Check the box to enable security authenticated via internal RADIUS server.</p>
<p>Local 802.1X</p>	<p>Check the box to enable security authenticated via internal 802.1X server.</p>

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

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

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

User Management >> User Group

Profile Index : 1

Name:

Available User Objects

1-admin
 2-Dial-In User
 3-LAN_User_Group_1
 4-WLAN_User_Group_A
 5-WLAN_User_Group_B

Selected User Objects(Max 32 Objects)

Available settings are explained as follows:

Item	Description
Name	Type a name for this user group.
Available User Objects	You can gather user profiles (objects) from User Profile page within one user group. All the available user objects that you have created will be shown in this box. Notice that user object, Admin and Dial-In User are factory settings. User defined profiles will be numbered with 3, 4, 5 and so on.

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

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

VI-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.

User Management >> User Online Status

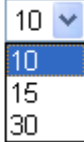
Current Time : 01-01 00:43:24 Refresh Seconds: Page: | [Refresh](#) |

Index	User	IP Address	Profile	Last Login Time	Expired Time	Data Quota	Idle Time	Action
1	admin	192.168.1.5	admin	01-01 00:00:15	Unlimited	Unlimited	Unlimited	Block Logout Delete

- Note:**
1. Please click "IP Address" to view all online users.
 2. Dial-in User profiles are linked to VPN clients and therefore cannot be logged-out or deleted while connecting.
 3. Information about 802.1X authentication can be found at [Authentication User List](#).

Total Number : 1

Available settings are explained as follows:

Item	Description
Refresh Seconds	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically. Refresh Seconds: <input type="text" value="10"/> 
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.
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.

User Management >> General Setup

General Setup

Mode Selection:

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

Notice for User-Based mode:

- In User-Based mode, **Active Rules** in Firewall will be applied to all LAN clients, packets that matches the Active Rules will be blocked or pass immediately, no user authentication is required.
- Only **Inactive Rules** in Firewall can be set for individual user profile. In User-Based mode, packets that do not match Active Rules will need authentication, and the Inactive Rule applied to the specific user profile will then take effect.

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**.

User Management >>User Profile

Profile Index 3

1. Common Settings

<input checked="" type="checkbox"/> Enable this account	
Username	<input type="text" value="user1"/>
Password	<input type="password" value="*****"/>
Confirm Password	<input type="password" value="*****"/>

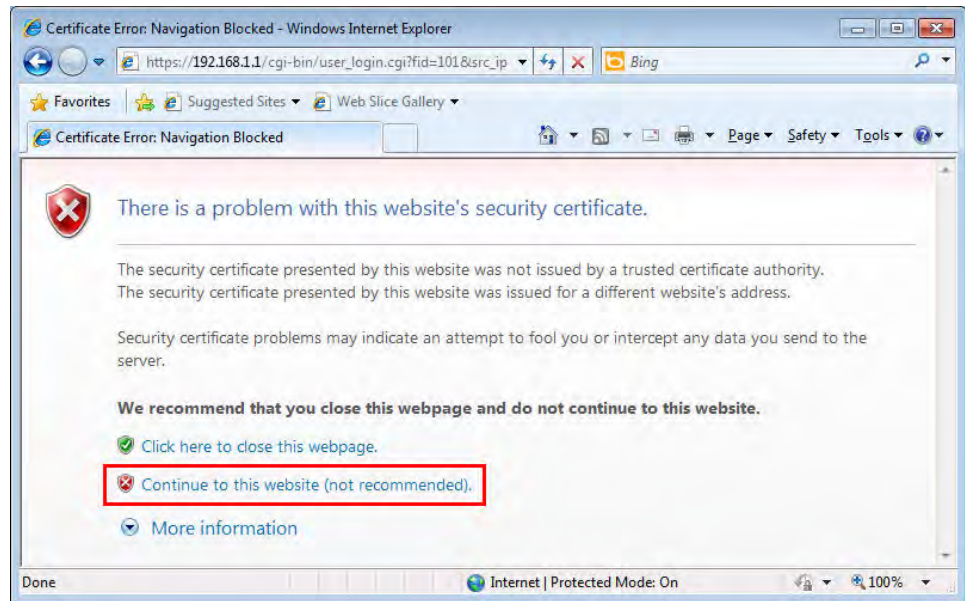
2. Web login Setting

Idle Timeout	<input type="text" value="10"/>	min(s) 0:Unlimited		
Max User Login	<input type="text" value="1"/>	0:Unlimited		
Policy	<input type="text" value="Default"/>			
External Server Authentication				
Log	<input type="text" value="None"/>			
Pop Browser Tracking Window	<input checked="" type="checkbox"/>			
Authentication	<input checked="" type="checkbox"/> Web <input checked="" type="checkbox"/> Alert Tool <input checked="" type="checkbox"/> Telnet			
Limiting Page				
Login Permission Schedule (Index: 1-15):	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>
Auto Logout every	<input type="text" value="0"/>	minutes (0~65535) (0:Off)		
<input checked="" type="checkbox"/> Enable Time Quota	0	min.	<input type="text" value="120"/>	min.
<input type="checkbox"/> Enable Data Quota	0	MB	<input type="text" value="0"/>	MB

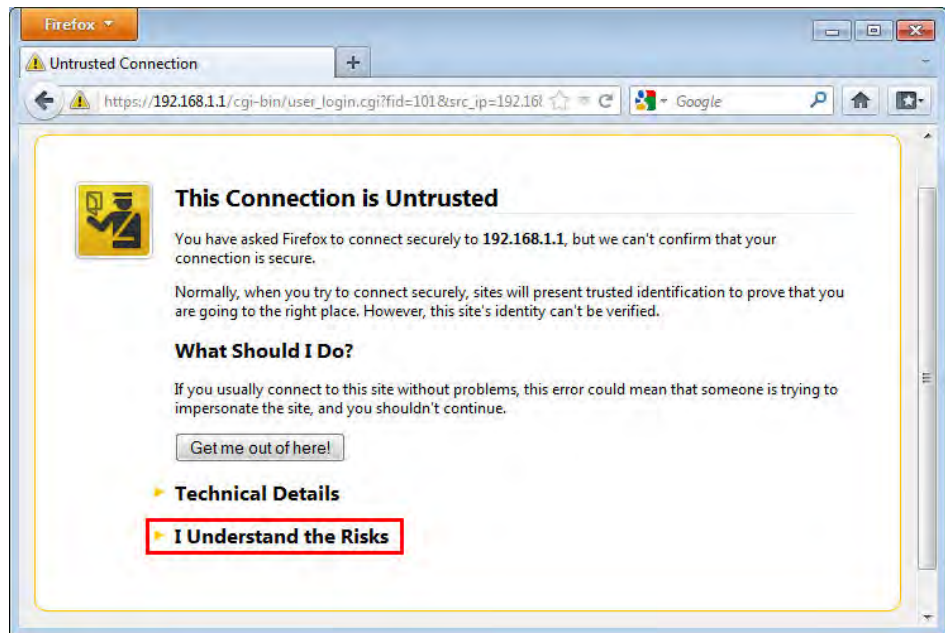
Authentication via Web

- 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.

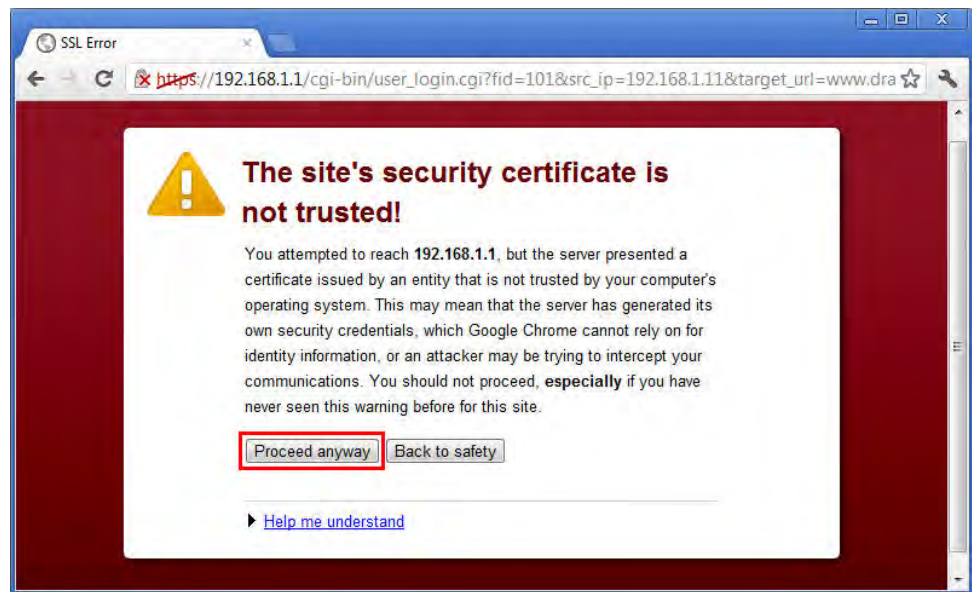
- With Microsoft Internet Explorer, you may get the following warning message. Please press **Continue to this website (not recommended)**.



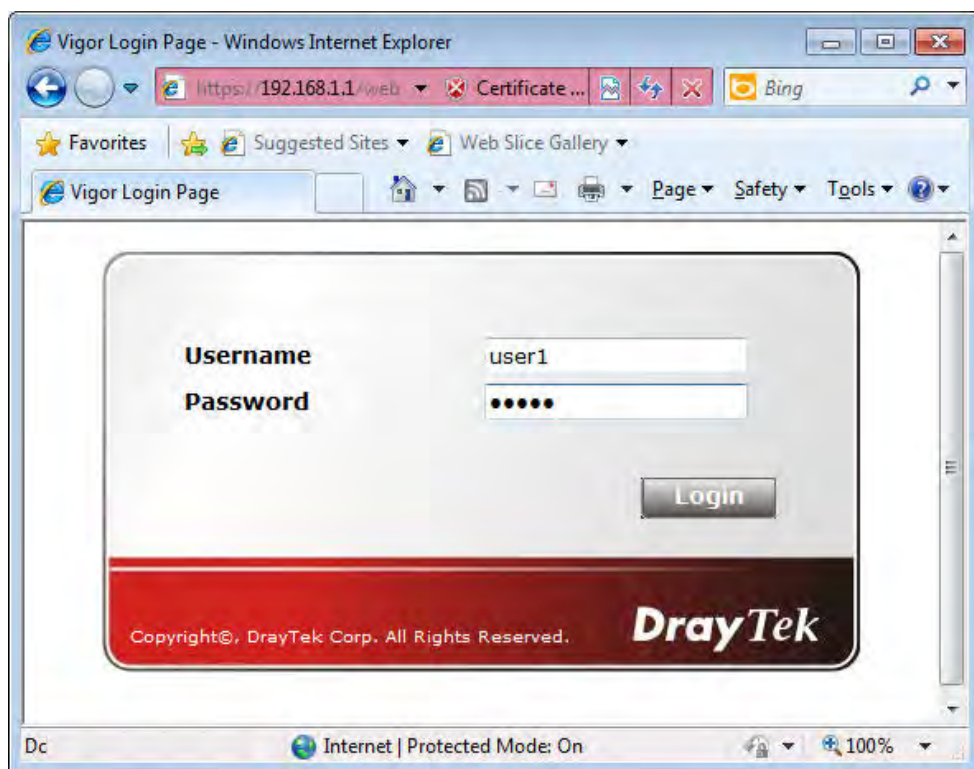
- With Mozilla Firefox, you may get the following warning message. Select **I Understand the Risks**.



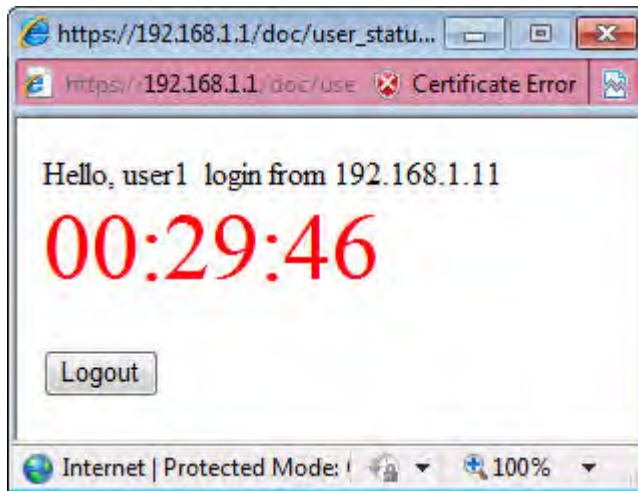
- With Chrome browser, you may get the following warning. Click Proceed anyway.



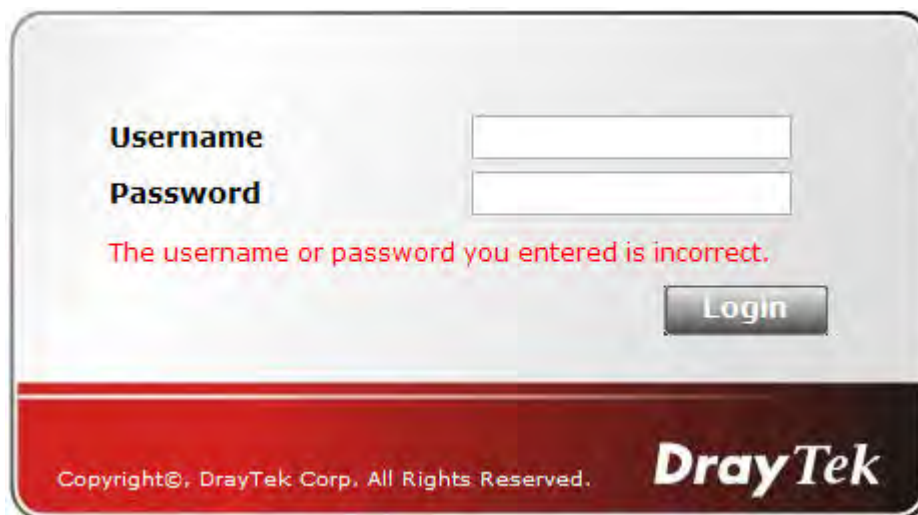
After that, the web authentication window will appear. Input the user name and the password for your account (defined in User Management) and click Login.



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

Mode Selection:

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

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

Notice for User-Based mode:

- In User-Based mode, **Active Rules** in Firewall will be applied to all LAN clients, packets that matches the Active Rules will be blocked or pass immediately, no user authentication is required.
- Only **Inactive Rules** in Firewall can be set for individual user profile. In User-Based mode, packets that do not match Active Rules will need authentication, and the Inactive Rule applied to the specific user profile will then take effect.

Authentication page:

Web Authentication: HTTPS HTTP

Login Page Logo: (Max 524 × 352 pixel)

Login Page Greeting

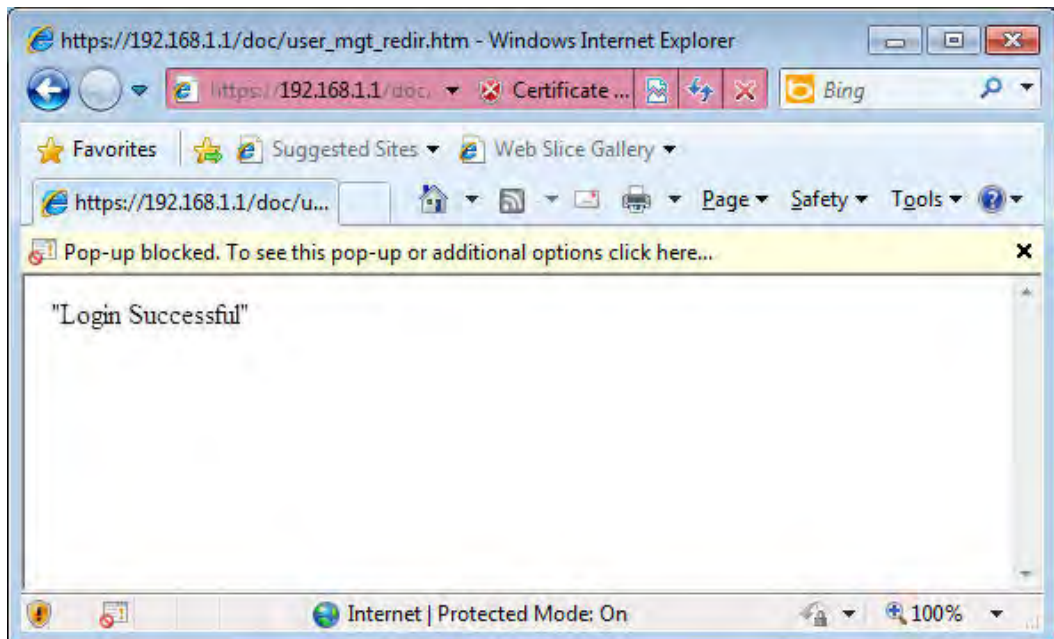
Display IP address on the dialog box pops up after successful login.

Landing page:

(Max 255 characters)

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

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.

VPN and Remote Access >> Remote Dial-in User

The screenshot shows the configuration interface for a Remote Dial-in User. The window is titled "Index No. 1" and "VPN and Remote Access >> Remote Dial-in User". It is divided into several sections:

- User account and Authentication:** Includes "Enable this account" (checked), "Idle Timeout" (300 seconds), and "Enable Mobile One-Time Passwords(mOTP)" (unchecked).
- Allowed Dial-In Type:** Lists various tunnel types: PPTP (checked), IPsec Tunnel (checked), L2TP with IPsec Policy (None), **SSL Tunnel (checked and highlighted with a red box)**, and OpenVPN Tunnel (checked). There are also options for "Specify Remote Node", "Remote Client IP", "or Peer ID", "Netbios Naming Packet" (Pass/Block), and "Multicast via VPN" (Pass/Block).
- IKE Authentication Method:** Includes "Pre-Shared Key" (checked) and "Digital Signature(X.509)" (unchecked).
- IPsec Security Method:** Includes "Medium(AH)" (checked), "High(ESP)" (checked), and "Local ID (optional)".

At the bottom of the window are "OK", "Clear", and "Cancel" buttons.

- 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.

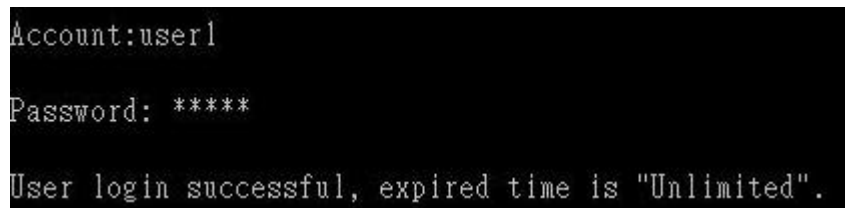
Authentication via Telnet

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.

User Management >>User Profile

Profile Index 3

1. Common Settings

<input checked="" type="checkbox"/> Enable this account	
Username	user1
Password	*****
Confirm Password	*****

2. Web login Setting

Idle Timeout	10	min(s)	0:Unlimited
Max User Login	1		0:Unlimited
Policy	Default		
<small>The selection of items could be created as rules and which not set to active.</small>			
External Server Authentication	None		
Log	None		
Pop Browser Tracking Window	<input checked="" type="checkbox"/>		
Authentication	<input checked="" type="checkbox"/> Web	<input checked="" type="checkbox"/> Alert Tool	<input checked="" type="checkbox"/> Telnet
Landing Page			
Login Permission	Schedule (Index: 1-15):		
Auto Logout every		minutes (0-65535) (0:Off)	
<input checked="" type="checkbox"/> Enable Time Quota	0	min.	+ - 0 min.
<input type="checkbox"/> Enable Data Quota	0	MB	+ - 0 MB

4. If the Time Quota is set with "0" minute, you will get the following message which means this account has no time quota.

```
Account:user1
Password: *****
User's time is up, or it has not enough time quota.
```

If the Time Quota is enabled and time is *not* 0 minute,

User Management >>User Profile

Profile Index 3

1. Common Settings

<input checked="" type="checkbox"/> Enable this account	
Username	user1
Password	*****
Confirm Password	*****

2. Web login Setting

Idle Timeout	10	min(s) 0:Unlimited
Max User Login	1	0:Unlimited
Policy	Default	
	The selection of items could be created as rules and which not set to active.	
External Server Authentication	None	
Log	None	
Pop Browser Tracking Window	<input checked="" type="checkbox"/>	
Authentication	<input checked="" type="checkbox"/> Web <input checked="" type="checkbox"/> Alert Tool <input checked="" type="checkbox"/> Telnet	
Landing Page		
Login Permission	Schedule (Index: 1-15):	
Auto Logout every	0	minutes (0-65535) (0:Off)
<input checked="" type="checkbox"/> Enable Time Quota	0	min. + - 120 min.
<input type="checkbox"/> Enable Data Quota	0	MB + - 0 MB

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.

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 Vigor2862 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 Vigor2862.
2. 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.

General Setup

Mode Selection:

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

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

Notice for User-Based mode:

- In User-Based mode, **Active Rules** in Firewall will be applied to all LAN clients, packets that matches the Active Rules will be blocked or pass immediately, no user authentication is required.
- Only **Inactive Rules** in Firewall can be set for individual user profile. In User-Based mode, packets that do not match Active Rules will need authentication, and the Inactive Rule applied to the specific user profile will then take effect.

Authentication page:

Web Authentication: HTTPS HTTP

Login Page Logo: (Max 524 × 352 pixel)

Login Page Greeting

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

Landing page:

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

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

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.

User Management >> User Profile

User Profile Table

Profile	Name
1.	admin
2.	Dial-In User
3.	
4.	

- In the following page, check the box of **Landing page** and click **OK** to save the settings.

User Management >>User Profile

Profile Index 3

1. Common Settings

<input checked="" type="checkbox"/> Enable this account	
Username	CaCa
Password	*****
Confirm Password	*****

2. Web login Setting **User Online Status : Block/ Unblock**

Idle Timeout	10	min(s) 0:Unlimited
Max User Login	1	0:Unlimited
Policy	Default	
The selection of items could be created as rules and which not set to active.		
External Server Authentication	None	
Log	None	
Pop Browser Tracking Window	<input checked="" type="checkbox"/>	
Authentication	<input checked="" type="checkbox"/> Web	<input checked="" type="checkbox"/> Alert Tool <input checked="" type="checkbox"/> Telnet
Landing Page	<input checked="" type="checkbox"/>	
Login Permission Schedule (Index: 1-15):		
Auto Logout every	0	minutes (0~65535) (0:Off)

- 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.

- 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>` ”

General Setup

Mode Selection:

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

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

Notice for User-Based mode:

- In User-Based mode, **Active Rules** in Firewall will be applied to all LAN clients, packets that matches the Active Rules will be blocked or pass immediately, no user authentication is required.
- Only **Inactive Rules** in Firewall can be set for individual user profile. In User-Based mode, packets that do not match Active Rules will need authentication, and the Inactive Rule applied to the specific user profile will then take effect.

Authentication page:

Web Authentication: HTTPS HTTP

Login Page Logo: (Max 524 × 352 pixel)

Login Page Greeting

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

Landing page:

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

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

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.

User Management >> User Profile

User Profile Table

Profile	Name
1.	admin
2.	Dial-In User
3.	
4.	

3. In the following page, check the box of Landing page and click OK to save the settings.

User Management >>User Profile

Profile Index 3

1. Common Settings

<input checked="" type="checkbox"/> Enable this account	
Username	CaCa
Password	*****
Confirm Password	*****

2. Web login Setting

User Online Status : Block/ Unblock

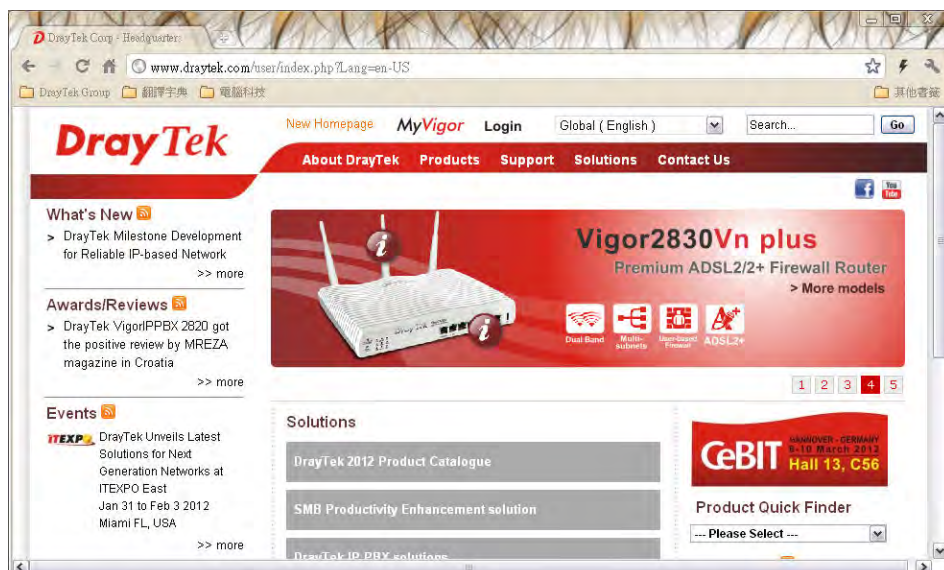
Idle Timeout	10	min(s) 0:Unlimited
Max User Login	1	0:Unlimited
Policy	Default	
<i>The selection of items could be created as rules and which not set to active.</i>		
External Server Authentication	None	
Log	None	
Pop Browser Tracking Window	<input checked="" type="checkbox"/>	
Authentication	<input checked="" type="checkbox"/> Web <input checked="" type="checkbox"/> Alert Tool <input checked="" type="checkbox"/> Telnet	
Landing Page	<input checked="" type="checkbox"/>	
Login Permission Schedule (Index: 1-15):		
Auto Logout every		minutes (0-65535) (0:Off)

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.

Username: CaCa
Password: *****
Login

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

5. Click Login. If the logging is successful, you will be directed into the website of www.draytek.com.



VI-4 Hotspot Web Portal

The Hotspot Web Portal feature allows you to set up profiles so that LAN users could either be redirected to specific URLs, or be shown messages when they first connect to the Internet through the router. Users could be required to read and agree to terms and conditions, or authenticate themselves, prior to gaining access to the Internet. Other potential uses include the serving of advertisements and promotional materials, and broadcast of public service announcements.

Web User Interface



VI-4-1 Profile Setup

Select **Profile Setup** to create or modify Portal profiles. Up to 4 profiles can be created to meet different requirements according to LAN subnets, WLAN SSIDs, origin and destination IP addresses, etc.

Hotspot Web Portal >> Profile Setup



Hotspot Web Portal Profile:

Index	Enable	Comments	Login Mode	Applied Interface	
1.	<input type="checkbox"/>		Click-through	None	Preview
2.	<input type="checkbox"/>		Click-through	None	Preview
3.	<input type="checkbox"/>		Click-through	None	Preview
4.	<input type="checkbox"/>		Click-through	None	Preview

Note:

1. The router must connect to the Internet before webpage redirection will work.
2. If the LAN clients are using another DNS server on LAN, please make sure the DNS query for domain name "portal.draytek.com" will be resolved by the router.

[OK](#)

Available settings are explained as follows:

Item	Description
Index	Click the index number link to view or update the profile settings.
Enable	Check the box to enable the profile.
Comments	Shows the description of the profile.
Login Mode	Shows the login mode used by the profile. See the section <i>Login Mode</i> for details.

Applied Interface	Shows the interfaces to which this profile applies.
Preview	Click this button to preview the Hotspot Web Portal page that will be displayed to users.

VI-4-1-1 Login Modes

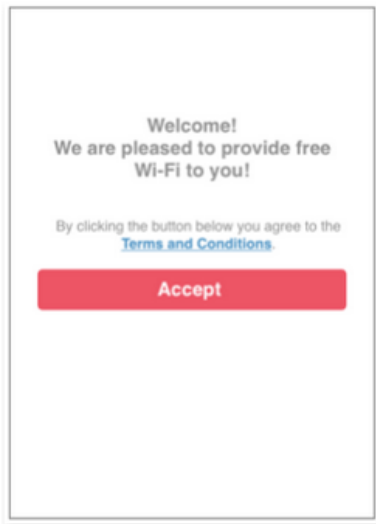
There are five login modes to choose from for authenticating network clients: **Skip Login**, **Click Through**, **Social Login**, **PIN Login**, and **Social or PIN Login**. Each login mode will present a different web page to users when they connect to the network.

Skip Login

This mode does not perform any authentication. The user will be redirected to the landing page. The user can then leave the landing page to visit other websites.

Click-through

The following page will be shown to the users when they first attempt to access the Internet through the router. After clicking **Accept** on the page, users will be directed to the landing page and be granted access to the Internet.



Social Login

The following page will appear when users attempt to access the Internet for the first time via the router. After authenticating themselves using either a Facebook or Google account, they will be directed to the landing page and be granted access to the Internet.

About This Login

Login with Facebook and Google account




Select Social Login

Login with Facebook

  Log in with Facebook

Login with Google

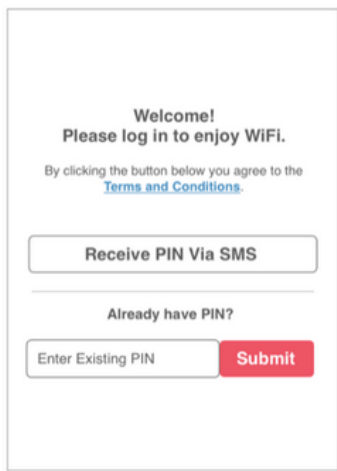
  Log in with Google

PIN Code Login

When users attempt to connect to the Internet for the first time, they will be prompted to enter a mobile number to receive a PIN by SMS. After they have authenticated themselves by entering the PIN, they will be redirected to the landing page, indicating that they have been granted Internet access.

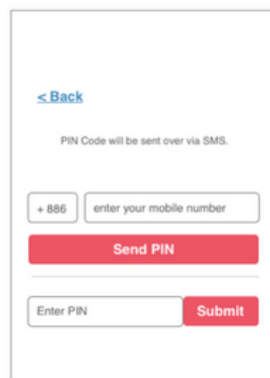
About This Login

Router can generate PIN and send to clients via SMS.



Receive PIN via SMS

Second page for entering mobile number to receive PIN

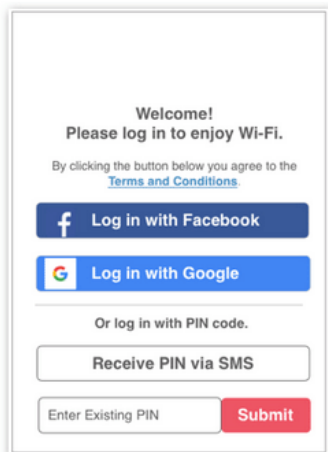


Social or PIN Login

This login mode presents both **Social Login** and **PIN Code Login** modes to the users, and allows them to select their preferred mode of authentication.

About This Login

Provide all kinds of login methods for Wi-Fi clients to choose.



Select Social Login

Login with Facebook

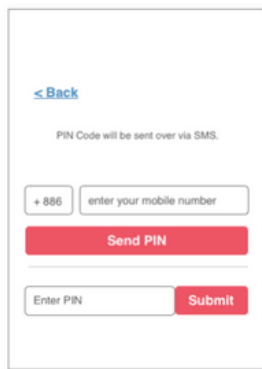
Login with Google

 Log in with Facebook

 Log in with Google

PIN Login

Second page for entering mobile number to receive PIN



VI-4-1-2 Steps for Configuring a Web Portal Profile

1. Login Method

Click the index link (e.g., #1) of the selected profile to display the following page.

Hotspot Web Portal >> Profile Setup



Enable this profile

Comments:

Choose Login Method

Available settings are explained as follows:

Item	Description
Enable this profile	Check to enable this profile.
Comments	Enter a brief description to identify this profile.
Choose Login	Select the desired Login Mode.

Method	
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to save the configuration on this page and proceed to the next page.

If you have chosen **Skip Login** as the Login Mode, skip to step 4 *Whitelisting* below.
Otherwise, proceed to configure the login page by following steps 2 and 3.

2. Background

If you have selected a Login Mode that requires authentication, select a background for the login page.



Choose Login Background


Color Background

Image Background

Login Page URL

Browser Table Title

Logo Image



Logo Background Color

(format : FFFFFFFF)

Login Method Background Color

(format : FFFFFFFF)

Available settings are explained as follows:

Item	Description
Choose Login	Select either Color Background or Image Background as the login

Background	page background scheme.
Login Page URL	Enter the URL for the login page.
Browser Tab Title	Enter the text to be shown as the webpage title in the browser.
Logo Image	The DrayTek Logo will be displayed by default. However, you can enter HTML text or upload an image to replace the default logo.
Logo Background Color	Select the background color of the logo from the predefined color list, or select Customize Color and enter the RGB values. Click Preview to preview the selected color.
Login Method Background Color	Select the background color of the login panel from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.
Opacity (10 ~ 100)	Available when Image Background is selected. Set the opacity of the background image.
Background Image	Available when Image Background is selected. Click Browse... to select an image file (.JPG or .PNG format), then click Upload to upload it to the router.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

If you have selected **Skip Login** as the Login Mode, proceed to Step 4 *Whitelist Setting*; otherwise, continue to Step 3 *Login Page Setup*.

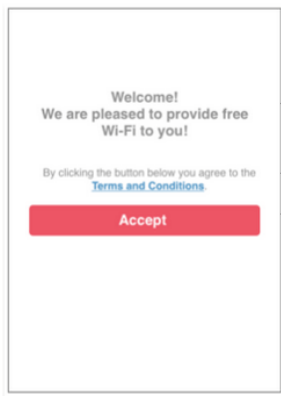
3. Login Page Setup

In this step you can configure settings for the login page.

Click Through

This section describes the Login Page setup if you have selected **Click Through** as the Login Mode.

Configure Login Method and Details



Welcome Message _____
 Terms and Conditions Description and Content _____
 Accept Button Description and Color _____

Welcome Message
 (Max 1360 characters)

Terms and Conditions Description
 (Max 170 characters)

Terms and Conditions Content
 (Max 170 characters)

Accept Button Description
 (Max 170 characters)

Accept Button Color (format : FFFFFFFF)

Available settings are explained as follows:

Item	Description
Welcome Message	Enter the text to be displayed as the welcome message.
Terms and Conditions Description	Enter the text to be displayed as the Terms and Conditions hyperlink text.
Terms and Conditions Content	Enter the text to be displayed in the Terms and Conditions pop-up window.
Accept Button Description	Enter the text to be displayed on the accept button
Accept Button Color	Select the color of the accept button from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

Social Login and PIN Login

This section describes the Login Page setup step if you have selected **PIN Login** and/or **Social Login** as the Login Mode. You will see only settings that are relevant to the selected login mode(s).



Configure Login Method and Details

- Welcome Message
- Terms and Conditions Description and Content
- Facebook Login
- Google Login
- Hint Message
- Receiving PIN via SMS Description
- Enter PIN and Submit Button

Welcome Message

Welcome!
We are pleased to provide free Wi-Fi to you!

(Max 1360 characters) Default

Terms and Conditions Description

By clicking the button below you agree to the Terms and Conditions.

(Max 170 characters) Default

Terms and Conditions Content

(Max 170 characters)

Settings that are common to Facebook, Google and PIN authentication are:

Item	Description
Welcome Message	Enter the text to be displayed as the welcome message.
Terms and Conditions Description	Enter the text to be displayed as the Terms and Conditions hyperlink text.
Terms and Conditions Content	Enter the text to be displayed in the Terms and Conditions pop-up window.

If you have selected Facebook login, these settings will appear:

Facebook Login Description
 (Max 170 characters) Default

Facebook APP ID

Facebook APP Secret

Item	Description
Facebook Login Description	Enter the text to be displayed on the Facebook login button.
Facebook APP ID	Enter a valid Facebook developer app ID. If you do not already have an app ID, refer to section A-1 <i>How to create a Facebook App ID for Web Portal Authentication</i> for instructions on obtaining an APP ID.
Facebook APP Secret	Enter the secret configured for the APP ID entered above. Refer to section A-1 <i>How to create a Facebook App ID for Web Portal Authentication</i> for details.

If you have selected Google login, these settings will appear:

Google Login Description
 (Max 170 characters) Default

Google App ID

Google App Secret

Item	Description
Google Login Description	Enter the text to be displayed on the Google login button.
Google App ID	Enter a valid Google app ID. If you do not already have an app ID, refer to section A-2 <i>How to create a Google App ID for Web Portal Authentication</i> for instructions on obtaining an APP ID.
Google App Secret	Enter the secret configured for the APP ID entered above. Refer to section A-2 <i>How to create a Google APP ID for Web Portal Authentication</i> for details.

If you have selected PIN login, these settings will appear:

Hint Message
(Max 170 characters)

Receiving PIN via SMS Description
(Max 170 characters)

Receiving PIN via SMS Content
(Max 150 characters)

Receiving PIN via SMS Provider Set SMS Provider in *Objects Setting >> SMS / Mail Service Object*

Enter PIN Description
(Max 170 characters)

Submit Button Description
(Max 170 characters)

Submit Button Color (format : FFFFFFFF)

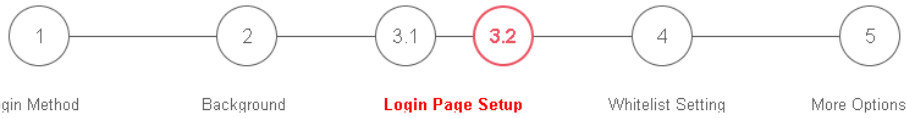
Item	Description
Hint Message	Enter the text used to suggest users to choose SMS authentication.
Receiving PIN via SMS Description	Enter the text to be displayed on the button that the user clicks to receive an SMS PIN.
Receiving PIN via SMS Content	Enter the message to be sent by SMS to inform the user of the PIN. The PIN variable is specified by <PIN> within the message.
Receiving PIN via SMS Provider	Select the SMS Provider used to send PIN notifications SMS providers are configured in Objects Setting >> SMS / Mail Service Object .
Enter PIN Description	Enter message to be displayed in the PIN textbox to prompt the user to enter the PIN.
Submit Button Description	Enter the text to be displayed on the submit PIN button
Submit Button Color	Select the color of the submit button from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.
Enter PIN Description	Enter message to be displayed in the PIN textbox to prompt the user to enter the PIN.

And finally, the save and cancel buttons are always displayed.

Item	Description
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

2nd-stage Page for PIN Login

If you have selected **PIN Login** as the login mode, you will also need to configure the page that is displayed to users when they request a PIN.



Configure 2nd-stage Page for SMS Login

[< Back](#)

PIN Code will be sent over via SMS.

+ 886

Send PIN

Submit

- Back Button
- PIN Code Message
- Default Country Code, Enter Mobile Number Description
- Send Button Description and Color
- Send Succeeded Message
- Enter PIN and Submit Button

Back Button Description

(Max 170 characters) Default

PIN Code Message

(Max 170 characters) Default

Default Country Code

Enter Mobile Number Description

(Max 170 characters) Default

Send Button Description

(Max 170 characters) Default

Send Button Color

(format : FFFFFFFF) Default

Send Succeeded Message

(Max 170 characters) Default

Available settings are explained as follows:

Item	Description
Back Button Description	Enter text for the label of the hyperlink to return to the previous page.
PIN Code Message	Enter text to be displayed as the body text on the page.
Default Country Code	Select the default country code to be displayed using the dropdown menu.

Enter Mobile Number Description	Enter message to be displayed in the mobile number textbox to prompt the user to enter the mobile number.
Send Button Description	Enter the label text of the send button.
Send Button Color	Select the color of the send button from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.
Send Succeeded Message	Enter text to be displayed to notify the user after the PIN has been sent.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

4. Whitelist Setting

In this step you can configure the whitelist settings. Users are allowed to send and receive traffic that satisfies whitelist settings.

Hotspot Web Portal >> Profile Setup



NAT Rules	Dest Domain	Dest IP	Dest Port	Source IP
Always allow outbound connections from hosts in		<input type="checkbox"/> NAT >> Port Redirection		
		<input type="checkbox"/> NAT >> Open Ports		
		<input type="checkbox"/> NAT >> DMZ		

Save and Next Cancel

Available settings are explained as follows:

Item	Description
NAT Rules	To prevent web portal settings from conflicting with NAT rules resulting in unexpected behavior, select the NAT rules that are allowed to bypass the web portal. Hosts listed in selected NAT rules can always access the Internet without being intercepted by the web portal.
Dest Domain	Enter up to 30 destination domains that are allowed to be accessed.
Dest IP	Enter up to 30 destination IP addresses that are allowed to be accessed.
Dest Port	Enter up to 30 destination protocols and ports that are allowed through the router.
Source IP	Enter up to 30 source IP addresses that are allowed through the router.

Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

5. More Options

In this step you can configure advanced options for the Hotspot Web Portal.

Hotspot Web Portal >> Profile Setup



Web Portal Options

Expired Time After Activation days hours min

HTTPS Redirection Enable

When an unauthenticated client opening a HTTPS page, redirect will work but certificate errors may be shown.
Disable this function to redirect only HTTP pages. HTTPS browsing will timeout without redirection and also no certificate errors.

Captive Portal Detection Enable

Trigger the unauthenticated client to automatically pop-up the Web Portal page when connects to Wi-Fi.
This function is not available when using **Social Login** because the page may not be shown correctly due to the limitation of the OS built-in Captive Portal Detection.

Landing Page After Authentication

Fixed URL

User Requested URL

Bulletin Message

(Max 511 characters)

Default Message

Note:

Landing Page may not be shown correctly when using OS built-in Captive Portal Detection.

Applied Interfaces

- Subnet LAN1 LAN2 LAN3 LAN4 LAN5 LAN6 LAN7 LAN8
- WLAN 2.4G SSID1 (DrayTek)
 SSID2 (DrayTek_Guest)
 SSID3
 SSID4
- 5G SSID1 (DrayTek_5G)
 SSID2 (DrayTek_5G_Guest)
 SSID3
 SSID4

Available settings are explained as follows:

Item	Description
Expired Time After Activation	Enter the time duration that users are allowed to have Internet access after logging in.
HTTPS Redirection	If this option is selected, unauthenticated clients accessing HTTPS websites will be redirected to the login page, but the browser may alert the user of certificate errors. If this option is not selected, attempts to access to HTTPS website will time out without redirection.
Captive Portal Detection	If this option is selected, the web portal page is triggered automatically when an unauthenticated client tries to access the Internet. This function is not available when the Login Mode is Social Login , as the web portal page may not be shown correctly due to the limitations of the operating system's built-in Captive Portal Detection.
Landing Page After Authentication	Specifies the webpage that will be displayed after the user has successfully authenticated. Fixed URL - The user will be redirected to the specified URL. This could be used for displaying advertisements to users, such as guests requesting wireless Internet access in a hotel. User Requested URL - The user will be redirected to the URL they initially requested. Bulletin Message -The message configured here will be briefly shown for a few seconds to the user. Default Message - This button is enabled when Bulletin Message is selected. Click to load the default text into the bulletin message textbox.
Applied Interfaces	Subnet - The current Hotspot Web Portal profile will be in effect for the selected subnets. WLAN - The current Hotspot Web Portal profile will be in effect for the selected WLAN SSIDs.
Cancel	Click to abort the configuration process and return to the profile summary page.
Finish	Click to complete the configuration.

VI-4-2 Users Information

The log information for users accessing into Internet through web portal will be shown on this page. Click a user link can open another web page displaying more detailed information.

VII-4-2-1 User Info

The page can display user information based on the filtering conditions (profile or login method).

Hotspot Web Portal >> Users Information

User Info
Database Setup

Select Columns to Filter Users

Profile	Login Method
<input checked="" type="checkbox"/> Profile 1	<input type="checkbox"/> Facebook
<input type="checkbox"/> Profile 2	<input type="checkbox"/> Google
<input checked="" type="checkbox"/> Profile 3	<input type="checkbox"/> Pincode
<input type="checkbox"/> Profile 4	<input type="checkbox"/> Click

User Table Auto Refresh (per min) | [Refresh Now](#) |

2 Online Users / 3 All Users

Index	Status	Profile	User	Login Methods	IP	MAC	Email	Phone Nur
1	Online	2	██████████	facebook	192.168.1.11	6c:8d:c1:45:25:9a	██████████	-
2	Offline	1	6c:8d:c1:45:25:9a	click-through	192.168.1.11	6c:8d:c1:45:25:9a	-	-
3	Online	1	2c:f0:a2:8b:cb:ab	click-through	192.168.1.12	2c:f0:a2:8b:cb:ab	-	-

Available settings are explained as follows:

Item	Description
Select Columns to Filter Users	Simply specify the profile and the login method for filtering users who want to access Internet through the login method. It is useful for system administrator to manage the user's access based on different conditions when there are a lot of users requiring to access into Internet.
User Table	Information for the users accessing into Internet via Hotspot Web Portal will be displayed and recorded in this page.

Click the MAC address link for certain user, information page related to the selected device will be shown as the following page.

6c:8d:c1:45:25:9a**Login Info**

User Name	Login Methods	ID	Email	Phone
6c:8d:c1:45:25:9a	click-through	6c:8d:c1:45:25:9a	-	-

Devices

Log Out Device

Index	Status	IP	MAC	Online Time
<input type="checkbox"/> 1	Offline	192.168.1.11	6c:8d:c1:45:25:9a	

Login History (Latest 10 entries)

Index	Login	Logout	Duration	IP	MAC
1	2017-09-29 10:30:02	2017-09-29 10:30:53	00d 00h:00m	192.168.1.11	6c:8d:c1:45:25:9a

OK

Basic information for the device will be shown on the field of Login Info; online/offline status for the device can be send on the field of Devices; and historical information for device login will be shown on the field of Login History. In addition, to forcefully log out a selected device, simply check the one you want to logout and click the Log Out Device button.

VII-4-2-2 Database Setup

This page allows the user to configure settings for database on USB disk.

Hotspot Web Portal >> Users Information

User Info	Database Setup
-----------	----------------

Enable database to record user information

File Path : /db

Database Usage : 0.2MB / 50MB

Notification and Action when Storage Exceeded

Notification

Don't send notification

Send notification

Email Notification Object 1 - ??? ▾

SMS Notification Object 1 - 11111 ▾

Action

Stop recording user information

Backup and clean up all user info, and start a new record

Available settings are explained as follows:

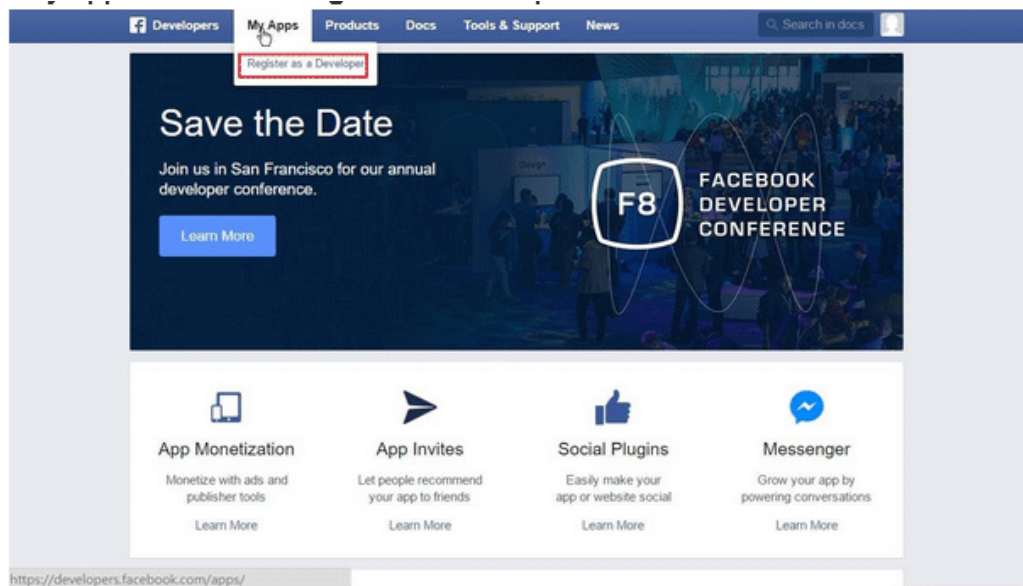
Item	Description
Enable database to record user information	Check the box to record user information on router's database. Before checking this box, insert a USB disk with adequate storage space, first.
File Path	If a USB disk has been inserted into the USB port of Vigor router, the file path will be shown in this area.
Database Usage	Display the usage and remaining space on the database. Clear User Info - The user information will be displayed on the page of User Info. You can delete the information by clicking this button.
Notification and Action when Storage Exceeded	
Notification	Don't send notification - Vigor router system will not send any notification to any recipient. Send notification - Vigor router system will not send a notification e-mail to specified recipient(s) that selected from Email Notification Object and SMS Notification Object .
Action	Stop recording user information - Vigor router system will stop to record the user information onto USB disk. Backup and clean up all user info, and start a new record - Vigor router system will backup all existed information on the USB disk onto the host and clean up the information from USB disk. Later, it will start a new record.

Application Notes

A-1 How to create Facebook APP for Web Portal Authentication?

The new web portal feature support social login as authentication method, and allows network administrator to authenticate LAN clients by their Google or Facebook account. This document introduces how to create Facebook APP, and generate the APP ID and APP secret that can be used in Web Portal setup.

1. Register as FB Developer: Go to <https://developers.facebook.com/> and login the FB account.
2. Register the Facebook account as a Developer (If the account has been verified previously, this step can be skipped.)
3. Click My Apps then choose Register as Developer.



4. Switch to YES then click Next on pop-up window.



5. Choose country then type phone number, click Send as Text in Get Confirmation Code. Wait confirmation code message received then enter the confirmation code. Click Register to finish the register process.

Register as a Facebook Developer ✕

We need to verify your account to complete your registration. Your Phone number will be added to your timeline but won't be visible to your friends.

Country: Taiwan (+886) Phone number: 0912345678

Get Confirmation Code

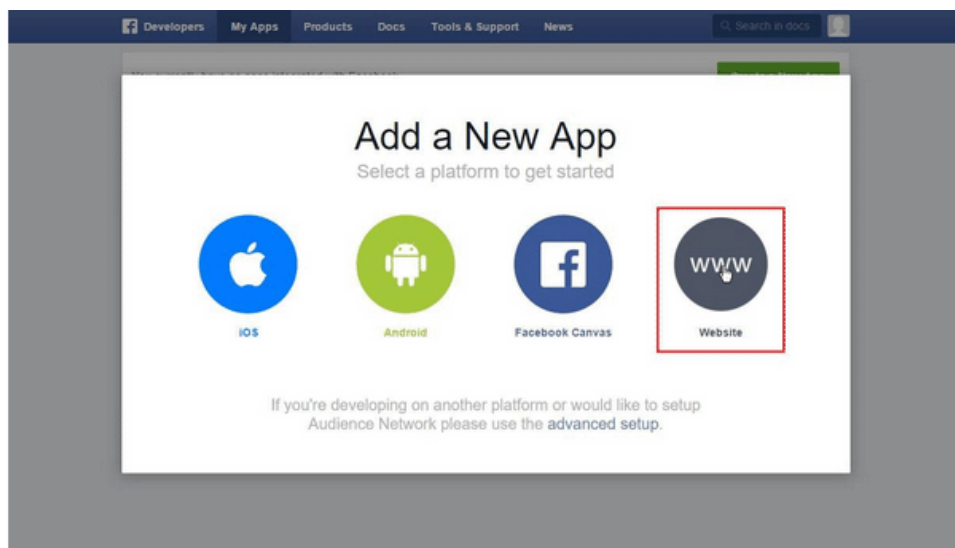
Send as Text Send via Phone Call

Confirmation code: 625535

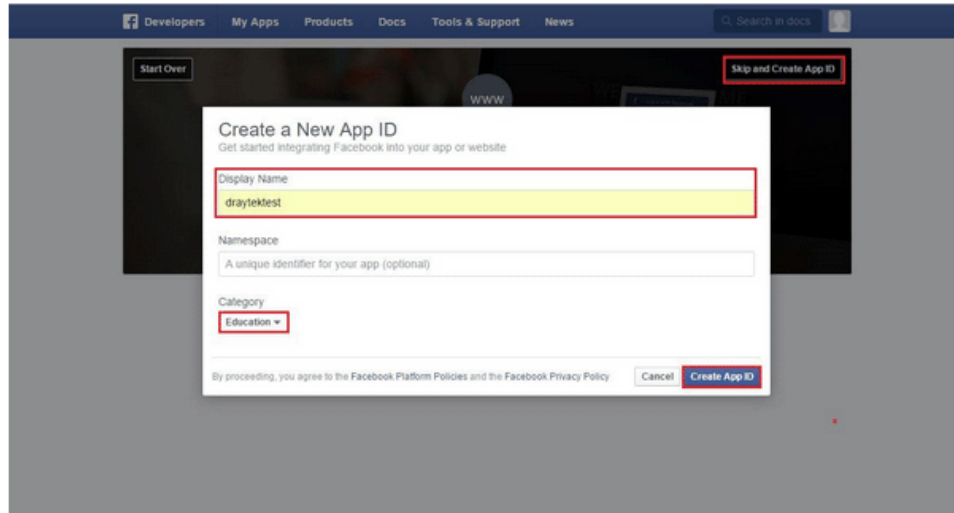
You can also verify your account by adding a credit card. [?]

Go Back Register

6. Add a New App. Click on My Apps > Add a New App. Choose Website platform.



7. Click Skip and Create App ID on first use. Type Display Name. Choose Category. Click Create App ID.



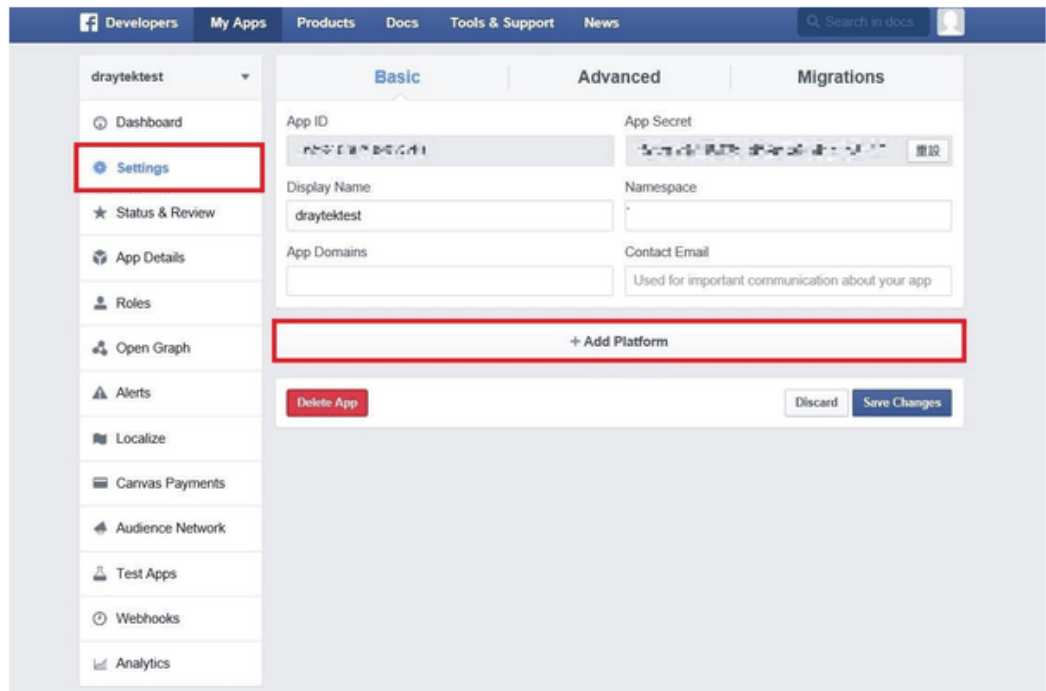
8. Pops up security check window, select the answer, and then click Submit to finish the process.



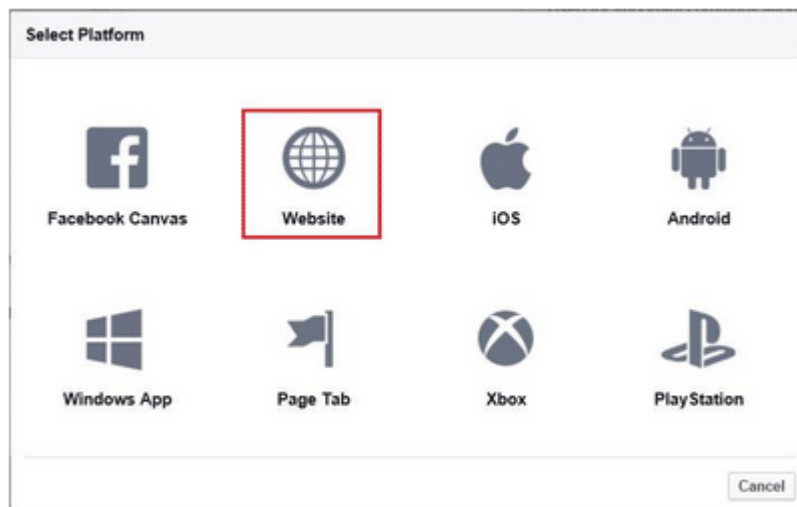
- On Dashboard, user can get **App ID** and **App Secret**, these information will be used in Vigor Router's Web Portal Setup.



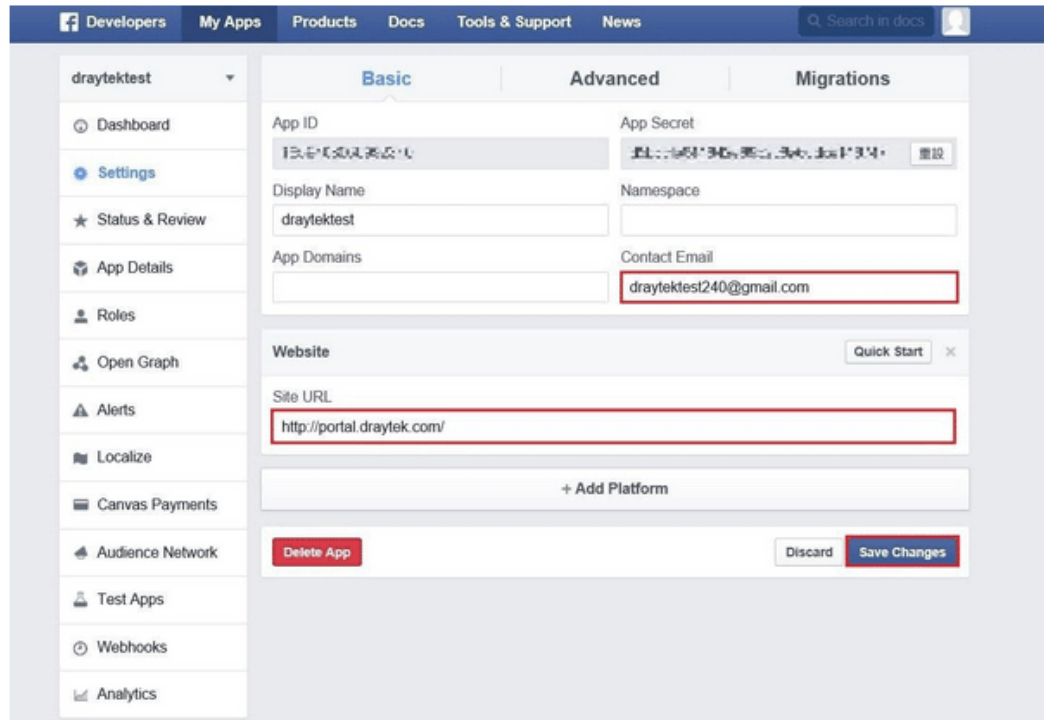
- Add Platform on My Apps. Go to Settings then click **Add Platform**.



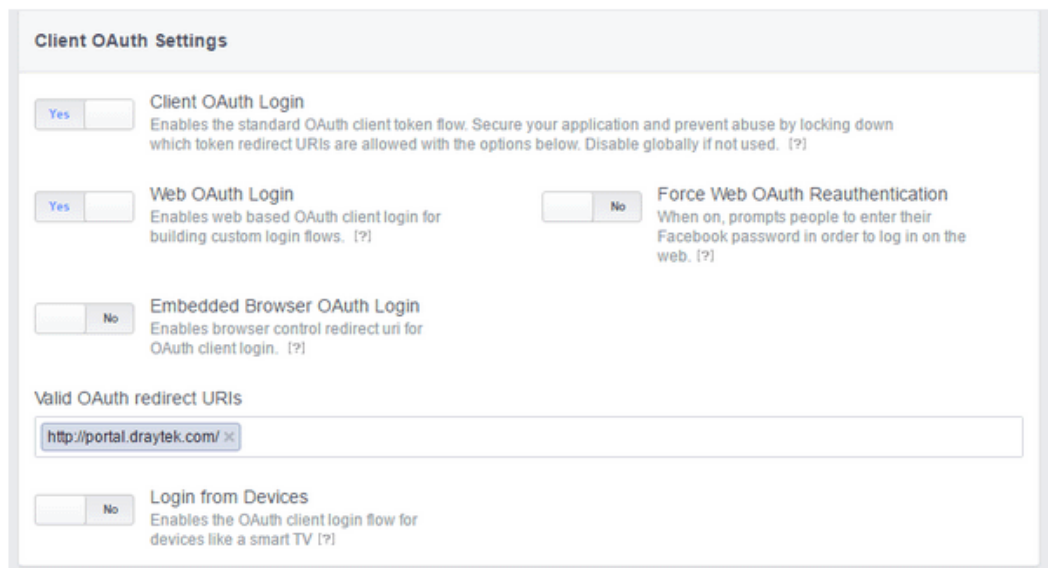
- Choose **Website** in Select Platform window.



- Enter the Site URL as <http://portal.draytek.com>. (Note: If you change http port in the vigor, please add http port in URLs. For example, we use 8080 as http port and we'll put <http://portal.draytek.com:8080>). Enter the Contact Email. And click Save Change.



13. Set up Client OAuth. Go to Settings >> Advanced >> Client OAuth Settings, enter "http://portal.draytek.com" in Valid OAuth redirect URIs, and save changes.



14. Go to My Apps >> Status & Review, and switch available status to YES to activate the APP.

Facebook Developers navigation bar: Developers | My Apps | Products | Docs | Tools & Support | News | Search in docs

Left sidebar (draytektest):

- Dashboard
- Settings
- Status & Review**
- App Details
- Roles
- Open Graph
- Alerts
- Localize
- Carvas Payments
- Audience Network

Main content area:

Status | Items in Review

draytektest •

Do you want to make this app and all its live features available to the general public? YES

Submit Items for Approval

Some Facebook integrations require approval before public usage. Before submitting your app for review, please consult our [Platform Policy and Review Guidelines](#).

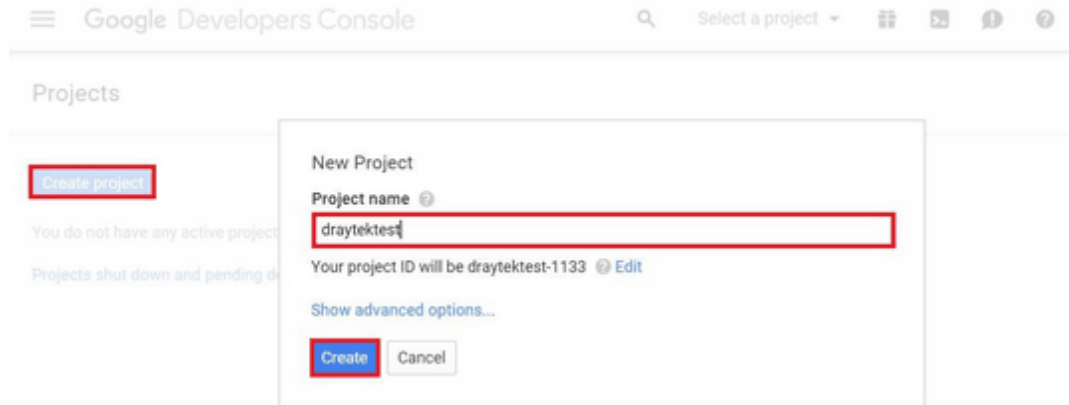
Approved Items (0)

LOGIN PERMISSIONS

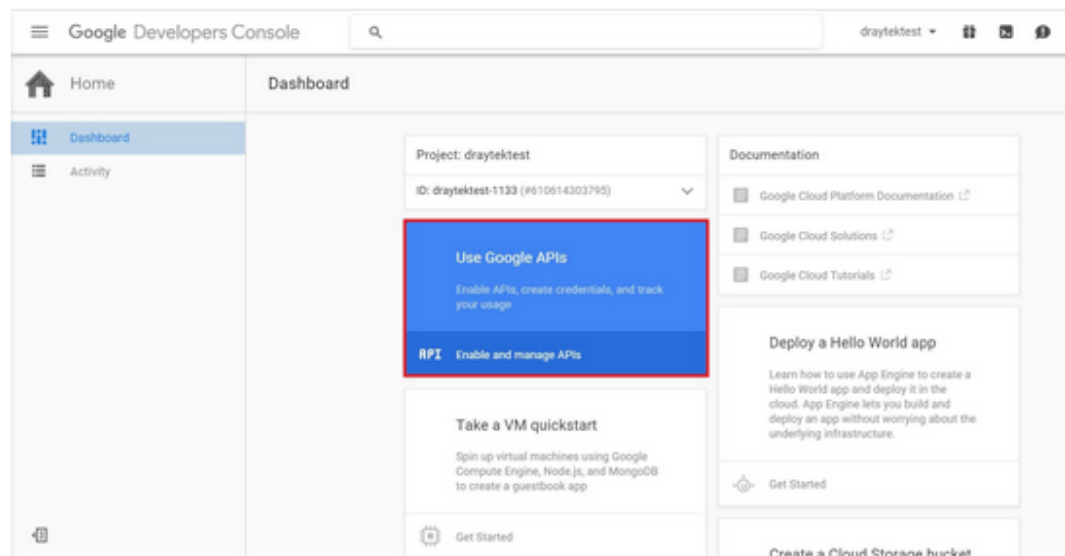
A-2 How to create Google APP for Web Portal Authentication?

The new web portal feature support social login as authentication method, and allows network administrator to authenticate LAN clients by their Google or Facebook account. This document introduces how to create Facebook APP, and generate the APP ID and APP secret that can be used in Web Portal setup.

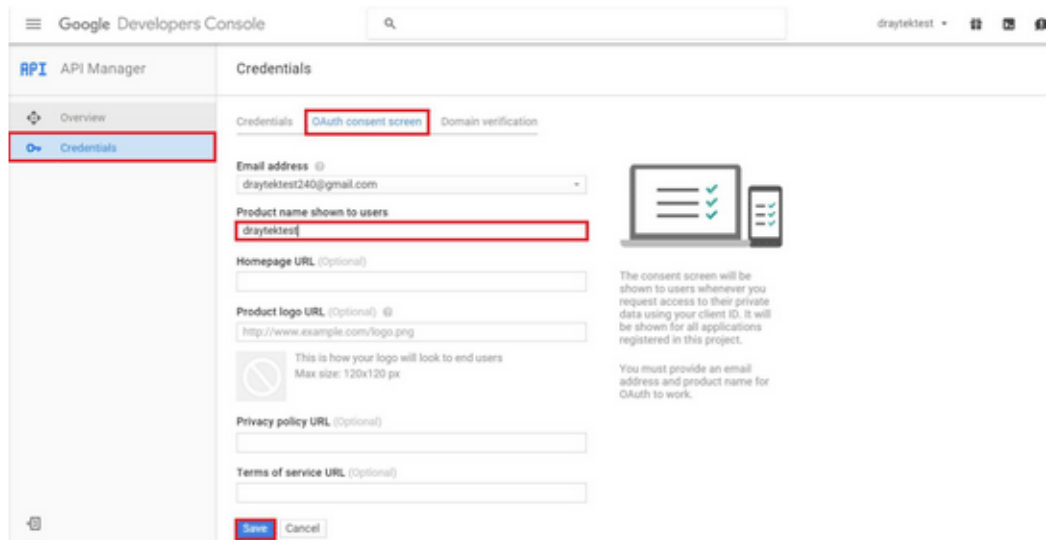
1. Create Developer project. Go to <https://code.google.com/apis/console>, login with a Google account then click Create project. Type project name then click Create.



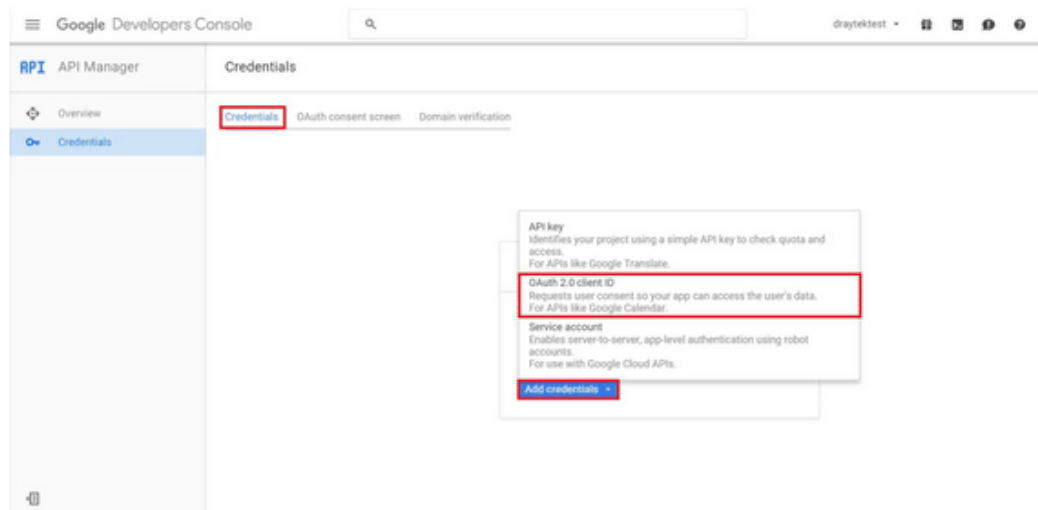
2. On Dashboard, choose Use Google APIs.



3. Edit Auth Consent screen. Go to Credentials > Auth consent screen. Enter your email, product name and other optional item then click on Save.



4. Create Client ID. Click Credentials and Click Add credentials > OAuth2.0 client ID.



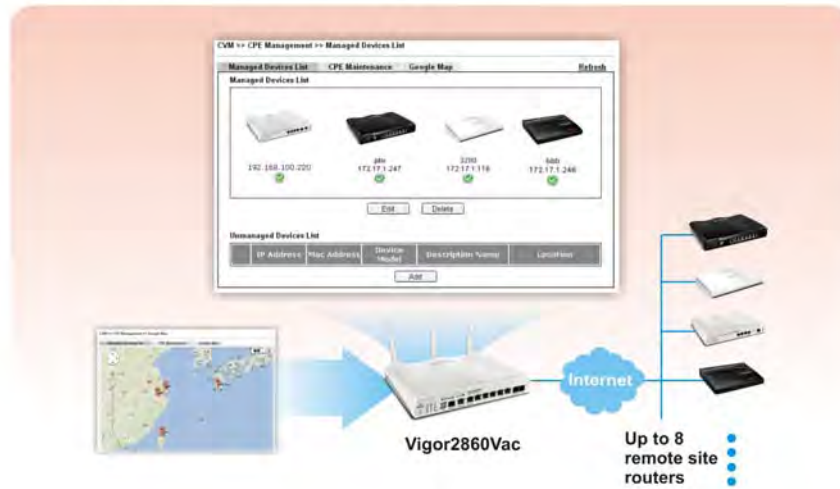
5. Choose **Web application** as Application Type, then enter **name**. Set **Authorized JavaScript origins** and **Authorized redirect URLs** as `http://portal.draytek.com`, and click **Create**. (*Note: If you change http port in the vigor, please add http port in URLs. For example, we use 8080 as http port and we'll put `http://portal.draytek.com:8080`*).
6. Get client ID and client secret. Such information will be used in Vigor Router's Web Portal Setup page.



VI-5 Central Management (VPN)

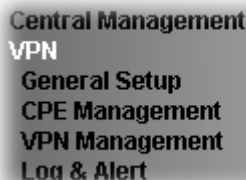
Vigor2862 can build virtual private network (VPN) between itself and any other TR-069 CPE by the function of central VPN management. In addition, it can be treated as a server (called CVM server) which can manage TR-069 CPE for periodical firmware upgrade, configuration backup and restoring configuration.

Central VPN Management



Web User Interface

Central VPN Management menu can manage the CPE connected through WAN only.



VI-5-1 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.

VI-5-1-1 General Settings

To enable the CVM feature, the first thing you have to do is enabling CVM port or CVM SSL Port.

Central Management >> VPN >> General Setup

General Settings	IPsec VPN Settings
<input checked="" type="checkbox"/> CVM SSL Port	<input type="text" value="8443"/>
<input checked="" type="checkbox"/> CVM Port	<input type="text" value="8000"/>
CVM WAN interface	<input type="text" value="WAN1"/> / <input type="text" value="---"/>
Username	<input type="text" value="acs"/>
Password	<input type="password" value="*****"/>
Polling Interval	<input type="text" value="600"/> Seconds

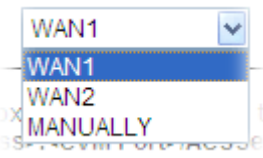
Note:

At least one port (CVM SSL Port or CVM Port) must be enabled for CVM to be operational. Use "CVM SSL port" for maximum security as all traffic will be encrypted.

OK

Available settings are explained as follows:

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.
CVM WAN interface	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 to specify WAN IP address.

	
Username	Type a username which will be used by any CPE trying to connect to Vigor router.
Password	Type the password for the user.
Polling Interval	Type the time value (unit is second). The range is from 60 ~ 86400.

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

VI-5-1-2 IPsec VPN Settings

Central VPN management is operated through IPsec VPN connection.

Central Management >> VPN >> General Setup

General Settings	IPsec VPN Settings
IPsec Mode:	Aggressive mode <input type="button" value="v"/>
Security Method:	ESP <input type="button" value="v"/>
Encryption Type:	AES <input type="button" value="v"/>
Local Subnet:	Manually <input type="button" value="v"/> <input type="text"/> / <input type="text"/>
<input type="button" value="OK"/>	

Available settings are explained as follows:

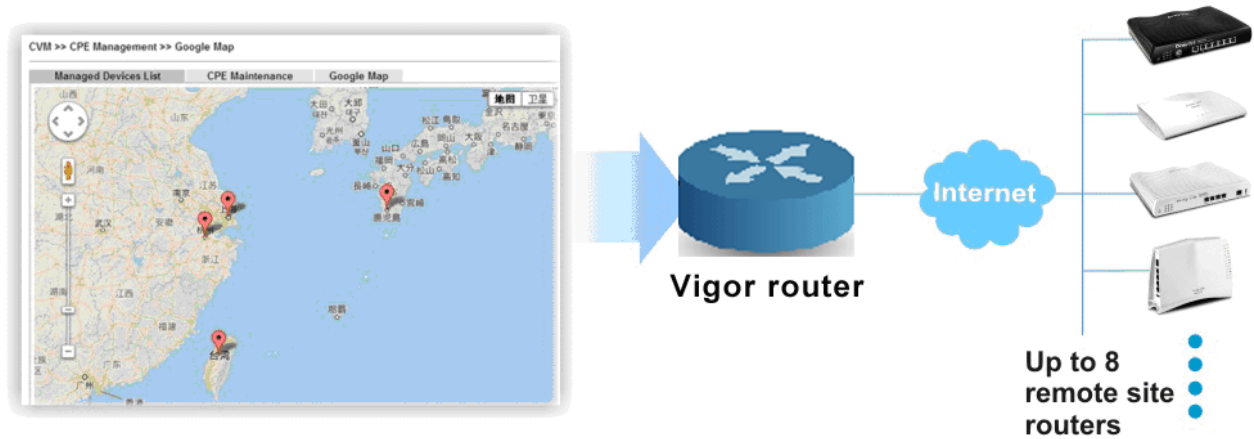
Item	Description
IPsec Mode	Choose Aggressive or Main as the IPsec Mode.
Security Method	Choose one of the following methods (AH or ESP) for the security of data transmission. For example, choose AH to specify the IPsec protocol for the Authentication Header protocol. The data will be authenticated but 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.

VI-5-2 CPE Management

All the CPEs managed by Vigor2862 series can be seen with icons from this page.

Before using such feature, make sure the CVM port has been enabled and configured properly.



VI-5-2-1 Managed Device List

This page allows you to manage the CPEs connected to Vigor2862 series.

Page without CPE connected


Central Management >> VPN >> CPE Management >> Managed Devices List

Managed Devices List	CPE Maintenance	Google Map	Refresh	
Managed Devices List				
Unmanaged Devices List				
IP Address	Mac Address	Device Model	Description Name	Location
<input type="button" value="Add"/>				


Page with CPE connected

Managed Devices List
CPE Maintenance
Google Map
Refresh

Managed Devices List



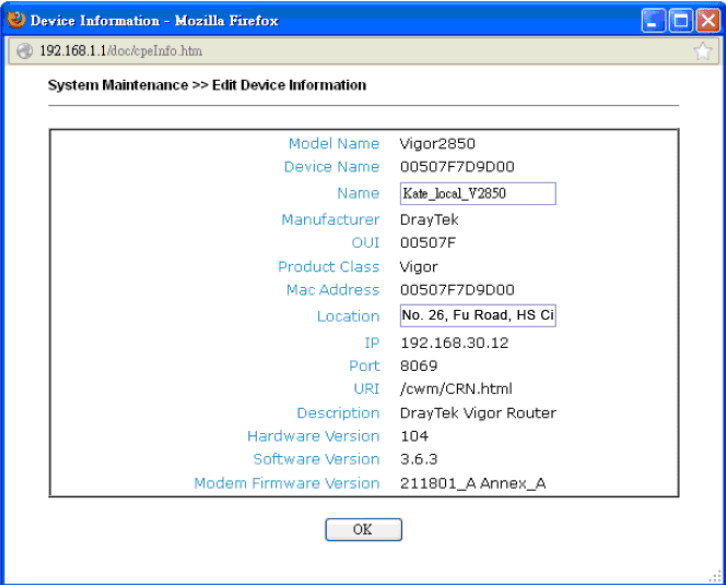
192.168.100.220

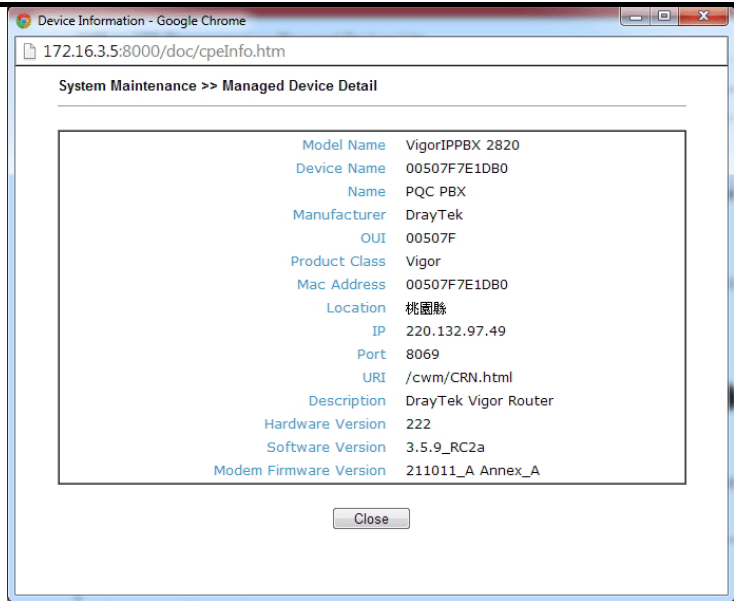


Unmanaged Devices List

IP Address	Mac Address	Device Model	Description Name	Location
<input type="button" value="Add"/>				

Available settings are explained as follows:

Item	Description
Managed Devices List	<p>This area displays device icons (up to 8) for the CPE managed by Vigor2862 series.</p> <p>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.</p> <div style="border: 1px solid blue; padding: 5px; margin: 10px 0;">  </div> <p>Delete - To disconnect the management of any CPE, click the CPE icon you want and click the Delete button.</p> <p>Double-clicking the CPE icon also can pop up the Managed Device Detail window. However, you cannot modify any data on the window.</p>



Unmanaged Devices List

Any device (CPE) which follows the standard of TR-069 can be configured and can be detected by Vigor2862 series automatically.

Only eight remote devices can be managed by Vigor2862 at one time. Therefore, other remote devices detected by Vigor2862 series might not be displayed in such field.

Add - Move the selected device from Unmanaged Devices List to Managed Devices List.

IP Address - Display the IP address of the remote device.

Mac Address - Display the MAC address of the remote device.

Device Model - Display the model name of the remote device.

Description Name - Define the name or type the additional description of CPE for identification in VPN management and CPE management.

Location - Type the location (address) of the CPE to be displayed by Google Map.

Refresh

Click it to refresh current web page.

VI-5-2-2 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.

Central Management >> VPN >> CPE Management >> CPE Maintenance

Managed Devices List
CPE Maintenance
Google Map
Refresh

USB Status: Disconnected
Disk Usage : ---
File Explorer

[Set to Factory Default](#)

Index	Enable	Profile Name	Device Name	Action	Schedule
1.	<input type="checkbox"/>				0,0 Now
2.	<input type="checkbox"/>				0,0 Now
3.	<input type="checkbox"/>				0,0 Now
4.	<input type="checkbox"/>				0,0 Now
5.	<input type="checkbox"/>				0,0 Now
6.	<input type="checkbox"/>				0,0 Now
7.	<input type="checkbox"/>				0,0 Now
8.	<input type="checkbox"/>				0,0 Now

<< 1.8 | 9.16 >>

Note:

1. USB storage must be connected before profiles can be enabled.
2. Click the "Now" button to execute the profile immediately.

Available settings are explained as follows:

Item	Description
Refresh	Click it to refresh current page.
USB Disk	USB Disk : - It means a USB disk connecting to Vigor2862. USB Disk : - It means no USB disk connecting to Vigor2862.
Disk Usage	Disk Usage : 1084MB / 2009MB - When a USB disk connects to Vigor2862, 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 Vigor2862, 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.
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 >> Maintenance Profile

Enable Only Run Once

Profile Name:

Device Name:

Router Name:

Router Model:

Action Type:

File Path:

Schedule Index: ,

Note:

1. Enable "Only Run Once" to automatically disable the profile after it has been run.
2. The Action setting in the schedule profile will be ignored.




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
Enable	Check it to enable such profile.
Only Run Once	Check it to activate such profile running for once.
Profile Name	Type the name of the maintenance profile.
Device Name	The drop down list will display all the CPE devices detected by Vigor2862 series. Choose the one which will be applied with such new created profile.
Router Name/ Router Model	It displays the name and model of Vigor router.
Action Type	There are three actions for you to choose for such profile.

	<ul style="list-style-type: none"> ● 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. <div style="border: 1px solid black; padding: 5px; margin: 10px 0;">  <p>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).</p> </div> <ul style="list-style-type: none"> ● Firmware Upgrade - It means such profile will be used for firmware upgrade.
File Path	When Config Restore is selected as Action Type , click Select to upload a configuration file from the connected USB disk. Later such file will be used for saving, restoring or firmware upgrade for CPE.
File Name	Specify a file name in this field to save the configuration file when Config Backup is selected as Action Type .
Schedule Index	Vigor2862 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.

VI-5-2-3 Google Map

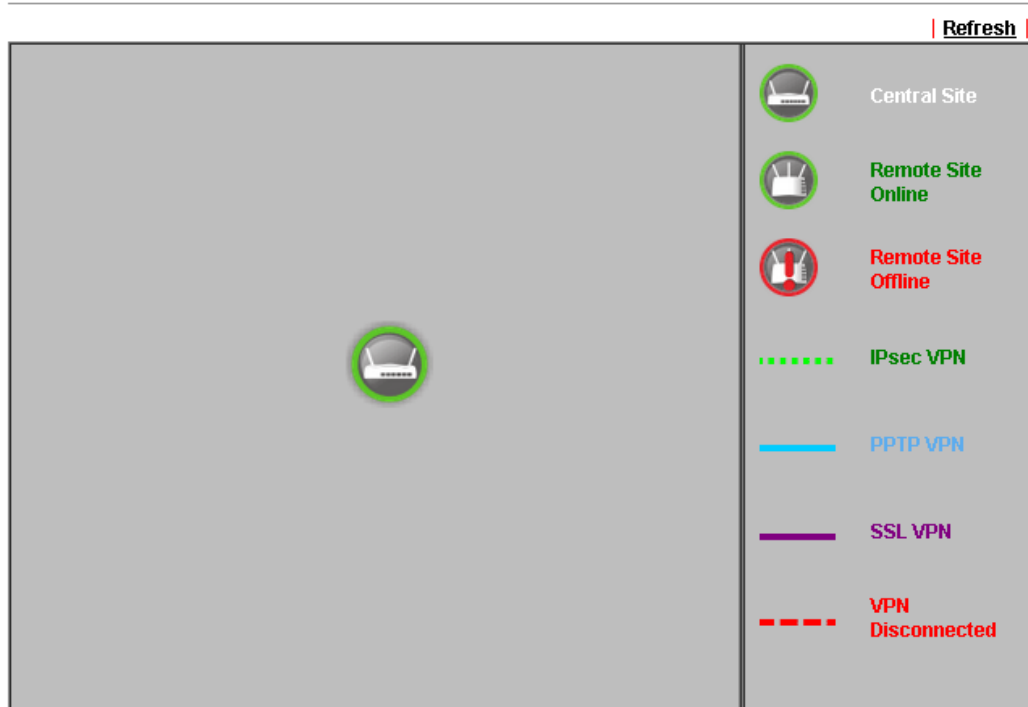
To display the location of the managed CPE with a bird's eye view, open **Central VPN Management>>CPE Management** and click the tab of **Google Map**.



VI-5-3 VPN Management

An easy and quick method is offered to configure VPN settings for building VPN connection automatically between Vigor2862 series (treated as VPN server) and other Vigor router (treated as CPE device, i.e., VPN client).

Central Management >> VPN >> 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.

CPE VPN Connection List

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	Up Time
-----	------	-----------	-----------------	---------	--------------	---------	--------------	---------

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 Vigor2862 and remote CPE.
Type	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 Vigor2862 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 Vigor2862 series, it will be displayed on such screen automatically. If not, refer to sections “How to manage the CPE (router) through Vigor2862?” for more detailed information.

VI-5-4 Log & Alert

This page offers brief information to identify the CPE connected to Vigor2862 series.

Central Management >> VPN >> Log & Alert

Log		Alert		
				Refresh Clear
				Display Mode <input type="text" value="Always record the new event"/>
Device Name	Description Name	time & date	Action Type	Message
001DAAB61BB8		2014-08-11 11:02:07	CPE Maintenance	CPE Online
001DAAB61BB8		2000-01-01 00:00:00	CPE Maintenance	Add CPE Successfully

Available settings are explained as follows:

Item	Description
Display Mode	Choose the mode you want to display the related information on the following table. <ul style="list-style-type: none"> ● 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 Vigor2862 series.
Action Type	Display the action that Vigor2862 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 Vigor2862 series.

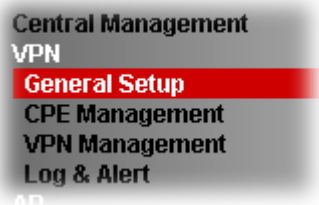
Application Notes

A-1 CVM Application - How to manage the CPE (router) through Vigor2862 series?

To manage CPEs through Vigor2862 series, you have to set URL on CPE first and set username and password for Vigor2862 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 Vigor2862 series

1. Access into the web user interface of Vigor2862 series.
2. Open Central Management >> VPN >> 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.

Central Management >> VPN >> General Setup

General Settings	IPsec VPN Settings
<input checked="" type="checkbox"/> CVM SSL Port	<input type="text" value="8443"/>
<input checked="" type="checkbox"/> CVM Port	<input type="text" value="8000"/>
CVM WAN interface	<input type="text" value="WAN1"/> / <input type="text" value="---"/>
Username	<input type="text" value="acs"/>
Password	<input type="password" value="*****"/>
Polling Interval	<input type="text" value="600"/> Seconds

Note:

At least one port (CVM SSL Port or CVM Port) must be enabled for CVM to be operational. Use "CVM SSL port" for maximum security as all traffic will be encrypted.

OK

4. 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 Vigor2862 series and type the same Username and Password defined on the page of Central VPN Management>>General Setup in Vigor2862 series. Then, click Enable for CPE Client and then click OK to save the settings.

System Maintenance >> TR-069 Setting

ACS and CPE Settings

ACS Server On	Internet
ACS Server	
URL	<code>http://172.17.1.182:9000</code>
Username	acs
Password	*****
CPE Client	
<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
URL	<code>http://172.17.1.208:8069/cwm/CRN.html</code>
Port	8069
Username	vigor
Password	*****

Periodic Inform Settings

<input type="radio"/> Disable	
<input checked="" type="radio"/> Enable	
Interval Time	60 second(s)

4. Open System Maintenance>>Management Setup.

5. Check **Allow management from the Internet** to set management access control and click **OK**.

System Maintenance >> Management

IPv4 Management Setup		IPv6 Management Setup													
Router Name <input type="text"/>		Management Port Setup													
Management Access Control <input checked="" type="checkbox"/> Allow management from the Internet <input type="checkbox"/> FTP Server <input checked="" type="checkbox"/> HTTP Server <input checked="" type="checkbox"/> HTTPS Server <input checked="" type="checkbox"/> Telnet Server <input type="checkbox"/> SSH Server <input checked="" type="checkbox"/> Disable PING from the Internet		<input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports Telnet Port <input type="text" value="23"/> (Default: 23) HTTP Port <input type="text" value="80"/> (Default: 80) HTTPS Port <input type="text" value="443"/> (Default: 443) FTP Port <input type="text" value="21"/> (Default: 21) SSH Port <input type="text" value="22"/> (Default: 22)													
Access List <table border="1"> <thead> <tr> <th>List</th> <th>IP</th> <th>Subnet Mask</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>2</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>3</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table>				List	IP	Subnet Mask	1	<input type="text"/>	<input type="text"/>	2	<input type="text"/>	<input type="text"/>	3	<input type="text"/>	<input type="text"/>
List	IP	Subnet Mask													
1	<input type="text"/>	<input type="text"/>													
2	<input type="text"/>	<input type="text"/>													
3	<input type="text"/>	<input type="text"/>													
<input type="button" value="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**.

WAN >> Internet Access

WAN 1		MPoA (RFC1483/2684)	
<input checked="" type="radio"/> Enable <input type="radio"/> Disable		WAN IP Network Settings <input type="button" value="WAN IP Alias"/>	
DSL Modem Settings Multi-PVC channel <input type="text" value="Channel 2"/> Encapsulation <input type="text" value="1483 Bridged IP LLC"/> VPI <input type="text" value="0"/> VCI <input type="text" value="88"/> Modulation <input type="text" value="Multimode"/>		<input type="radio"/> Obtain an IP address automatically Router Name <input type="text" value="Vigor"/> Domain Name <input type="text"/> <small>* : Required for some ISPs</small>	
WAN Connection Detection Mode <input type="text" value="ARP Detect"/> Ping IP <input type="text"/> TTL: <input type="text"/>		<input checked="" type="radio"/> Specify an IP address IP Address <input type="text" value="192.168.30.12"/> Subnet Mask <input type="text" value="255.255.0.0"/> Gateway IP Address <input type="text" value="172.16.3.4"/>	
RIP Protocol <input type="checkbox"/> Enable RIP		<input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: <input type="text" value="00"/> · <input type="text" value="50"/> · <input type="text" value="7F"/> : <input type="text" value="00"/> · <input type="text" value="00"/> · <input type="text" value="01"/>	
Bridge Mode <input type="checkbox"/> Enable Bridge Mode		DNS Server IP Address Primary IP Address <input type="text"/> Secondary IP Address <input type="text"/>	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>			



Info

Reboot the CPE device and re-log into Vigor2862 series. CPE which has registered to Vigor2862 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 Vigor2862 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.

Device Information - Mozilla Firefox
192.168.1.1@oc/cpeinfo.htm

System Maintenance >> Edit Device Information



Model Name: Vigor2850
Device Name: 00507E7D9D00
Name: Kate_local_V2850
Manufacturer: DrayTek
OUI: 00507F
Product Class: Vigor
Mac Address: 00507E7D9D00
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

4. The selected CPE will be moved and displayed on Managed Devices List which means it is controlled / managed by Vigor2862 series from now on.

Managed Devices List CPE Maintenance Google Map Refresh

Managed Devices List


Kate_local...
192.168.30.12


Edit Delete

Unmanaged Devices List

IP Address	Mac Address	Device Model	Description	Name	Location
------------	-------------	--------------	-------------	------	----------

Add

A-2 CVM Application - How to build the VPN between remote devices and Vigor2862 series?

When a remote device is managed by Vigor2862 series, it is easy to build VPN between these two devices.

1. Access into the web user interface of Vigor2862 series.
2. Open Central Management >> VPN >> CPE Management.


VPN Management



CPE VPN Connection List

PPTP IPsec Advanced

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	Up Time
-----	------	-----------	-----------------	---------	--------------	---------	--------------	---------

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.

CVM >> VPN Management

VPN Management



CPE VPN Connection List

PPTP IPsec Advanced

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	Up Time
1 (cvm_7D9D00)	PPTP/MPPE	192.168.30.12 via WAN2	192.168.50.1/24	805	3	1088	3	0:40:30

- 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.

VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles:

View: All Trunk

Index	Name	Active	Status	Index	Name	Active	Status
<u>1.</u>	cvm_7D9D00	<input checked="" type="checkbox"/>	online	<u>17.</u>	???	<input type="checkbox"/>	---



Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="cvm_7D9D00"/> <input checked="" type="checkbox"/> Enable this profile VPN Dial-Out Through <input type="text" value="WAN1 First"/> Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block <small>(for some IGMP,IP-Camera,DHCP Relay..etc.)</small>	Call Direction <input type="radio"/> Both <input type="radio"/> Dial-Out <input checked="" type="radio"/> Dial-in <input type="checkbox"/> Always on Idle Timeout <input type="text" value="0"/> second(s) <input type="checkbox"/> Enable PING to keep alive PING to the IP <input type="text"/>
--	---

3. Dial-In Settings

Allowed Dial-In Type <input checked="" type="checkbox"/> PPTP <input type="checkbox"/> IPsec Tunnel <input type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/>	Username <input type="text" value="7D9D00"/> Password(Max 11 char) <input type="password" value="●●●●●●"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Authentication Method
---	---

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 Vigor2862 series?

Download the newest firmware from your Draytek website to USB Storage Disk for the device (e.g., Vigor2850) managed by Vigor2862 series.

Vigor2850, as an example, is chosen for Vigor2862 to perform the CPE firmware upgrade remotely in this case.

1. Plug in USB storage disk onto Vigor2862 series via USB interface. Make sure the USB disk has been installed correctly, otherwise, the firmware upgrade will not be successful.
2. Access into web user interface of Vigor2862 series. Open Central VPN Management>>CPE Management and click the CPE Maintenance tab.

Central Management >> VPN >> CPE Management >> CPE Maintenance

Managed Devices List
CPE Maintenance
Google Map
Refresh

USB Disk : Disk Usage : USB Storage Disconnected

| [Set to Factory Default](#) |

Index	Enable	Profile Name	Device Name	Action	Schedule
1.	<input type="checkbox"/>				0 0 Now
2.	<input type="checkbox"/>				0 0 Now
3.	<input type="checkbox"/>				0 0 Now
4.	<input type="checkbox"/>				0 0 Now
5.	<input type="checkbox"/>				0 0 Now
6.	<input type="checkbox"/>				0 0 Now
7.	<input type="checkbox"/>				0 0 Now
8.	<input type="checkbox"/>				0 0 Now

<< [1-8](#) | [9-16](#) >>

Note:
 To enable the schedulings, an USB storage **MUST** be plugged onto router.
 This action is add to task queue, you can check the result later on page "Central Management >> VPN >> Alert/Log"

3. Click any index number link, e.g., Index 1.

Managed Devices List
CPE Maintenance

Maintenance Profile List

Index	Profile Name	Device
1.		
2.		
3.		

- The Maintenance profile dialog appears.

Central VPN Management >> CPE Management >> Maintenance Profile

Profile Name:

Enable
 Only Run Once

Device Name:

Router Name:
Router Model:

Action Type:

- Config Backup
- Config Restore
- Firmware Upgrade

File Name:

Index in **Schedule**:

Note:
1. Action and Idle Timeout settings will be ignored.
2. If you enable 'Only Run Once', the profile will be automatically disabled after running.

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.

- Now, a new maintenance profile has been created.

Central Management >> VPN >> CPE Management >> CPE Maintenance

Managed Devices List
CPE Maintenance
Google Map
Refresh

USB Disk : Disk Usage : USB Disk Connected

Index	Enable	Profile Name	Device Name	Action	Schedule	Set to Factory Default
1.	<input checked="" type="checkbox"/>	V2850	00507F7D900	Config Backup	0 0	Now
2.	<input type="checkbox"/>				0 0	Now
3.	<input type="checkbox"/>				0 0	Now
4.	<input type="checkbox"/>				0 0	Now
5.	<input type="checkbox"/>				0 0	Now
6.	<input type="checkbox"/>				0 0	Now
7.	<input type="checkbox"/>				0 0	Now
8.	<input type="checkbox"/>				0 0	Now

<< 1-8 | **9-16** >>



Note:
To enable the schedulings, an USB storage **MUST** be plugged onto router.
This action is add to task queue, you can check the result later on page "Central Management >> VPN >> Alert/Log"

- Click **Now** to perform the firmware upgrade immediately for Vigor2850.
- 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**.

Managed Devices List | CPE Maintenance | Google Map | Refresh

Managed Devices List


Kate_local...
192.168.30.12


Edit Delete

Unmanaged Devices List

IP Address	Mac Address	Device Model	Description	Name	Location
------------	-------------	--------------	-------------	------	----------

Add

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**.

VI-6 Central Management (AP)

Vigor2862 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

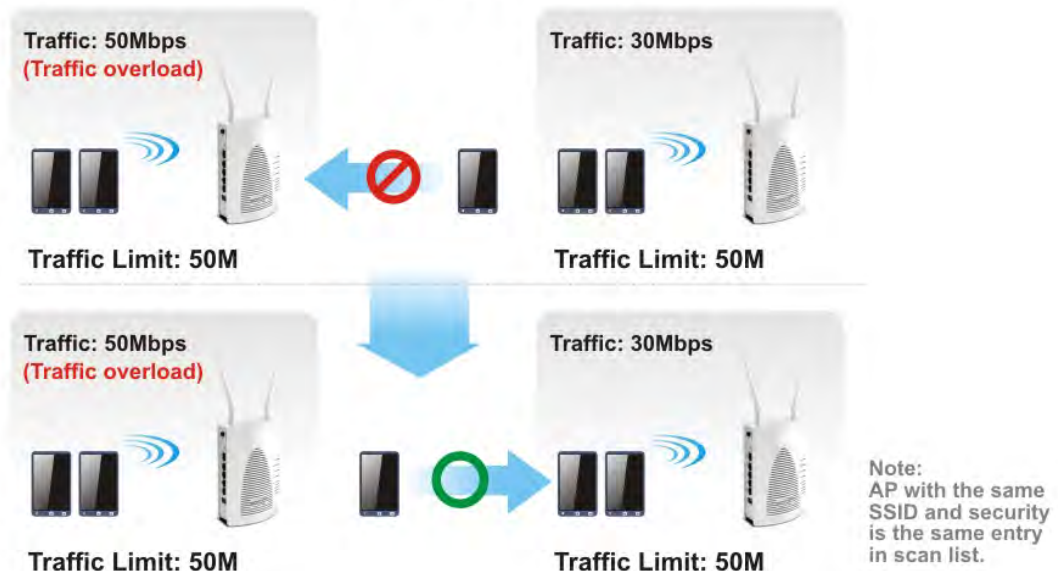
AP Maintenance

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.

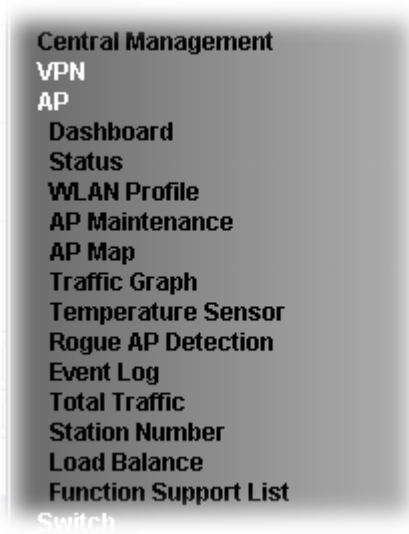
Load Balance for AP

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)



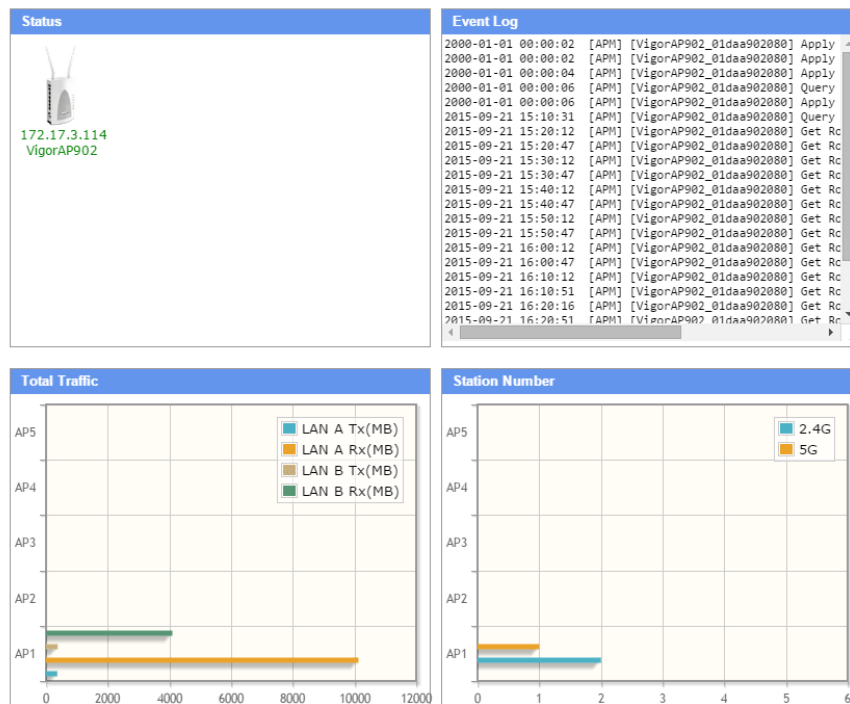
Web User Interface



VI-6-1 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.

Central AP Management >> Dashboard



AP1-- IP:172.17.3.114 Device Name:VigorAP902
 Note: Only browser supporting HTML5 can display dashboard correctly.

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.

VI-6-2 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.

Central Management >> AP >> Status

Index	Device Name	IP Address	SSID	Ch.	STA List	AP List	Uptime	Ver.	Password
1	VigorAP902	192.168.1.10	DrayTek-LAN-A DrayTek5G-LAN-A	11 36	0/64 0/64	0 0	0d 00:01	1.1.5.1	Password

Note:

: Online : Offline : Hidden SSID

Maximum support 20 APs.

When AP Devices connect via an intermediary switch, please ensure that **UDP:4944** port and the **HTTP** port of AP Devices are not blocked so that the AP status can be retrieved.

Available settings are explained as follows:

Item	Description
Index	Click the index number link for viewing the settings summary of the access point.
Device Name	The name of the AP managed by Vigor router will be displayed here.
IP Address	Display the true IP address of the access point.
SSID	Display the SSID configured for the access point(s) connected to Vigor2862.
Ch.	Display the channel used by the access point.
STA List	Display the number of wireless clients (stations) connecting to the access point. In which, 0/64 means that up to 64 clients are allowed to connect to the access point. But, now no one connects to the access point. The number displayed on the left side means 2.4GHz; and the number displayed on the right side means 5GHz.
AP List	Display the number of the AP around the device.
Uptime	Display the duration of the AP powered up.
Version	Display the firmware version used by the access point.
Password	Vigor2862 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.

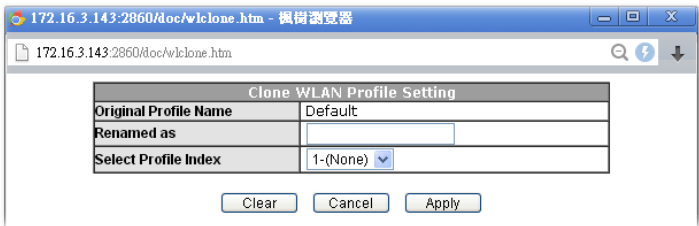
VI-6-3 WLAN Profile

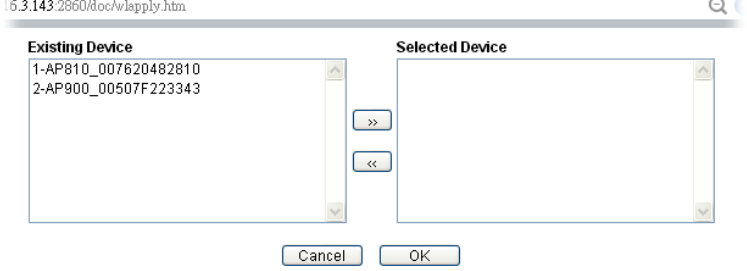
WLAN profile is used to apply to a selected access point. It is very convenient for the administrator to configure the setting for access point without opening the web user interface of the access point.

Central Management >> AP >> WLAN Profile

Profile	Name	Main SSID	Security	Multi-SSID	WLAN ACL	Rate Ctrl	Clone	To AP	To Local
1	Default	DrayTek-LAN-A	WPA+WPA2/PSK	Enable	None	None			
2	---	---	---	---	---	---	---	---	---
3	---	---	---	---	---	---	---	---	---
4	---	---	---	---	---	---	---	---	---
5	---	---	---	---	---	---	---	---	---

Click the number link of the selected profile to modify the content of the profile. Available settings are explained as follows:

Item	Description
Profile	There are five WLAN profiles offered to be configured. Simply click the index number link to open the modification page.
Name	Display the name of the profile. The default profile cannot be renamed.
Main SSID	Display the SSID configured by such wireless profile.
Security	Display the security mode selected by such wireless profile.
Multi-SSID	Enable means multiple SSIDs (more than one) are active. Disable means only SSID1 is active.
WLAN ACL	Display the name of the access control list.
Rate Ctrl	Display the upload and/or download transmission rate.
Clone	<p>It can copy settings from an existing WLAN profile to another WLAN profile.</p> <p>First, you have to check the box of the existing profile as the original profile. Second, click Clone. The following dialog will appear.</p>  <p>Third, choose the profile index to accept the settings from the original profile. Forth, type a new name in the field of Renamed as. Last, click Apply to save the settings on this dialog.</p> <p>The new profile has been created with the settings coming from the original profile.</p>
To AP	Click it to apply the selected wireless profile to the specified Access Point.

	 <p>Simply choose the device you want from Existing Device field. Click >> to move the device to Selected Device field. Then, click OK.</p> <p>The selected WLAN profile will be applied to the selected access point immediately. Later the access point will reboot.</p>
<p>To Local</p>	<p>WLAN Profile configured in this page is specified for VigorAP connected to Vigor router.</p> <p>If required, these settings also can be applied to Vigor router. Select and check one of wireless profiles and click this button to apply the settings onto the WI-Fi wireless settings configured for such Vigor router.</p>

How to edit the wireless LAN profile?

1. Select the WLAN profile (index number 1 to 5) you want to edit.
2. Click the index number link to display the following page.

Central Management >> AP >> WLAN Profile

WLAN Profile Edit

Device Settings	
Profile Name	Default <input type="checkbox"/> Auto Provision
Administrator	admin
Password	*****
2nd Subnet	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

2.4G WLAN General Settings	
Wireless LAN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Limit Client	<input type="checkbox"/> Enable 64 (3 ~ 128) (Default: 64)
Operation Mode	AP
2.4G Mode	Mixed(11b+11g+11n)
2.4G Channel	2462MHz (Channel 11)
Airtime Fairness	<input type="checkbox"/> Enable Airtime Fairness: Triggering Client Number 2 (2 ~ 128) (Default: 2)
Band Steering	<input type="checkbox"/> Enable Band Steering: Check Time for WLAN Client 5G Cap. 15 sec(s) (1 ~ 60) (Default: 15)
Roaming	<input type="checkbox"/> Minimum Basic Rate 1 Mbps
	<input checked="" type="radio"/> Disable RSSI Requirement
	<input type="radio"/> Strictly Minimum RSSI - 73 dbm (42 %) (Default: -73)
	<input type="radio"/> Minimum RSSI - 66 dbm (60 %) (Default: -66) with Adjacent AP RSSI over 5 dB (Default: 5)
	<input type="checkbox"/> Enable Fast Roaming(WPA2/802.1x): PMK Cache Period 10 minutes (10 ~ 600, default: 10)
WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Tx Power	100%

5G WLAN General Settings	
Wireless LAN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Limit Client	<input type="checkbox"/> Enable 64 (3 ~ 128) (Default: 64)
Operation Mode	AP
5G Mode	Mixed (11a+11n)
5G Channel	5180MHz (Channel36)
Airtime Fairness	<input type="checkbox"/> Enable Airtime Fairness: Triggering Client Number 2 (2 ~ 128) (Default: 2)
Roaming	<input type="checkbox"/> Minimum Basic Rate 6 Mbps
	<input checked="" type="radio"/> Disable RSSI Requirement
	<input type="radio"/> Strictly Minimum RSSI - 73 dbm (42 %) (Default: -73)
	<input type="radio"/> Minimum RSSI - 66 dbm (60 %) (Default: -66) with Adjacent AP RSSI over 5 dB (Default: 5)
	<input type="checkbox"/> Enable Fast Roaming(WPA2/802.1x): PMK Cache Period 10 minutes (10 ~ 600, default: 10)

Cancel Next



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.

Central Management >> AP >> WLAN Profile

SSID1	SSID2	SSID3	SSID4
2.4G SSID			
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
SSID	DrayTek-LAN-A	LAN-A	<input type="checkbox"/> Hide SSID
VLAN	0 (0:untag)		
Isolate	<input type="checkbox"/> From Member		
Security Settings			
Encryption	WPA+WPA2/PSK		
	Set up RADIUS Server if 802.1X is enabled.		
	WPA		
	WPA Algorithms	<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES	
	Pass Phrase	*****	
	Key Renewal Interval	3600	Seconds
	WEP		
	Setup WEP Key if WEP is enabled.		
	802.1X WEP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Access Control			
Mode	None		
List			
	Client's MAC Address : [] : [] : [] : [] : [] : []		
	<input type="button" value="Add"/>	<input type="button" value="Delete"/>	<input type="button" value="Edit"/> <input type="button" value="Cancel"/>
Bandwidth Limit			
Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Auto Adjustment	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Upload	0 Kbps	Download	0 Kbps
<input type="button" value="Back"/> <input type="button" value="Cancel"/> <input type="button" value="Next"/>			
Backup ACL Cfg : <input type="button" value="Backup"/>		Upload From File: <input type="button" value="選擇檔案"/> 未選擇檔案 <input type="button" value="Restore"/>	

- After finished the above web page configuration, click **Next** to open the following page for 5G wireless security settings.

Central AP Management >> WLAN Profile

5G SSID1	5G SSID2	5G SSID3	5G SSID4
5G SSID			
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
SSID	DrayTek-5G	LAN-A	<input type="checkbox"/> Hide SSID
VLAN	0 (0:untag)		
Isolate	<input type="checkbox"/> From Member		
Security Settings			
Encryption	Disable		
	Set up RADIUS Server if 802.1X is enabled.		
	WPA WPA Algorithms <input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES Pass Phrase <input type="text"/> Key Renewal Interval <input type="text" value="3600"/> Seconds		
	WEP Setup WEP Key if WEP is enabled. 802.1X WEP <input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Access Control			
Mode	None		
List			
	Client's MAC Address : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> <input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/>		
Bandwidth Limit			
Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		Auto Adjustment <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Upload	<input type="text" value="0"/> Kbps	Download	<input type="text" value="0"/> Kbps

Note : 5G SSID Configuration only work with VigorAP800 v1.1.1 and newer APM Client.

Backup ACL Cfg : <input type="button" value="Backup"/>	Upload From File: <input type="button" value="Select"/>	<input type="button" value="Restore"/>
--	---	--

- 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.

Central Management >> AP >> WLAN Profile

Set to Factory Default										
Profile	Name	Main SSID	Security	Multi-SSID	WLAN ACL	Rate Ctrl	Clone	To AP	To Local	
1	Default	DrayTek-LAN-A	WPA+WPA2/PSK	Enable	None	None				
2	123	DrayTek	Disable	Disable	None	None				
3	---	---	---	---	---	---	---	---	---	---
4	---	---	---	---	---	---	---	---	---	---
5	---	---	---	---	---	---	---	---	---	---

VI-6-4 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.



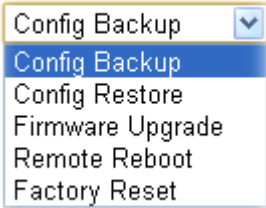
Info

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 Vigor2862.

Central Management >> AP >> AP Maintenance

AP Maintenance

Available settings are explained as follows:

Item	Description
Action	<p>There are four actions provided by Vigor router to manage the access points.</p>  <p>Vigor router can backup the configuration of the selected AP, restore the configuration for the selected AP, perform the firmware upgrade of the selected AP, reboot the selected AP remotely and perform the factory reset for the selected AP.</p>
File/Path	Specify the file and the path which will be used to perform Config Restore or Firmware Upgrade .
Select Device	Display all the available access points managed by Vigor

	router. Simply click << or >> to move the device(s) between Select Device and Selected Device areas.
Selected Device	Display the access points that will be applied by such function after clicking OK.

After finishing all the settings here, please click **OK** to perform the action.

VI-6-5 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 Management >> AP >> AP Map

Refresh Set to Factory Default							
Profile	Location	Online APs	Total APs	Clients	Dimension(m)	View	Delete
<u>1</u>	---	---	---	---	---	---	---
<u>2</u>	---	---	---	---	---	---	---
<u>3</u>	---	---	---	---	---	---	---
<u>4</u>	---	---	---	---	---	---	---
<u>5</u>	---	---	---	---	---	---	---

Available settings are explained as follows:

Item	Description
Set to Factory Default	Click the link to clear current page configuration.
Profile	Click the link to to view or edit the AP Map.
Location	Display a brief description (e.g., ground, roof) of the AP Map.
Online APs	Display the number of VigorAP configured and powered up.
Total APs	Display the total number of VigorAP configured.
Clients	Display the number of clients accessing Internet through the VigorAP.
Dimension(m)	Display the width and length of the AP map.
View	Click it to review the layout for the selected AP map.

Creating /Editing the AP Map Profile

1. Select a number index and click **Edit** to open the following web page.

Central Management >> AP >> AP Map

AP Map Profile Edit

Geographic Settings	
Location(Profile Name)	Marketing_floor
Upload Map	<input type="button" value="選擇檔案"/> Floor_MAP.png

Note:

The size of the map should be 200KB or smaller.(Only JPG,PNG,and GIF are supported)

Available settings are explained as follows:

Item	Description
Location (Profile Name)	Type a name (e.g., 3F) for the AP map profile.
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**. In the web page of **Dimension**, set dimension for the map.


Central Management >> AP >> AP Map


AP Map Profile Edit

Dimension **Planning**

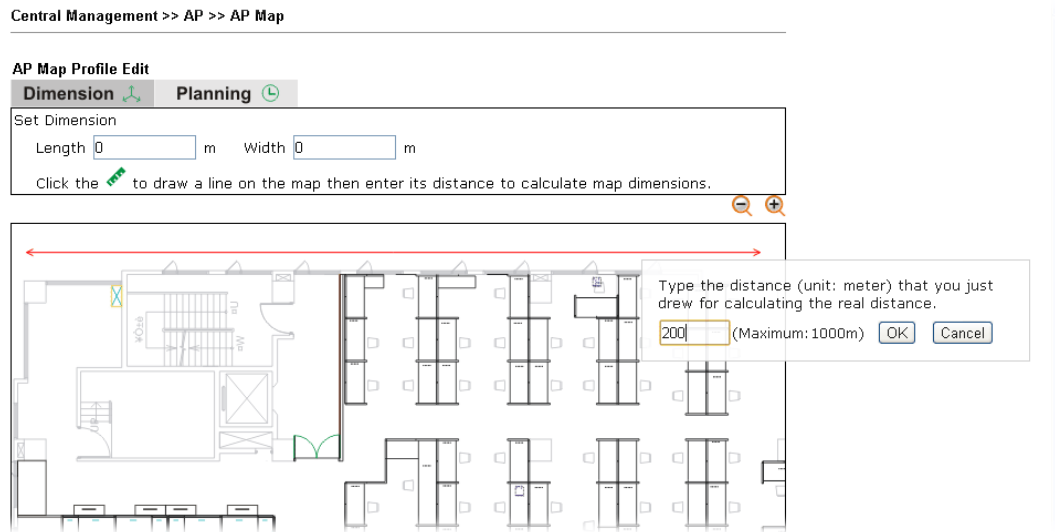
Set Dimension

Length m Width m

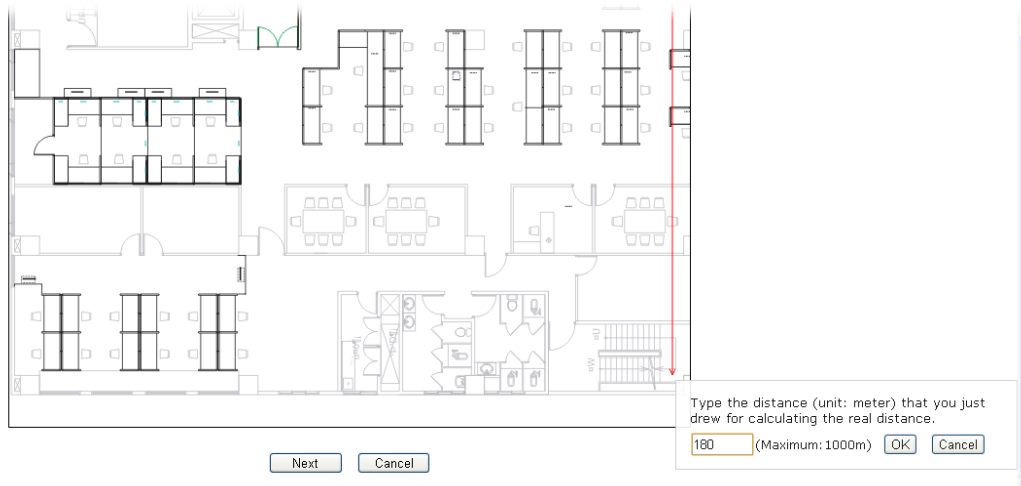
Click the  to draw a line on the map then enter its distance to calculate map dimensions.



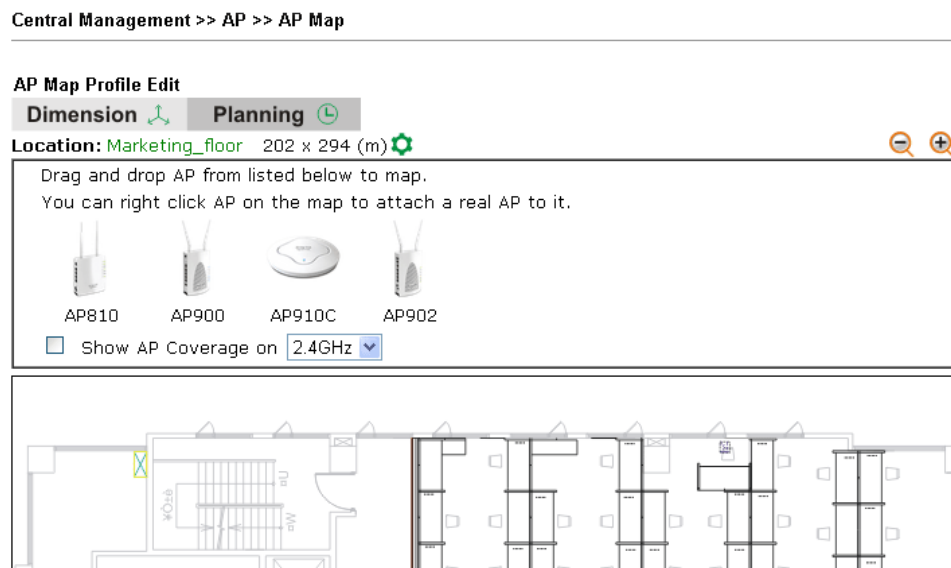
- Follow the instruction listed on the web page to draw a red line for length / width. Then, type the value on the pop up dialog to determine the real distance.



The values for length and width will be displayed on the web page.

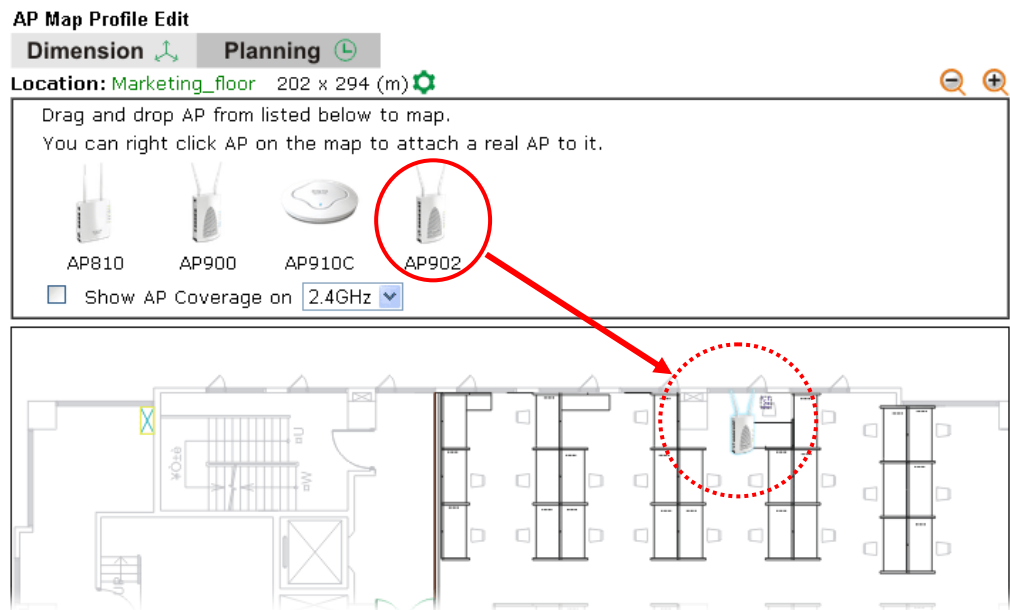


- Click Next to open the web page of Planning. Available APs detected by Vigor router will be displayed on the upper end.



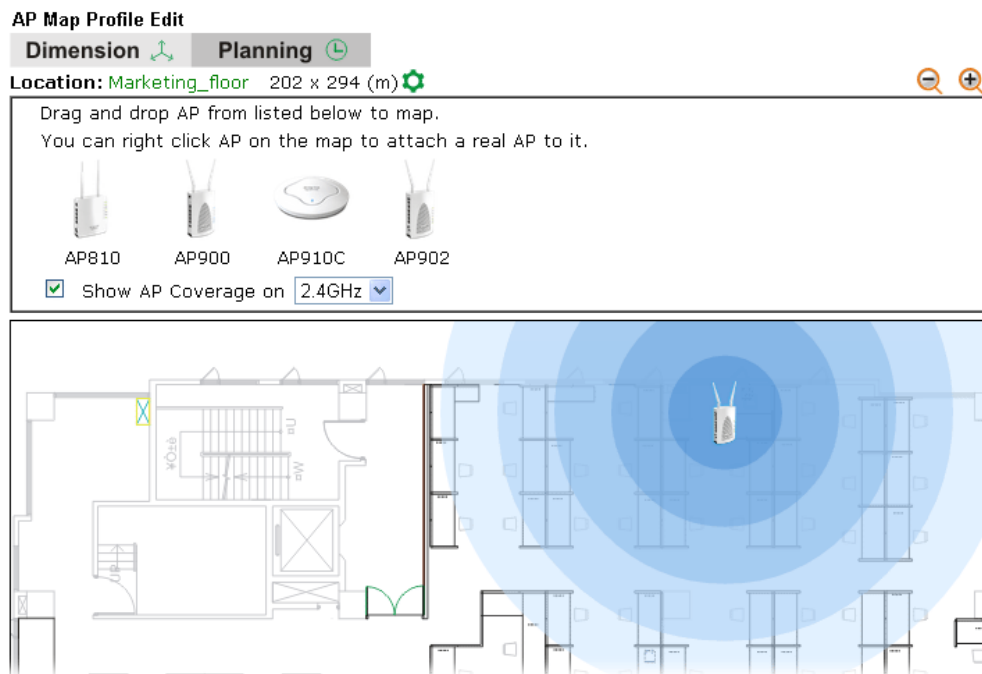
5. Select the AP you need; drag and drop an AP icon from upper end to the map on the bottom.

Central Management >> AP >> AP Map





6. Check the box of Show AP Coverage and choose 2.4GHz or 5GHz of wireless signal for the AP located on the floor plan.

Central Management >> AP >> AP Map



- Adjust the AP on the map to find out which place can have the best wireless coverage. At last, click Save.

Central Management >> AP >> AP Map

Refresh Set to Factory Default							
Profile	Location	Online APs	Total APs	Clients	Dimension(m)	View	Delete
1	Marketing_floor	0	1	0	202X294		
2	---	---	---	---	---	---	---
3	---	---	---	---	---	---	---
4	---	---	---	---	---	---	---
5	---	---	---	---	---	---	---

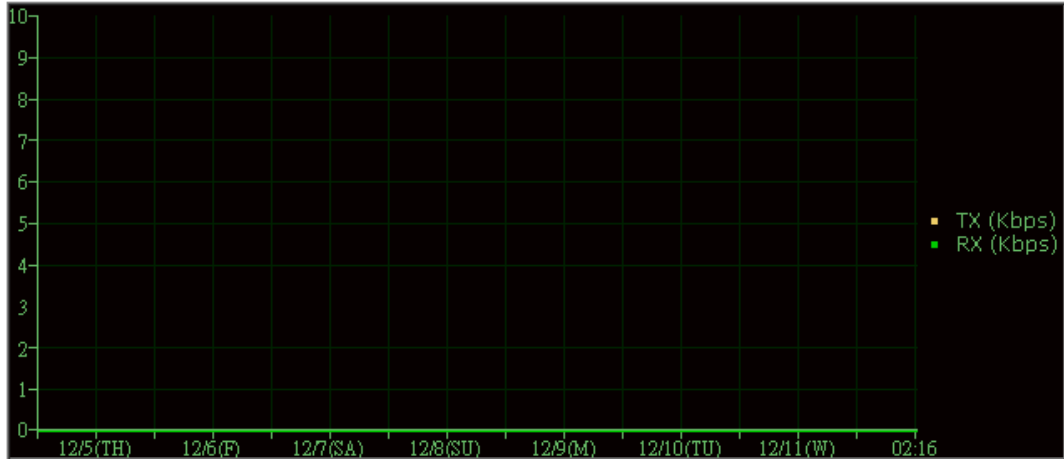
VI-6-6 Traffic Graph

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.

Central AP Management >> Traffic Graph

Enable

Show Chart: Refresh Min(s): | **Refresh** |



Note : Enabling/Disabling AP Traffic Graph will also Enable/Disable the External Devices Function.

The horizontal axis represents time; the vertical axis represents the transmission rate (in kbps).



Info

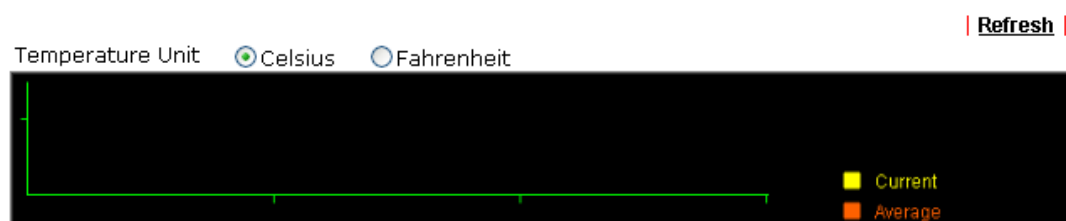
Enabling/Disabling such function will also enable/disable the External Devices function.

VI-6-7 Temperature Sensor

Many VigorAP and Vigor router can be installed with temperature sensor. If VigorAP (e.g., VigorAP 910C) is managed under Vigor router (e.g, Vigor2862), then Vigor router can obtain the temperature change graph of the USB temperature sensor installed onto VigorAP.

This page displays data including current temperature, maximum temperature, minimum temperature and average temperature.

Central Management >> AP >> Temperature Sensor



Note:

Only browser supporting **HTML5** can display temperature sensor correctly.

VI-6-8 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 Management >> AP >> Rogue AP Detection

Rogue AP Detection

Enable: Neighbor AP Detection Local WLAN Detection

All APs Total: 8 Refresh Min(s): 1 Page: 1 | Refresh |

idx	Ch	SSID	Mode	BSSID	Security	Signal (%)	Beacon Period	Last Detected
1	161	staffs_4F	AP	00:1d:aa:9d:68:ae	Mixed	11	100	Jan 02,03:19:29
2	161	staffs	AP	02:1d:aa:9d:68:ae	Mixed	19	100	Jan 02,03:19:29
3	161	guests	AP	06:1d:aa:9d:68:ae	Mixed	15	100	Jan 02,03:19:29
4	36	staffs_5F5G	AP	00:1d:aa:fe:fa:4a	Mixed	87	100	Jan 02,03:19:29
5	36	staffs	AP	02:1d:aa:fe:fa:4a	Mixed	87	100	Jan 02,03:19:29
6	36	DrayTek_5G	AP	00:1d:aa:c6:4c:42	Mixed	100	100	Jan 02,03:19:29
7	36	Hotspot1_5G	AP	00:1d:aa:cb:a3:12	NONE	70	100	Jan 02,03:19:29
8	36	MK-2925-mamie	AP	00:1d:aa:d4:9e:d2	Mixed	36	100	Jan 02,03:19:29

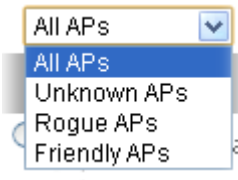
Note:

:Friendly APs :Rogue APs :Unknown APs

Vigor2862 does not apply security policies to Rogue AP List.

Available settings are explained as follows:

Item	Description
Enable	<p>Neighbor AP Detection - The access point(s) registered to Vigor2862 will be used to detect other access points and send the scanned results to Vigor2862. Later, the scanned result will be displayed on this page.</p> <p>Local WLAN Detection - The router will detect all the access</p>

	points through wireless LAN connection.
	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.

1. Click the radio button on one of the access points. In this case, DrayTek-LAN-A is selected.

Central AP Management >> Rogue AP Detection

Rogue AP Detection

Enable: Neighbor AP Detection Local WLAN Detection

All APs Refresh Min(s) : 1

	Ch	SSID	Mode	BSSID	Security	Signal (%)	Beacon Period	Last Detected
<input type="radio"/>	11	James_AP800	AP	00:50:7f:cc:08:e8	Mixed	68	100	Jan 01,00:50:26
<input type="radio"/>	11	DrayTek-LAN-B	AP	02:1d:aa:74:20:44	Mixed	100	100	Jan 01,00:50:26
<input checked="" type="radio"/>	11	DrayTek-LAN-A	AP	00:1d:aa:76:20:44	Mixed	99	100	Jan 01,00:50:26
<input type="radio"/>	11	James_900	AP	00:1d:aa:9c:f0:20	WPA	89	100	Jan 01,00:50:26

2. Later, some options will appear on the bottom of the page.




6 DrayTek AP 00:1d:aa:9c:f7:38 Mixed 78 100 Jan 01,00:50:26

AP's MAC Address : 00 : 1d : aa : a8 : b6 : b0 AP's SSID

Add to Friendly APs: Rogue APs:

Delete from Rogue APs: Friendly APs:

Note:

 Green :Friendly APs  Red :Rogue APs  Black :Unknown APs

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	<p>Friendly APs - If the selected AP shall be treated as Friendly AP, simply click Add to change its classification from unknown to Friendly.</p> <p>Rogue APs - If the selected AP shall be treated as rogue AP, simply click Add to change its classification from unknown to Rogue.</p>
Delete From	<p>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.</p> <p>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.</p>

3. Click OK to save the settings.










The following figure shows the APs classified and displayed in different colors.

Central Management >> AP >> Rogue AP Detection




Rogue AP Detection

Enable: Neighbor AP Detection Local WLAN Detection

All APs Total: 9 Refresh Min(s) : 1 Page: 1 | Refresh |

idx	Ch	SSID	Mode	BSSID	Security	Signal (%)	Beacon Period	Last Detected
1		48 Draytek_5G_Ian	AP	00:1d:aa:00:00:02	NONE	36	100	Jan 02,03:39:28
2		161 staffs_4F	AP	00:1d:aa:9d:68:ae	Mixed	11	100	Jan 02,03:19:29
3		161 staffs	AP	02:1d:aa:9d:68:ae	Mixed	19	100	Jan 02,03:19:29
4		161 guests	AP	06:1d:aa:9d:68:ae	Mixed	15	100	Jan 02,03:39:28
5		36 staffs_5F5G	AP	00:1d:aa:fe:fa:4a	Mixed	87	100	Jan 02,03:19:29
6		36 staffs	AP	02:1d:aa:fe:fa:4a	Mixed	87	100	Jan 02,03:39:28
7		36 DrayTek_5G	AP	00:1d:aa:c6:4c:42	Mixed	100	100	Jan 02,03:39:28
8		36 Hotspot1_5G	AP	00:1d:aa:cb:a3:12	NONE	70	100	Jan 02,03:39:28
9		36 MK-2925-mamie	AP	00:1d:aa:d4:9e:d2	Mixed	36	100	Jan 02,03:39:28

Note:

 : Friendly APs  : Rogue APs  : Unknown APs

VI-6-9 Event Log

Time and event log for all of the APs managed by Vigor router will be shown on this page. It is useful for troubleshooting if required.

Central AP Management >> Event Log

All Event Log

| Clear | Refresh |

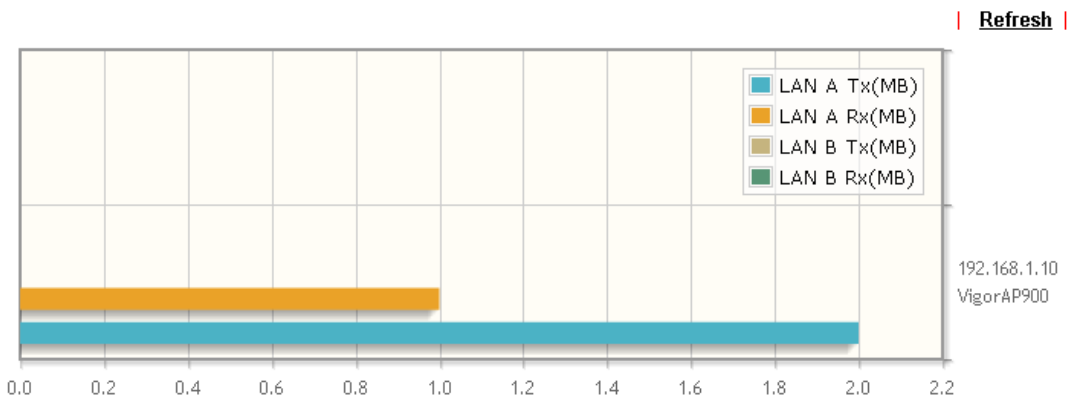
Time	APM Event Log	
2000-01-01 00:00:24	[APM] [VigorAP900_01daa9e2b38]	Apply Rogue AP Detection settings
2000-01-01 00:00:24	[APM] [VigorAP900_01daa9e2b38]	Apply Load Balance settings
2000-01-01 00:00:26	[APM] [VigorAP900_01daa9e2b38]	Apply Rogue AP Detection settings S
2000-01-01 00:00:29	[APM] [VigorAP900_01daa9e2b38]	Query AP status
2000-01-01 00:00:29	[APM] [VigorAP900_01daa9e2b38]	Apply Load Balance settings success
2000-01-01 00:00:35	[APM] [VigorAP900_01daa9e2b38]	Query AP status

Note 1: Only browser supporting **HTML5** can display Event Log correctly.

Note 2: The APs Log can be refreshed after at least 30 seconds.

VI-6-10 Total Traffic

Such page will display the total traffic of data receiving and data transmitting for VigorAPs managed by Vigor router.



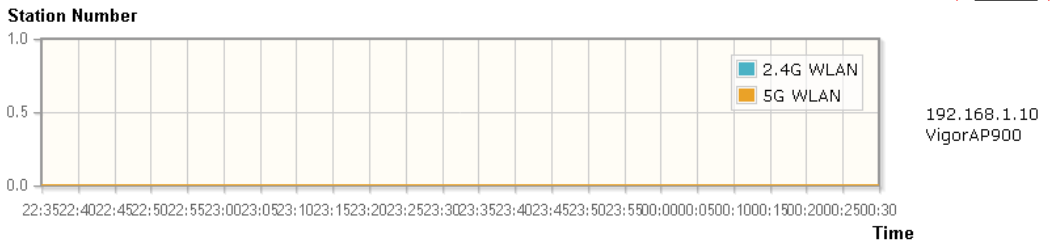
Note: Only browser supporting **HTML5** can display Total Traffic correctly.

VI-6-11 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.

Central AP Management >> Station Number

Hourly Records(2 Hours)



Note: Only browser supporting [HTML5](#) can display Station Number correctly.

VI-6-12 Load Balance

The parameters configured for Load Balance can help to distribute the traffic for all of the access points registered to Vigor router. Thus, the bandwidth will not be occupied by certain access points.

Central Management >> AP >> Load Balance

AP Load Balance By Station Number or Traffic ▾

Station Number Threshold

Wireless LAN (2.4GHz) (3-64)

Wireless LAN (5GHz) (3-64)

Traffic Threshold

Upload Limit bps (Default unit: K)

Download Limit bps (Default unit: K)

Action When Threshold Exceeded

Stop accepting new connections

Dissociate existing station by longest idle time

Dissociate existing station by worst signal strength if it is less than - dBm (%)

Note:

The maximum station number of Wireless LAN (2.4GHz) will be applied to both Wireless LAN (2.4GHz) and Wireless LAN (5GHz) if the firmware version of AP900 is less than or equal to 1.1.4.1.

Available settings are explained as follows:

Item	Description
AP Load Balance	It is used to determine the operation mode when the system detects overload between access points. Disable - Disable the function of AP load balance.

	<p>By Station Number -The operation of load balance will be executed based on the station number configured in this page. It is used to limit the allowed number for the station connecting to the access point. The purpose is to prevent lots of stations connecting to access point at the same time and causing traffic unbalanced. Please define the required station number for WLAN (2.4GHz) and WLAN (5GHz) separately.</p> <p>By Traffic - The operation of load balance will be executed according to the traffic configuration in this page.</p> <p>By Station Number or Traffic - The operation of load balance will be executed based on the station number or the traffic configuration.</p>
Station Number Threshold	Set the number of stations as a threshold to activate AP load balance.
Traffic Threshold	<p>Upload Limit -Use the drop down list to specify the traffic limit for uploading.</p> <p>Download Limit - Use the drop down list to specify the traffic limit for downloading.</p>
Action When Threshold Exceeded	<p>Stop accepting new connections - When the number of stations or the traffic reaches the threshold defined in this web page, Vigor router will stop any new connection asked by other access point.</p> <p>Dissociate existing station by longest idel time - When the access point is overload (e.g., reaching the limit of station number or limit of network traffic), it will terminate the network connection of the client's station which is idle for a longest time.</p> <p>Dissociate existing station by worst signal strength if it is less than - When the access point is overload (e.g., reaching the limit of station number or limit of network traffic), it will terminate the network connection of the client's station with the weakest signal.</p>

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

VI-6-13 Function Support List

List the AP management functions that the Access Points support under different firmware versions.

Central AP Management >> Function Support List

Model Name	AP710	AP800	AP810	AP900	AP902	AP910C
FW Version	1.2.0	1.1.6	1.1.6.1	1.1.7	1.1.7	1.1.6
Register						
DHCP	•	•	•	•	•	•
Static IP	•	•	•	•	•	•
Profile						
2.4GHz	•	•	•	•	•	•
5GHz		• (with N65)		•	•	•
AP Mode	•	•	•	•	•	•
Auto Provision	•	•	•	•	•	•
WLAN Enable/Disable	•	•	•	•	•	•
Limit Client	•		•	•	•	•
Airtime Fairness	•		•	•	•	•
Band Steering				•	•	•
Fast Roaming	•		•	•	•	•

Application Notes

A-1 How to use AP Management function (in Vigor2862) to check AP status and deploy WLAN profile

The administrator can manage the access points linked to Vigor2862.

1. Open External Devices>>Access Point Devices. Vigor2862 will detect the AP connecting to the router automatically and display as below:

External Device >> Access Point Devices

Status	WLAN Profile								
Clear Refresh									
Index	Device Name	IP Address	SSID	Encryption	Ch.	WL Client	Version	Password	
1	AP800_00507F6EE490	192.168.1.10	DrayTek-LAN-A	WPA+WPA2/PSK	ch11	0/64	1.0.5	Password	x

Note:
Green : Online Red : Offline Grey : Hidden SSID

Maximum support 20 APs.

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.

External Device >> Access Point Devices

Status	WLAN Profile					
Set to Factory Default						
	Profile Name	Main SSID	Security	Multi-SSID	WLAN ACL	Rate Control
<input checked="" type="checkbox"/>	Default	DrayTek-LAN-A	WPA+WPA2/PSK	Enable	None	None
<input type="checkbox"/>	---	---	---	---	---	---
<input type="checkbox"/>	---	---	---	---	---	---
<input type="checkbox"/>	---	---	---	---	---	---
<input type="checkbox"/>	---	---	---	---	---	---

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.

WLAN Profile Edit

Device Settings	
Profile Name	Default <input checked="" type="checkbox"/> Apply to All APs
Administrator	admin
Password	*****
2nd Subnet	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Operation Mode	AP

2.4G WLAN General Settings	
2.4G Mode	Mixed(11b+11g+11n)
2.4G Channel	2462MHz (Channel 11)
WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Tx Power	100%

5G WLAN General Settings	
5G Mode	Mixed (11a+11n)



Info

Apply to All APs can automatically apply the settings on Default profile to all of the access points registered to Vigor2862 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”.

- 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.

SSID1	SSID2	SSID3	SSID4
2.4G SSID			
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
SSID	DrayTek-LAN-A	LAN-A	<input type="checkbox"/> Hide SSID
VLAN	0 (0:untag)		
Isolate	<input type="checkbox"/> From Member		
Security Settings			
Encryption	WPA+WPA2/PSK		
	Set up RADIUS Server if 802.1X is enabled.		
	WPA		
	WPA Algorithms	<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES	
	Pass Phrase	*****	
	Key Renewal Interval	3600	Seconds
PMK Cache Period	10	Minutes	
Pre-Authentication	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
WEP			
Setup WEP Key if WEP is enabled.			
802.1X WEP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Access Control			
Mode	None		
List			
	Client's MAC Address : [] : [] : [] : [] : [] : []		
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/>			
Bandwidth Limit			
Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Auto Adjustment	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Upload	0 kbps	Download	0 kbps

- 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**.

External Device >> Access Point Devices

5G SSID1	5G SSID2	5G SSID3	5G SSID4
5G SSID			
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
SSID	DrayTek-5G	LAN-A	<input type="checkbox"/> Hide SSID
VLAN	0 (0:untag)		
Isolate	<input type="checkbox"/> From Member		
Security Settings			
Encryption	Disable		
	Set up RADIUS Server if 802.1X is enabled.		
	WPA		
	WPA Algorithms	<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES	
	Pass Phrase	<input type="text"/>	
Key Renewal Interval	3600	Seconds	
PMK Cache Period	10	Minutes	
Pre-Authentication	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
WEP			
Setup WEP Key if WEP is enabled.			
802.1X WEP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Access Control			
Mode	None		
List			
	Client's MAC Address : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>		
	<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/>		
Bandwidth Limit			
Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		Auto Adjustment <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Upload	0	Kbps	Download 0 Kbps

- Now, the AP (represented with *AP800_00507F6EE4980*) detected by Vigor router will be applied with the settings modified by Vigor router.

VI-7 Central Management (Switch)

Vigor router can manage lots of VigorSwitch devices connected to it. Through profile and group settings, the administrator can execute firmware/configuration backup, restore for VigorSwitch device, reboot the device or return to factory default settings of VigorSwitch at one time.



VI-7-1 Status

VI-7-1-1 Switch Status

Such page displays information, including Group, Switch name, IP address, model, System Up Time, Port in Use, Clients, and Firmware Version of VigorSwitch connected to Vigor2862 series.

Before checking the switch status, go to **Central Management >> External Device** to enable **External Device Auto Discovery**. Wait for the system to display available device(s).

Central Management >> External Device

- External Device Syslog
 External Device Auto Discovery

External Devices Connected

| [Refresh](#) |

Below shows available devices that connected externally:

On Line G1241, Switch Connection Uptime:00:05:32
IP Address:192.168.1.10:80
Account Clear

For security reason:

If you have changed the administrator password on External Device, please click the **Account** button to retype new username and password. Otherwise, the router will be unable to monitor the External Device device properly. Click the **Clear** button to Clear the off-line information and account information.

[OK](#)

Later, open **Central Management >> Switch >> Status**. Available VigorSwitch to be managed by such router will be listed under the New Switch List.

Central Management >> Switch >> Status

Switch Status	Switch Hierarchy	Detailed Info	Refresh
---------------	------------------	---------------	---------

View Group:

Status

Group	Switch Name	IP Address	Model	System Up Time	Port in Use	Clients	Firmware Version
-------	-------------	------------	-------	----------------	-------------	---------	------------------

New Switch List

Index	Switch Name	IP Address	MAC Address	Model	Firmware Version	Add Device
1	G1241	192.168.1.10	00:50:7F:F1:05:FD	G1241		<input type="button" value="Add New"/>

Note:

Supported VigorSwitch model and firmware version P2261 V3.11, G2260 V3.11, G1241 2.1.0, P1100 2.1.0.



Info

VigorSwitch listed below Status means the switch is managed by Viogr2862; VigorSwitch listed below New Switch List means it is not managed by Vigor2862 yet.

Click Add New to make the selected VigorSwitch to be managed by Vigor router.

Central Management >> Switch >> Status

Switch Status	Switch Hierarchy	Detailed Info	Refresh
---------------	------------------	---------------	---------

View Group:

Status

Group	Switch Name	IP Address	Model	System Up Time	Port in Use	Clients	Firmware Version
Default	Switch	192.168.1.10	G1241	0:00:00	0/24	0	2.1.0.1886

Note:

Supported VigorSwitch model and firmware version P2261 V3.11, G2260 V3.11, G1241 2.1.0, P1100 2.1.0.

Available settings are explained as follows:

Item	Description
Group	Display the name link of the group. You can click the link to modify the group settings if required.
Switch Name	Display the name link of VigorSwitch. You can click the name link to access into the switch profile.
IP Address	Display the IP address of VigorSwitch.
Model	Display the model name of VigorSwitch.
System Up Time	Display the time accumulated since this Vigorwitch is powered up.
Port in Use	Display how many devices connected to VigorSwitch.
Clients	Display the number of LAN ports used in VigorSwitch.
Firmware Version	Display the firmware version that VigorSwitch current used.
Add New	Such button will appear only when there is more than one switch connected to Vigor2862. The one under New Switch List is allowed to be managed under current used group. Simply click Add New.

Group	Switch Name	IP Address	Model	System Up Time	Port in Use	Clients	Firmware Version
111	SWITCH.G1241	192.168.1.10	G1241	0:02:19	1/24	0	2.1.0.1886

Index	Switch Name	IP Address	MAC Address	Model	Firmware Version	Add Device
1	P2261	192.168.1.226	00:50:7F:FD:C3:3C	P2261	v3.18	Add New

Note: Supported VigorSwitch model and firmware version P2261 V3.11, G2260 V3.11, G1241 2.1.0.Beta2, P1100 2.1.0.RC3a.

It will be better to group VigorSwitch devices with the same model.

VI-7-1-2 Switch Hierarchy

Such page displays the hierarchy of VigorSwitch(es) managed under Vigor2862.

Central Management >> Switch >> Status

Switch Status
Switch Hierarchy
Detailed Info
[Refresh](#)

Central Management >> Switch >> Status

Switch Status
Switch Hierarchy
Detailed Info
[Refresh](#)

Please note that, **Shutdown Port** is available for LAN port of VigorSwitch connects to a LAN device. When it is checked, after clicking OK, the network connection between that device and VigorSwitch will be terminated.

VI-7-2 Profile

This page will show general information, such as name, group, IP address, MAC address, model and password of VigorSwitch only when it connects to Vigor2862 series. By clicking the index number link, a profile setting page for that switch will be shown. Note that each profile represents one VigorSwitch.

Central Management >> Switch >> Profile

Profile List

Index	Name	Group	IP Address	MAC Address	Model	Password	Delete Profile
1	SWITCH-G1241	111,	192.168.1.10	00:50:7F:F1:05:FD	G1241	Password	X
2	P2261	111,	192.168.1.226	00:50:7F:FD:C3:3C	P2261	Password	X

Available settings are explained as follows:

Item	Description
Index	Click the number link to access into the switch profile. Note: Each connected VigorSwitch will have one setting profile. If there are many switches connected to Vigor2862, different index number will be used to represent different VigorSwitch.
Name	Display the user defined name of VigorSwitch.
Group	Display the group name of VigorSwitch(es).
IP Address	Display the IP address of VigorSwitch.
MAC Address	Display the MAC address of VigorSwitch.
Model	Display the model name of VigorSwitch.
Password	Click it to display the account information including username and password.
Delete Profile	Click the mark of "X" to delete the switch profile.

To edit profile for the selected switch:

- Click index number link (e.g. #1) to open the following page.

Central Management >> Switch >> Profile

Switch Profile 1 | [Get Setting from External Switch](#) |

General | **VLAN** | **Port** | [Set to Factory Default](#)

Switch Name	<input type="text" value="Switch"/>
Comment	<input type="text"/>
<input type="checkbox"/> Copy configuration from:	<input type="text" value="None"/>
Login Password	<input type="text" value="admin"/>
IP Address	DHCP 192.168.1.10

Note:

The router configuration will be updated when getting profile settings from external switch.

Available settings are explained as follows:

Item	Description
Switch Name	Type a name for the Switch. The purpose of name is used for identification. It is useful when there are many VigorSwitch (same modes) devices connecting to Vigor2862 series.
Comment	Type the text in such field if additional explanation for the switch is required.
Copy configuration from	Check the box to copy configuration from other device. Use the drop down list to choose the one you need. Note, if there is only one VigorSwitch connected and managed by Vigor2862 series, then such field is unavailable.
Login Password	Display the original login password for the VigorSwitch. However, if Group Password (in Central Management >>Switch>>Group) is configured with other string, then such field is not allowed to type any other password. And only the group password will be shown, instead.
IP Address	Display the dynamic IP address (of the connected switch) assigned by Vigor2862.
Save	Click it to save the settings.
Cancel	Click it to return to previous web page without saving the setting changes.
Send to Device	Click it to transfer the configuration change (e.g, login password, switch name, etc.) to the VigorSwitch immediately.

- After finished the settings, click VLAN tab to open following page.

Blank page due to LAN>>VLAN not configured previously:

Central Management >> Switch >> Profile

Switch Profile 1 Switch | [Get Setting from External Switch](#) |
| [Set to Factory Default](#) |

General **VLAN** Port

Router VLAN				LAN Port				WLAN 2.4G SSID				WLAN 5G SSID			
Group	Subnet	VID	Priority	1	2	3	4	1	2	3	4	1	2	3	4

External Switch VLAN

Port Members

Remove Tag (PVID)

Note:
The router configuration will be updated when getting profile settings from external switch

Setting page with LAN>>VLAN configured previously:

Central Management >> Switch >> Profile

Switch Profile 1 SWITCH-G1241 | Get Setting from External Switch |
| Set to Factory Default |

General **VLAN** Port

Router VLAN

Tag based VLAN				LAN Port						WLAN 2.4G SSID				WLAN 5G SSID			
Group	Subnet	VID	Priority	1	2	3	4	5	6	1	2	3	4	1	2	3	4
VLAN0	LAN1	0	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN1	LAN1	20	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN2	LAN1	100	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

External Switch VLAN

Port Members

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Remove Tag (PVID)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VLAN0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Note: The router configuration will be updated when getting profile settings from external switch

- Click **Save** to save VLAN configuration. Then, click **Port** tab to access the following page:

Central Management >> Switch >> Profile

Switch Profile 1 Switch1241 | Get Setting from External Switch |
| Set to Factory Default |

General **VLAN** **Port**

Port	Description	Port Control	Schedule	Rate Limit	
				Ingress Rate(Kbps)	Egress Rate(Kbps)
*		Enable Port <input type="checkbox"/>			
1		Enable Port <input type="checkbox"/>			
2	Uplink	Enable Port <input type="checkbox"/>			
3		Enable Port <input type="checkbox"/>			
4		Enable Port <input type="checkbox"/>			
5		Enable Port <input type="checkbox"/>			
6		Enable Port <input type="checkbox"/>			
7		Enable Port <input type="checkbox"/>			
8		Enable Port <input type="checkbox"/>			
9		Enable Port <input type="checkbox"/>			
10		Enable Port <input type="checkbox"/>			
11		Enable Port <input type="checkbox"/>			
12		Enable Port <input type="checkbox"/>			
13		Enable Port <input type="checkbox"/>			
14		Enable Port <input type="checkbox"/>			
15		Enable Port <input type="checkbox"/>			
16		Enable Port <input type="checkbox"/>			
17		Enable Port <input type="checkbox"/>			
18		Enable Port <input type="checkbox"/>			
19		Enable Port <input type="checkbox"/>			
20		Enable Port <input type="checkbox"/>			
21		Enable Port <input type="checkbox"/>			
22		Enable Port <input type="checkbox"/>			
23		Enable Port <input type="checkbox"/>			
24		Enable Port <input type="checkbox"/>			

Note:

- The router configuration will be updated when getting profile settings from external switch.
- Double quotation mark (*) is not supported in Description columns.

Available settings are explained as follows:

Item	Description
Description	If required, type a brief description to explain the device connected to VigorSwitch via the LAN port.
Port Control	Disable Port - The port (e.g, Port 2 in this case) which is used

	<p>to connect VigorSwitch and Vigor2862 will not be shutdown by Vigor2862 series.</p> <p>Other LAN ports of VigorSwitch allow to connect to any LAN device. When it is checked, after clicking Save, the network connection between that device and VigorSwitch will be terminated.</p> <p>Schedule - Two sechule profiles can be specified here to force Vigor2862 executing specific action to VigorSwitch.</p>
Rate Limit	<p>Check the box for typing the ingress rate / egress rate for the selected VigorSwitch. After clicking Save, the value modified in this page will be written to VigorSwitch and enabled.</p>


- Click **Save** to save the changes and then click **Send to Device**. Settings will be sent to VigorSwitch immediately.

Central Management >> Switch >> Profile

Switch Profile 1 SWITCH-G1241 | [Get Setting from Extenal Switch](#) |

General **VLAN** **Port** | [Set to Factory Default](#) |

Post Settings to Vigor Switch



Note: The router configuration will be updated when getting profile settings from external switch.
 Double quotation mark (") is not supported in Description columns.

VI-7-3 Group

Different switches can be classified into different group(s). Specific password for a group can be defined and applied to every switch under that group.

Through the common password setting, it is not necessary for the system administrator to remember various login passwords to access into different VigorSwitch devices.

Central Management >> Switch >> Group

Index	Group Name	Member Switch
1	Default	Switch1241(192.168.1.10)
2		
3		
4		
5		
6		
7		
8		
9		
10		

Click any index number link to create a new switch group.

Index 2:

Available settings are explained as follows:

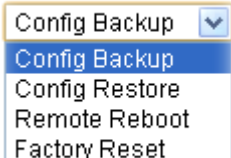
Item	Description
Group Name	Type a name as the group name. Different switches can be classified within a group.
Group Password	Type a password that administrator can use to access into the managed VigorSwitch connecting to Vigor2862 series. All of the switches under the same group can be accessed into via such group password.
Existing Switch	Display all of the VigorSwitch devices connecting to Vigor2862.
Member Switch	Choose the switches you want to group and click the button ">>" to move the selected devices onto the field of Member Switch. Devices under Member Switch will be grouped under such group profile.
OK	Click it to save the configuration.
Cancel	Click it to exit the setting page without saving any change.

VI-7-4 Maintenance

Such feature can execute configuration backup, restore of selected VigorSwitch device(s) or reboot the VigorSwitch devices remotely or reset the VigorSwitch devices with factory default settings, without accessing into the web user interface of VigorSwitch respectively. It is convenient for system administrator to manage VigorSwitch devices.

Central Management >> Switch >> Maintenance

Available settings are explained as follows:

Item	Description
Select Action	<p>Action Type - Four actions including configuration backup, configuration restore, remote reboot and factory reset are offered by Vigor2862 to perform on VigorSwitch.</p>  <p>File/Path - Click the button to find out the required file.</p>
Select Device	<p>Existing Device - Display all of the VigorSwitch devices connecting to Vigor2862.</p> <p>Selected Device - Choose the switches you want to group and click the button ">>" to move the existing devices onto the field of Selected Device. Devices under Selected Device will be applied with the action</p>
OK	Click it to immediately perform the action (configuration backup, configuration restore, remote reboot and factory reset) on the device(s) listed in Selected Device.
Cancel	Click it to cancel the setting changes.

VI-7-5 Alert and Log

Alert and Log is helpful for the user to understand the abnormal situation occurred in VigorSwitch quickly. When the system detects an error, information of abnormal condition will be recorded to the database; or the system will send an alert to the specified device (via e-mail or SMS) to warn the user.

VI-7-5-1 Alert Setup

This page is used to define the name of alert, level of alert (in color), and determine to record the data in the database, or send a notification message to the user based on the level.

Central Management >> Switch >> Alert and Log

Alert Setup **Switch and Port Setup** **Alert Logs**

Alert and Log

Alert Levels and Action | [Set to Factory Default](#)

Index	Enable	Level Name	Color	Create Log	Send Notification	SMS/Email Service object
1	<input checked="" type="checkbox"/>	No Alert	No Color	No Log	No Notification	
2	<input checked="" type="checkbox"/>	Minor Alert	 	Enable	No Notification	
3	<input checked="" type="checkbox"/>	Moderate Alert	 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	sms 1 - ??? sms 1 - ???
4	<input checked="" type="checkbox"/>	Major Alert	 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	sms 1 - ??? sms 1 - ???
5	<input type="checkbox"/>		 	<input type="checkbox"/>	<input type="checkbox"/>	sms 1 - ??? sms 1 - ???
6	<input type="checkbox"/>		 	<input type="checkbox"/>	<input type="checkbox"/>	sms 1 - ??? sms 1 - ???
7	<input type="checkbox"/>		 	<input type="checkbox"/>	<input type="checkbox"/>	sms 1 - ??? sms 1 - ???
8	<input type="checkbox"/>		 	<input type="checkbox"/>	<input type="checkbox"/>	sms 1 - ??? sms 1 - ???

Available settings are explained as follows:

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

Alert and Log	Check it to enable this feature.
Alert Levels and Action	<p>Level Name - Define names for representing the severity of alert event. The default names for index 1 to index 4 will be shown on each setting box. Index 5 to index 8 are reserved for user-defined.</p> <p>Color - Define the color for each level of alert. However, the color of index 1 is No color and unable to be changed.</p> <p>Create Log - Check the box to create log of alert. Such log will be seen on Alert Logs page. Note that No Log for index 1; and log for index 2 is enabled in default.</p> <p>Send Notification - If it is checked, Vigor router's system will send notification to specified phone number via SMS.</p> <p>SMS/Email Service Object - Choose the SMS object which will get the SMS from Vigor router. Up to 4 objects can be selected at one time.</p>

VI-7-5-2 Switch and Port Setup

This page defines enabling switch alert and/or port alert for each switch.

Central Management >> Switch >> Alert and Log

Alert Setup		Switch and Port Setup		Alert Logs	
Index	Switch Name	IP	Model	Switch Alert	Port Alert
1	G2260	192.168.1.11	G2260	Enable ▾	Enable ▾

OK Cancel

Available settings are explained as follows:

Item	Description
Switch Alert	Enable - Check it to enable alert mechanism for VigorSwitch.
Port Alert	Enable - Check it to enable alert mechanism for each port of VigorSwitch.

Click the Switch Name link (e.g., G2260 in this case) to get detailed settings.

Alert Setup		Switch and Port Setup		Alert Logs	
Index	Switch Name	IP	Model	Switch Alert	Port Alert
1	G2260	192.168.1.11	G2260	Enable ▼	Enable ▼

G2260

[|Set to Factory Default|](#)

Switch Alert

Incident	Level
Cold Start	Major Alert ▼
Warm Start	Major Alert ▼
Disconnect	Major Alert ▼
Reconnect	Minor Alert ▼

Port Alert

Port	Description	Device Disconnects	Device Reconnects	Schedule on/off	Shutdown En/Dis
1	Uplink	Minor Alert ▼	Minor Alert ▼	Minor Alert ▼	Minor Alert ▼
2		Minor Alert ▼	Minor Alert ▼	Minor Alert ▼	Minor Alert ▼
3		Minor Alert ▼	Minor Alert ▼	Minor Alert ▼	Minor Alert ▼
4		Minor Alert ▼	Minor Alert ▼	Minor Alert ▼	Minor Alert ▼
5		Minor Alert ▼	Minor Alert ▼	Minor Alert ▼	Minor Alert ▼
6		Minor Alert ▼	Minor Alert ▼	Minor Alert ▼	Minor Alert ▼
7		Minor Alert ▼	Minor Alert ▼	Minor Alert ▼	Minor Alert ▼
8		Minor Alert ▼	Minor Alert ▼	Minor Alert ▼	Minor Alert ▼
9		Minor Alert ▼	Minor Alert ▼	Minor Alert ▼	Minor Alert ▼

Available settings are explained as follows:

Item	Description
Switch Alert	<p>When VigorSwitch encounters the following alert events, alert mechanism will perform corresponding actions based on the severity level of the incident encountered.</p> <p>Incident - At present, Cold Start, Warm Start, Disconnect and Reconnect will be treated as alert events.</p> <p>Level - Specify the severity level for each incident. To define more severity level for choosing in this page, simply open Central Management>>Switch>>Alert and Log and click Alert Setup.</p>
Port Alert	<p>Port - Available Ethernet ports for the selected VigorSwitch (e.g., G2260 in this case) will be shown on this page. Each port can be configured with different alert level for different alert events.</p>

VI-7-5-3 Alert Logs

The user can get the information by filtering the collective information based on the conditions specified in this page.

Central Management >> Switch >> Alert and Log

Alert Setup	Switch and Port Setup	Alert Logs										
<input type="checkbox"/> Select Columns to Filter Logs												
<table border="1"> <thead> <tr> <th>Level</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> No Alert</td> </tr> <tr> <td><input checked="" type="checkbox"/> Minor Alert</td> </tr> <tr> <td><input type="checkbox"/> Moderate Alert</td> </tr> <tr> <td><input checked="" type="checkbox"/> Major Alert</td> </tr> </tbody> </table>	Level	<input type="checkbox"/> No Alert	<input checked="" type="checkbox"/> Minor Alert	<input type="checkbox"/> Moderate Alert	<input checked="" type="checkbox"/> Major Alert	<table border="1"> <thead> <tr> <th>Type</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> Switch ALert</td> </tr> <tr> <td><input type="checkbox"/> Port Alert</td> </tr> </tbody> </table>	Type	<input checked="" type="checkbox"/> Switch ALert	<input type="checkbox"/> Port Alert	<table border="1"> <thead> <tr> <th>Switch</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> Switch1241</td> </tr> </tbody> </table>	Switch	<input checked="" type="checkbox"/> Switch1241
Level												
<input type="checkbox"/> No Alert												
<input checked="" type="checkbox"/> Minor Alert												
<input type="checkbox"/> Moderate Alert												
<input checked="" type="checkbox"/> Major Alert												
Type												
<input checked="" type="checkbox"/> Switch ALert												
<input type="checkbox"/> Port Alert												
Switch												
<input checked="" type="checkbox"/> Switch1241												
<input type="button" value="OK"/>												

Alert Logs

Show per page | [Refresh](#) |

0 Logs

Index	Level Name	Time	Type	Switch	Port	Incident
-------	------------	------	------	--------	------	----------

Available settings are explained as follows:

Item	Description
Select Columns to Filter Logs	<p>Level - The alert can be divided into four levels, No Alert, Minor Alert, Moderate Alert and Major Alert. Check the one(s) you want to check in Alert Logs list.</p> <p>Type - Check the type (switch / port) of the log to be displayed in Alert Logs list.</p> <p>Switch - Switch(es) connecting to Vigor router will be shown in this area. Click the one you need.</p> <p>OK - Click it to save the configuration.</p> <p>Log related to the items selected above will be shown in Alert Logs list.</p>
Alert Logs	This area displays logs (level name, time, type, switch, port, and incident) related to VigorSwitch managed by Vigor router.

VI-7-6 Database Setup

The database of switch can be used to record alert logs and traffic history. This page is used to determine if it is necessary for the user information to be recorded in the database of switch.

Central Management >> Switch >> Database Setup

Enable Database to Record alert logs and traffic history

File Path : /db

Database Usage : 0.0MB / 45MB

Notification and Action when Storage Exceeded

Notification Don't send notification

Send notification

Email Notification Object 1 - ???

SMS Notification Object 1 - John

Action Stop recording user information

Backup and clean up all user info, and start a new record

OK

Available settings are explained as follows:

Item	Description
Enable Database to Record alert logs and traffic history	Check the box to make the database (in USB disk) to record the alert logs and traffic history.
Notification and Action when Storage Exceeded	
Notification	<p>Don't send notification - No notification will be sent out when there is no capacity for storage in USB.</p> <p>Send notification - A notification will be sent out when there is no capacity for storage in USB.</p>
Action	<p>Stop recording user information - When the capacity of log is full, the system will stop recording.</p> <p>Backup and clean up all user infor, and start a new record - Only the newest events will be recorded by the system.</p>

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

VI-7-7 Support List

This page lists all models of VigorSwitch which can be managed by Vigor2862 via Central Management>>Switch.

Central Management >> Switch >> Support List

Model	Status	Firmware Version
Vigor Switch P2261	V	v3.11
Vigor Switch G2260	V	v3.11
Vigor Switch P1280	V	v2.0.0

VI-8 Central Management (External Devices)

Vigor router can be used to connect with many types of external devices. In order to control or manage the external devices conveniently, open **External Devices** to make detailed configuration.

Central Management >> External Device

- External Device Syslog
- External Device Auto Discovery

External Devices Connected

| [Refresh](#) |

Below shows available devices that connected externally:

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.

OK

Available settings are explained as follows:

Item	Description
External Device Syslog	Check this box to display information of the detected device on Syslog.
External Device Auto Discovery	Check this box to detect the external device automatically and display on this page.

From this web page, check the box of **External Device Auto Discovery**. Later, all the available devices will be displayed in this page with icons and corresponding information. You can change the device name if required or remove the information for off-line device whenever you want.

External Device >> All Devices

- External Device Syslog
- External Device Auto Discovery

External Devices Connected

Below shows available devices that connected externally:

On Line VigorAP900, VigorAP900, Connection Uptime:18:15:27
IP Address:10.28.60.12

Account

Clear

On Line P2261, Connection Uptime:18:15:17

IP Address:192.168.1.226

Account

Clear

For security reason:

If you have changed the administrator password on External Device, please click the **Account** button to retype new username and password. Otherwise, the router will be unable to monitor the External Device device properly. Click the **Clear** button to Clear the off-line information and account information.

OK

When you finished the configuration, click **OK** to save it.



Info

Only DrayTek products can be detected by this function.

Part VII Others



Objects Settings



USB

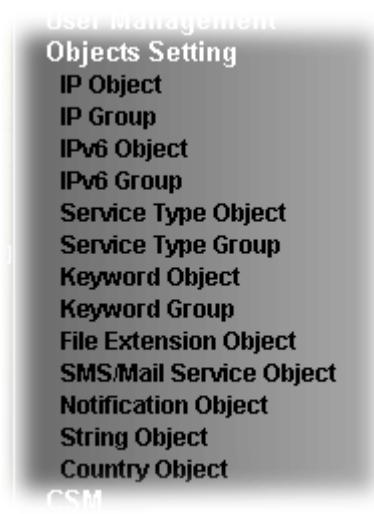
Define objects such as IP address, service type, keyword, file extension and others. These pre-defined objects can be applied in CSM.

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.

VII-1 Objects Settings

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

Web User Interface



VII-1-1 IP Object

For IPs in a range and service ports in a limited range usually will be applied in configuring router's settings, therefore we can define them with *objects* and bind them with *groups* for using conveniently. Later, we can select that object/group for applying it. For example, all the IPs in the same department can be defined with an IP object (a range of IP address).

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

[Create from ARP Table](#)
[Create from Routing Table](#)

IP Object Profiles:

| [Set to Factory Default](#) |

View:

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

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

[Next](#) >>

<p>Export IP Object</p> <p><input checked="" type="radio"/> Backup the current IP Objects with a CSV file</p> <p><input type="radio"/> Download the default CSV template to edit</p> <p><input type="button" value="Download"/></p>	<p>Restore IP Object</p> <p><input type="button" value="選擇檔案"/> 未選擇檔案</p> <p><input type="button" value="Restore"/></p>
--	--

Note:

For better compatibility, it's suggested to edit IP Objects with the provided default CSV template.

Available settings are explained as follows:

Item	Description
View	Use the drop down list to choose a type (Single Address, Range Address, Subnet Address, Mac Address or all) that IP object with the selected type will be shown on this page.
Set to Factory Default	Clear all profiles.
Search	Type a string of the IP object that you wan to search.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.
Address	Display the IP address configured for the object profile.

Export IP Object	<p>Usually, the IP objects can be created one by one through the web page of Objects>>IP Object. However, to a user who wants to save more time in bulk creating IP objects, a quick method is offered by Vigor router to modify the IP objects with a single file, a CSV file.</p> <p>All of the IP objects (or the template) can be exported as a file by clicking Download. Then the user can open the CSV file through Microsoft Excel and modify all the IP objects at the same time.</p> <p>Backup the current IP Objects with a CSV file - Click it to backup current IP objects as a CSV file. Such file can be restored for future use.</p> <p>Download the default CSV template to edit - After clicking it, press Download to store the default CSM template (a table without any input data) to your hard disk.</p> <p>Download - Download the CSV file from Vigor router and store in your hard disk.</p>
Restore IP Object	<p>Select - Click it to specify a predefined CSV file.</p> <p>Restore - Import the selected CSV file onto Vigor router.</p>

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

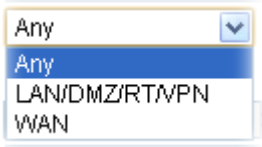
1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:

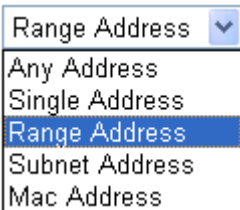
Objects Setting >> IP Object

Profile Index : 1

Name:	<input type="text" value="RD Department"/>
Interface:	<input type="text" value="Any"/>
Address Type:	<input type="text" value="Range Address"/>
Mac Address:	<input type="text" value="00"/> <input type="text" value="00"/> <input type="text" value="00"/> <input type="text" value="00"/> <input type="text" value="00"/> <input type="text" value="00"/>
Start IP Address:	<input type="text" value="192.168.1.59"/>
End IP Address:	<input type="text" value="192.168.1.65"/>
Subnet Mask:	<input type="text" value="0.0.0.0"/>
Invert Selection:	<input type="checkbox"/>

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Interface	<p>Choose a proper interface.</p>  <p>For example, the Direction setting in Edit Filter Rule will ask you specify IP or IP range for WAN or LAN/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</p>

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

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

VII-1-2 IP Group

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

Objects Setting >> IP Group

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

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

Available settings are explained as follows:

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

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

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:

Objects Setting >> IP Group

Profile Index : 1

Name:

Interface: ▼

Available IP Objects

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

Selected IP Objects

(Empty)

Available settings are explained as follows:

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

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

VII-1-3 IPv6 Object

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

Objects Setting >> IPv6 Object

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

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

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

Available settings are explained as follows:

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

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

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:

Objects Setting >> IPv6 Object

Profile Index : 1

Name:	<input type="text"/>
Address Type:	Range Address <input type="button" value="v"/>
Match Type:	<input checked="" type="radio"/> 128 Bits <input type="radio"/> Suffix 64 Bits(Interface ID)
Mac Address:	<input type="text" value="00:00:00:00:00:00"/>
Start IP Address:	<input type="text" value="FE80::21D:AFF:FEF7:C048"/> <input type="button" value="Select"/>
End IP Address:	<input type="text"/> <input type="button" value="Select"/>
Prefix Length:	<input type="text" value="0"/>
Invert Selection:	<input type="checkbox"/>

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Address Type	<p>Determine the address type for the IPv6 address.</p> <p>Select Single Address if this object contains one IPv6 address only.</p> <p>Select Range Address if this object contains several IPv6s within a range.</p> <p>Select Subnet Address if this object contains one subnet for IPv6 address.</p> <p>Select Any Address if this object contains any IPv6 address.</p> <p>Select Mac Address if this object contains Mac address.</p> <div style="border: 1px solid black; padding: 2px; margin-top: 5px;"> Range Address <input type="button" value="v"/> Any Address Single Address Range Address Subnet Address Mac Address </div>
Match Type	When Range Address is selected as Address Type, please specify the match type (128 Bits or Suffix 64 Bits) for the IPv6 address.
Mac Address	Type the MAC address of the network card which will be controlled.
Start IP Address	Type the start IPv6 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.

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

VII-1-4 IPv6 Group

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

Objects Setting >> IPv6 Group

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

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

Available settings are explained as follows:

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

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

- Click the number (e.g., #1) under Index column for configuration in details.
- The configuration page will be shown as follows:

Objects Setting >> IPv6 Group

Profile Index : 1

Name:

Available IPv6 Objects	<input type="button" value=">>"/> <input type="button" value="<<"/>	Selected IPv6 Objects
------------------------	--	-----------------------

Available settings are explained as follows:

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

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

VII-1-5 Service Type Object

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

Objects Setting >> Service Type Object

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

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

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

Available settings are explained as follows:

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

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

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:

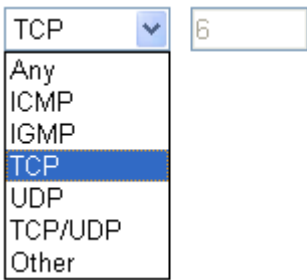
Objects Setting >> Service Type Object Setup

Profile Index : 1

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

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Protocol	Specify the protocol(s) which this profile will apply to. 
Source/Destination Port	Source Port and the Destination Port columns are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number. (=) - when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this profile. (!=) - when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type. (>) - the port number greater than this value is available. (<) - the port number less than this value is available for this profile.

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

Objects Setting >> Service Type Object

Service Type Object Profiles:

Index	Name	Index
<u>1.</u>	www	<u>17.</u>
<u>2.</u>	SIP	<u>18.</u>
<u>3.</u>		<u>19.</u>
<u>4.</u>		<u>20.</u>

VII-1-6 Service Type Group

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

Objects Setting >> Service Type Group

Service Type Group Table:

[Set to Factory Default](#)

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

Available settings are explained as follows:

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

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

1. Click the number (e.g., #1) under Group column for configuration in details.
2. The configuration page will be shown as follows:

Objects Setting >> Service Type Group Setup

Profile Index : 1

Name:

Available Service Type Objects	Selected Service Type Objects
<div style="border: 1px solid black; padding: 2px;"> <p>1-www</p> <p style="background-color: #000080; color: white;">2-SIP</p> </div>	<div style="border: 1px solid black; height: 80px; width: 100%;"></div>
<input type="button" value=">>"/> <input type="button" value="<<"/>	

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.

VII-1-7 Keyword Object

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

Objects Setting >> Keyword Object

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

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

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

Available settings are explained as follows:

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

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

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:

Objects Setting >> Keyword Object Setup

Profile Index : 1

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

Limit of Contents: Max 3 Words and 63 Characters.
Each word should be separated by a single space.

You can replace a character with %HEX.
Example:
Contents: backdoo%72 virus keep%20out

Result:
1. backdoor
2. virus
3. keep out

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile, e.g., game. Maximum 15 characters are allowed.
Contents	Type the content for such profile. For example, type <i>gambling</i> as Contents. When you browse the webpage, the page with gambling information will be watched out and be passed/blocked based on the configuration on Firewall settings.

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

VII-1-8 Keyword Group

This page allows you to bind several keyword objects into one group. The keyword groups set here will be chosen as black /white list in CSM >>URL /Web Content Filter Profile.

Objects Setting >> Keyword Group

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

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

Available settings are explained as follows:

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

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

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:


Objects Setting >> Keyword Group Setup

Profile Index : 1

Name:

Available Keyword Objects	Selected Keyword Objects(Max 16 Objects)
1-Key-1 2-Key-2	

Available settings are explained as follows:

Item	Description
Name	Type a name for this group. Maximum 15 characters are allowed.
Available Keyword Objects	You can gather keyword objects from Keyword Object page within one keyword group. All the available Keyword objects that you have created will be shown in this box.
Selected Keyword Objects	Click  button to add the selected Keyword objects in this box.

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

VII-1-9 File Extension Object

This page allows you to set eight profiles which will be applied in **CSM>>URL Content Filter**. All the files with the extension names specified in these profiles will be processed according to the chosen action.

Objects Setting >> File Extension Object

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

Profile	Name	Profile	Name
<u>1.</u>		<u>5.</u>	
<u>2.</u>		<u>6.</u>	
<u>3.</u>		<u>7.</u>	
<u>4.</u>		<u>8.</u>	

Available settings are explained as follows:

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

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

1. Click the number (e.g., #1) under Profile column for configuration in details.
2. The configuration page will be shown as follows:

Objects Setting >> File Extension Object Setup

Profile Index: 1 Profile Name:

Categories	File Extensions
Image <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .bmp <input type="checkbox"/> .dib <input type="checkbox"/> .gif <input type="checkbox"/> .jpeg <input type="checkbox"/> .jpg <input type="checkbox"/> .jpg2 <input type="checkbox"/> .jp2 <input type="checkbox"/> .pct <input type="checkbox"/> .pcx <input type="checkbox"/> .pic <input type="checkbox"/> .pict <input type="checkbox"/> .png <input type="checkbox"/> .tif <input type="checkbox"/> .tiff
Video <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .asf <input type="checkbox"/> .avi <input type="checkbox"/> .mov <input type="checkbox"/> .mpe <input type="checkbox"/> .mpeg <input type="checkbox"/> .mpg <input type="checkbox"/> .mp4 <input type="checkbox"/> .qt <input type="checkbox"/> .rm <input type="checkbox"/> .wmv <input type="checkbox"/> .3gp <input type="checkbox"/> .3gpp <input type="checkbox"/> .3gpp2 <input type="checkbox"/> .3g2
Audio <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .aac <input type="checkbox"/> .aiff <input type="checkbox"/> .au <input type="checkbox"/> .mp3 <input type="checkbox"/> .m4a <input type="checkbox"/> .m4p <input type="checkbox"/> .ogg <input type="checkbox"/> .ra <input type="checkbox"/> .ram <input type="checkbox"/> .vox <input type="checkbox"/> .wav <input type="checkbox"/> .wma
Java <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .class <input type="checkbox"/> .jad <input type="checkbox"/> .jar <input type="checkbox"/> .jav <input type="checkbox"/> .java <input type="checkbox"/> .jcm <input type="checkbox"/> .js <input type="checkbox"/> .jse <input type="checkbox"/> .jsp <input type="checkbox"/> .jtk
ActiveX <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .alx <input type="checkbox"/> .apb <input type="checkbox"/> .axs <input type="checkbox"/> .ocx <input type="checkbox"/> .olb <input type="checkbox"/> .ole <input type="checkbox"/> .tlb <input type="checkbox"/> .viv <input type="checkbox"/> .vrm
Compression <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for this profile. The maximum length of the name you can set is 7 characters.

3. Type a name for such profile and check all the items of file extension that will be processed in the router. Finally, click **OK** to save this profile.

VII-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>	Custom 1		
<u>10.</u>	Custom 2		

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.
Index	Display the profile number that you can configure.
Profile	Display the name for such SMS profile.
SMS Provider	Display the service provider which offers SMS service.

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

1. Click the **SMS Provider** tab, and click the number (e.g., #1) under Index column for configuration in details.

Object Settings >> SMS / Mail Service Object

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

- The configuration page will be shown as follows:

Objects Setting >> SMS / Mail Service Object

Profile Index: 1

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

Note:

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

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such SMS profile. The maximum length of the name you can set is 31 characters.
Service Provider	Use the drop down list to specify the service provider which offers SMS service.
Username	Type a user name that the sender can use to register to selected SMS provider. The maximum length of the name you can set is 31 characters.
Password	Type a password that the sender can use to register to selected SMS provider. The maximum length of the password you can set is 31 characters.
Quota	Type the number of the credit that you purchase from the service provider chosen above. Note that one credit equals to one SMS text message on the standard route.
Sending Interval	To avoid quota being exhausted soon, type time interval for sending the SMS.

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

Object Settings >> SMS / Mail Service Object

SMS Provider		Mail Server		Set to Factory Default
Index	Profile Name	SMS Provider		
1.	Line_down	kotsms.com.tw (TW)		
2.		kotsms.com.tw (TW)		
3.		kotsms.com.tw (TW)		
4.		kotsms.com.tw (TW)		

Customized SMS Service

Vigor router offers several SMS service provider to offer the SMS service. However, if your service provider cannot be found from the service provider list, simply use Index 9 and Index 10 to make customized SMS service. The profile name for Index 9 and Index 10 are fixed.

Object Settings >> SMS / Mail Service Object

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

You can click the number (e.g., #9) under Index column for configuration in details.

Objects Setting >> SMS / Mail Service Object

Profile Index: 9

Profile Name	<input type="text" value="Custom 1"/>
Service Provider	<input type="text"/>
<div style="border: 1px solid black; height: 50px; width: 100%;"></div>	
<p>Please contact with your SMS provide to get the exact URL String eg:bulksms.vsms.net:5567/eapi/submission/send_sms/2/2.0? username=###txtUser### &password=###txtPwd###&msisdn=###txtDest###&message=###txtMsg###</p>	
Username	<input type="text"/>
Password	<input type="text"/>
Quota	<input type="text" value="10"/>
Sending Interval	<input type="text" value="3"/> (seconds)

Note:

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

Available settings are explained as follows:

Item	Description
Profile Name	Display the name of this profile. It cannot be modified.
Service Provider	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 Factory Default
Index	Profile Name		
<u>1.</u>			
<u>2.</u>			
<u>3.</u>			
<u>4.</u>			
<u>5.</u>			
<u>6.</u>			
<u>7.</u>			
<u>8.</u>			
<u>9.</u>			
<u>10.</u>			

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.
Index	Display the profile number that you can configure.
Profile	Display the name for such mail server profile.

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

1. Click the **Mail Server** tab, and click the number (e.g., #1) under Index column for configuration in details.

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	<input type="text" value="Mail_Notify"/>
SMTP Server	<input type="text" value="192.168.1.98"/>
SMTP Port	<input type="text" value="25"/>
Sender Address	<input type="text" value="carrie_ni@draytek.com"/>
<input type="checkbox"/> Use SSL	
<input checked="" type="checkbox"/> Authentication	
Username	<input type="text" value="John"/>
Password	<input type="password" value="••••"/>
Sending Interval	<input type="text" value="0"/> (seconds)

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

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such mail service profile. The maximum length of the name you can set is 31 characters.
SMTP Server	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.

Sending Interval	Define the interval for the system to send the SMS out.
-------------------------	---

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

Object Settings >> SMS / Mail Service Object

SMS Provider	Mail Server	Set to Factory Default
Index	Profile Name	
<u>1.</u>	Mail_Notify	
<u>2.</u>		
<u>3.</u>		

VII-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

Set to Factory Default		
Index	Profile Name	Settings
<u>1.</u>		
<u>2.</u>		
<u>3.</u>		
<u>4.</u>		
<u>5.</u>		
<u>6.</u>		
<u>7.</u>		
<u>8.</u>		

To set a new profile, please do the steps listed below:

- Open **Object Setting>>Notification Object**, and click the number (e.g., #1) under Index column for configuration in details.

Object Settings >> Notification Object

Index	Profile Name
<u>1.</u>	
<u>2.</u>	
<u>3.</u>	
<u>4.</u>	
<u>5.</u>	

- The configuration page will be shown as follows:

Objects Setting >> Notification Object

Profile Index: 1

Profile Name

Category	Status
WAN	<input type="checkbox"/> Disconnected <input type="checkbox"/> Reconnected
VPN Tunnel	<input type="checkbox"/> Disconnected <input type="checkbox"/> Reconnected
Temperature Alert	<input type="checkbox"/> Out of Range
WAN Budget	<input type="checkbox"/> Limit Reached
Central VPN Management	<input type="checkbox"/> CPE Offline <input type="checkbox"/> CPE Config Backup Fail <input type="checkbox"/> CPE Config Restore Fail <input type="checkbox"/> CPE Firmware Upgrade Fail <input type="checkbox"/> CPE VPN Profile Setup Fail
High Availability	<input type="checkbox"/> Failover Occurred <input type="checkbox"/> Config Sync Fail <input type="checkbox"/> Router Unstable

Note:

When High Availability is enabled, "Sending Interval" of **SMS Provider profile** should set to 0.

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.

- After finishing all the settings here, please click **OK** to save the configuration.

Object Settings >> Notification Object

[Set to Factory Default](#)

Index	Profile Name	Settings
<u>1.</u>	Notify_attack	WAN VPN
<u>2.</u>		
<u>3.</u>		

VII-1-12 String Object

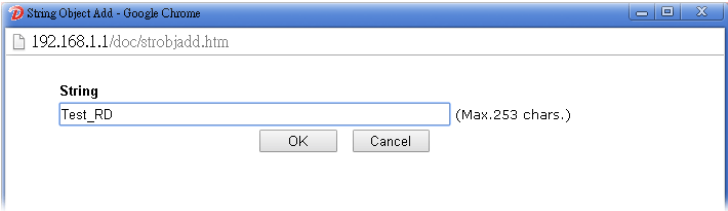
This page allows you to set string profiles which will be applied in route policy (domain name selection for destination) and etc.

Objects Setting >> String Object

10 ▼ strings per page | [Set to Factory Default](#) |

Index	String	<input type="button" value="Clear"/>
1	DrayTek Hotspot	<input type="checkbox"/>
2	Test_RD	<input type="checkbox"/>

Available settings are explained as follows:

Item	Description
Add	Click it to open the following page for adding a new string object. 
Set to Factory Default	Click it to clear all of the settings in this page.
Index	Display the number link of the string profile.
String	Display the string defined.
Clear	Choose the string that you want to remove. Then click this check box to delete the selected string.

Below shows an example to apply string object (in Route Policy):

Load-Balance/Route Policy

Index: 1

Enable

Comment

Criteria

Protocol

Source Any Src IP Range Src IP Subnet

Destination Any Dest IP Range Dest IP Subnet Domain Name

Destination Port Any Dest Port Start ~ Dest Port End

Send via if Criteria Matched

VII-1-13 Country Object

The country object profile can determine which country/countries shall be blocked by the Vigor router's Firewall.

Objects Setting >> Country Object

Country Object Table: | [Set to Factory Default](#) |

Index	Name	Index	Name
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

The country object, by grouping IP addresses for multiple countries, can be applied by other functions such as router policy destination (refer to the following figure for example).

Load-Balance/Route Policy

Index: 1

Enable

Comment

Criteria

Protocol

Source

Destination

Destination Port

Send via if Criteria Matched

To set a new profile, please do the steps listed below:

1. Open **Object Setting>>Country Object**, and click the number (e.g., #1) under Index column for configuration in details.

- The configuration page will be shown as follows:

Objects Setting >> Country Object

Profile Index : 1

Name:

Available Country		Selected Country
<div style="border: 1px solid gray; padding: 2px;"> 220-Taiwan 221-Tajikistan 222-Tanzania, United Republic of 223-Thailand 224-Timor-Leste 225-Togo 226-Tokelau 227-Tonga 228-Trinidad and Tobago </div>	<input type="button" value="»"/> <input type="button" value="«"/>	<div style="border: 1px solid gray; height: 100px;"></div>

Note:

The maximum number of Selected Country is 16.

Available settings are explained as follows:

Item	Description
Name	Type a name for such profile. The maximum length of the name you can set is 15 characters.
Countries	Check the box(es) for the country/countries to be blocked by Firewall. Note that one country profile can contain 1 up to 16 countries.

- After finishing all the settings here, please click **OK** to save the configuration.

Objects Setting >> Country Object

Country Object Table:

| [Set to Factory Default](#) |

Index	Name	Index	Name
<u>1.</u>	Taiwan	<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>	

Application Notes

A-1 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection

Follow the steps listed below:

1. Log into the web user interface of Vigor router.
2. Configure relational objects first. Open Object Settings>>SMS/Mail Server Object to get the following page.

Object Settings >> SMS / Mail Service Object

Index	Profile Name	SMS Provider
1.		kotsms.com.tw (TW)
2.		kotsms.com.tw (TW)
3.		kotsms.com.tw (TW)
4.		kotsms.com.tw (TW)
5.		kotsms.com.tw (TW)
6.		kotsms.com.tw (TW)
7.		kotsms.com.tw (TW)
8.		kotsms.com.tw (TW)
9.	Custom 1	
10.	Custom 2	

Index 1 to Index 8 allows you to choose the built-in SMS service provider. If the SMS service provider is not on the list, you can configure Index 9 and Index 10 to add the new service provider to Vigor router.

3. Choose any index number (e.g., Index 1 in this case) to configure the SMS Provider setting. In the following page, type the username and password and set the quota that the router can send the message out.

Object Settings >> SMS / Mail Service Object

Profile Index: 1

Profile Name	<input type="text" value="Local number"/>
Service Provider	<input type="text" value="kotsms.com.tw (TW)"/>
Username	<input type="text" value="abc5026"/>
Password	<input type="password" value="•••"/>
Quota	<input type="text" value="3"/>
Sending Interval	<input type="text" value="3"/> (seconds)

- After finished the settings, click OK to return to previous page. Now you have finished the configuration of the SMS Provider profile setting.

Object Settings >> SMS / Mail Service Object

SMS Provider		Mail Server	Set to Factory Default
Index	Profile Name	SMS Provider	
1.	Local number	kotsms.com.tw (TW)	
2.		kotsms.com.tw (TW)	
3.		kotsms.com.tw (TW)	
4.		kotsms.com.tw (TW)	
5.		kotsms.com.tw (TW)	
6.		kotsms.com.tw (TW)	
7.		kotsms.com.tw (TW)	
8.		kotsms.com.tw (TW)	
9.	Custom 1		
10.	Custom 2		

- Open Object Settings>>Notification Object to configure the event conditions of the notification.

Object Settings >> Notification Object

			Set to Factory Default
Index	Profile Name	Settings	
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			

- 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.

Objects Setting >> Notification Object

Profile Index: 1

Profile Name:

Category	Status	
WAN	<input checked="" type="checkbox"/> Disconnected	<input checked="" type="checkbox"/> Reconnected
VPN Tunnel	<input type="checkbox"/> Disconnected	<input type="checkbox"/> Reconnected
Temperature Alert	<input type="checkbox"/> Out of Range	
WAN Budget	<input type="checkbox"/> Limit Reached	
Central VPN Management	<input type="checkbox"/> CPE Offline <input type="checkbox"/> CPE Config Backup Fail <input type="checkbox"/> CPE Config Restore Fail <input type="checkbox"/> CPE Firmware Upgrade Fail <input type="checkbox"/> CPE VPN Profile Setup Fail	
High Availability	<input type="checkbox"/> Failover Occurred <input type="checkbox"/> Config Sync Fail <input type="checkbox"/> Router Unstable	

OK Clear Cancel

Note:

When High Availability is enabled, "Sending Interval" of **SMS Provider profile** should set to 0.

- After finished the settings, click **OK** to return to previous page. You have finished the configuration of the notification object profile setting.

Object Settings >> Notification Object

| [Set to Factory Default](#) |

Index	Profile Name	Settings
1.	WAN_Notify	WAN
2.		
3.		
4.		
5.		
6.		
7.		
8.		

- Now, open **Application >> SMS / Mail Alert Service**. Use the drop down list to choose SMS Provider and the Notify Profile (specify the time of sending SMS). Then, type the phone number in the field of Recipient (the one who will receive the SMS).

Applications >> SMS / Mail Alert Service

| [Set to Factory Default](#) |

SMS Alert		Mail Alert			
Index	SMS Provider	Recipient Number	Notify Profile	Schedule(1-15)	
1 <input checked="" type="checkbox"/>	1 - John	0910222356	1 - WAN_Notificatio		
2 <input type="checkbox"/>	1 - John		1 - WAN_Notificatio		
3 <input type="checkbox"/>	1 - John		1 - WAN_Notificatio		
4 <input type="checkbox"/>	1 - John		1 - WAN_Notificatio		
5 <input type="checkbox"/>	1 - John		1 - WAN_Notificatio		
6 <input type="checkbox"/>	1 - John		1 - WAN_Notificatio		
7 <input type="checkbox"/>	1 - John		1 - WAN_Notificatio		
8 <input type="checkbox"/>	1 - John		1 - WAN_Notificatio		
9 <input type="checkbox"/>	1 - John		1 - WAN_Notificatio		
10 <input type="checkbox"/>	1 - John		1 - WAN_Notificatio		

Note:

All the SMS Alert profiles share the same "Sending Interval" setting if they use the same SMS Provider.

- Click **OK** to save the settings. Later, if one of the WAN connections fails in your router, the system will send out SMS to the phone number specified. If the router has only one WAN interface, the system will send out SMS to the phone number while reconnecting the WAN interface successfully.

Remark: How the customize the SMS Provider

Choose one of the Index numbers (9 or 10) allowing you to customize the SMS Provider. In the web page, 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.

Objects Setting >> SMS / Mail Service Object

Profile Index: 9

Profile Name	<input type="text" value="Custom 1"/>
Service Provider	<input type="text" value="clickatell"/>
<div style="border: 1px solid black; height: 50px; width: 100%;"></div>	
Please contact with your SMS provide to get the exact URL String eg: bulksms.vsms.net:5567/eapi/submission/send_sms/2/2.0?username=###txtUser### &password=###txtPwd###&msisdn=###txtDest###&message=###txtMsg###	
Username	<input type="text" value="ilan123"/>
Password	<input type="password" value="*****"/>
Quota	<input type="text" value="10"/>
Sending Interval	<input type="text" value="3"/> (seconds)

Note:

1. Only one message can be sent during the "Sending Interval" time.
2. If the "Sending Interval" was set to 0, there will be no limitation.

VII-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

- SSL VPN
- USB Application**
- USB General Settings
- USB User Management
- File Explorer
- USB Device Status
- Temperature Sensor
- Modem Support List
- SMB Client Support List
- System Maintenance

VII-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 (Maximum 6)

Default Charset

SMB File Sharing Service (Network Neighborhood)

Enable Disable

Access Mode

LAN Only LAN And WAN

NetBios Name Service

Workgroup Name

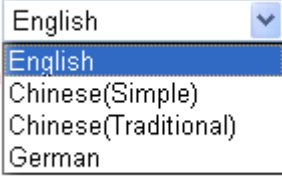
Host Name

Printer Server

Enable Disable

Available settings are explained as follows:

Item	Description
General Settings	<p>Simultaneous FTP Connections - This field is used to specify the quantity of the FTP sessions. The router allows up to 6 FTP sessions connecting to USB storage disk at one time.</p> <p>Default Charset - At present, Vigor router supports four types of character sets. Default Charset is for English based file name.</p>

	
SMB File Sharing Service	Click Enable to invoke SMB service (file sharing) via the router.
Access Mode	<p>LAN Only - Users coming from internet cannot connect to the SMB server of the router.</p> <p>LAN And WAN - Both LAN and WAN users can access SMB server of the router.</p>
NetBios Name Service	<p>For the NetBios service of USB storage disk, you have to specify a workgroup name and a host name. A workgroup name must not be the same as the host name. The workgroup name can have as many as 15 characters and the host name can have as many as 23 characters. Both them cannot contain any of the following--- ; : " < > * + = \ ?.</p> <p>Workgroup Name - Type a name for the workgroup.</p> <p>Host Name - Type the host name for the router.</p>
Printer Server	Enable - Click it to make Vigor router act as a printer server (with USB printer attached).

After finishing all the settings here, please click **OK** to save the configuration.

VII-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


USB User Management | [Set to Factory Default](#) |

Index	Username	Home Folder	Index	Username	Home Folder
1.			9.		
2.			10.		
3.			11.		
4.			12.		
5.			13.		
6.			14.		
7.			15.		
8.			16.		

Click index number to access into configuration page.

USB Application >> USB User Management


Profile Index: 1

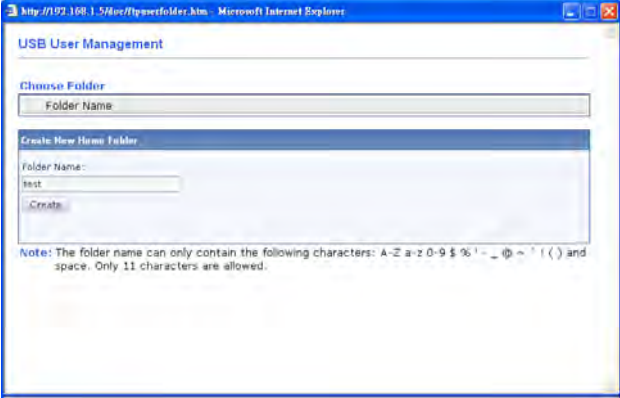
FTP/SMB User	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	<input type="text" value="Carrie"/>
Password	<input type="password" value="....."/> (Maximum 11 Characters)
Confirm Password	<input type="password" value="....."/>
Home Folder	<input type="text" value="/CA"/> 
Access Rule	
File	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Delete
Directory	<input checked="" type="checkbox"/> List <input checked="" type="checkbox"/> Create <input checked="" type="checkbox"/> Remove

Note:

The folder name can only contain the following characters: A-Z a-z 0-9 \$ % ' - _ @ ~ ` ! () and space.

Available settings are explained as follows:

Item	Description
FTP/SMB User	<p>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.</p> <p>Disable - Click this button to disable such profile.</p>
Username	<p>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.</p> <p>Note: "Admin" could not be typed here as username, for the word is specified for accessing into web pages of Vigor router only. Also, it is reserved for FTP firmware upgrade usage.</p> <p>Note: FTP Passive mode is not supported by Vigor Router. Please disable the mode on the FTP client.</p>
Password	<p>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.</p>
Confirm Password	<p>Type the password again to make confirmation.</p>
Home Folder	<p>It determines the folder for the client to access into. The user can enter a directory name in this field. Then, after clicking OK, the router will create the specific/new folder in the USB storage disk. In addition, if the user types "/" here, he/she can access into all of the disk folders and files in USB storage disk.</p> <p>Note: When write protect status for the USB storage disk is ON, you cannot type any new folder name in this field. Only "/" can be used in such case.</p> <p>You can click  to open the following dialog to add any new folder which can be specified as the Home Folder.</p>

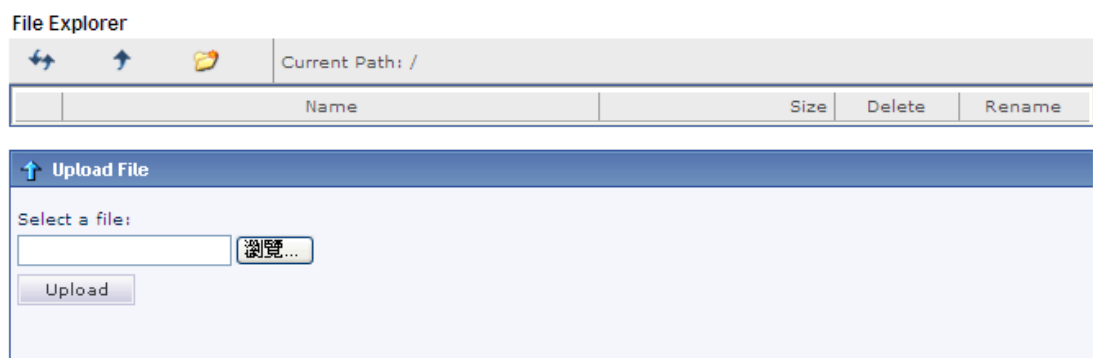
	
<p>Access Rule</p>	<p>It determines the authority for such profile. Any user, who uses such profile for accessing into USB storage disk, must follow the rule specified here.</p> <p>File - Check the items (Read, Write and Delete) for such profile.</p> <p>Directory -Check the items (List, Create and Remove) for such profile.</p>

Before you click OK, you have to insert a USB storage disk into the USB interface of the Vigor router. Otherwise, you cannot save the configuration.

VII-2-3 File Explorer




File Explorer offers an easy way for users to view and manage the content of USB storage disk connected on Vigor router.

USB Application >> File Explorer



Note: The folder can not be deleted when it is not empty.

Available settings are explained as follows:

Item	Description
 Refresh	Click this icon to refresh files list.
 Back	Click this icon to return to the upper directory.
 Create	Click this icon to add a new folder.
Current Path	Display current folder.

Upload	Click this button to upload the selected file to the USB storage disk. The uploaded file in the USB diskette can be shared for other user through FTP.
---------------	--

VII-2-4 USB Device Status

This page is to monitor the status for USB device connecting to Vigor router. . In addition, the status of the USB modem or USB printer or USB sensor connecting to Vigor router can be checked from such page. If you want to remove the storage disk from USB port in router, please click **Disconnect USB Disk** first. And then, remove the USB device later.

USB Application >> USB Device Status

Disk	Modem	Printer	Sensor	 Refresh
USB Mass Storage Device Status				
Connection Status: No Disk Connected				<input type="button" value="Disconnect USB Disk"/>
Disk Capacity: 0 MB				
Free Capacity: 0 MB Refresh				
USB Disk Users Connected				
Index	Service	IP Address(Port)	Username	

Note: If the write protect switch of USB disk is turned on, the USB disk is in **READ-ONLY** mode. No data can be written to it.

Available settings are explained as follows:

Item	Description
Connection Status	If there is no USB device connected to Vigor router, "No Disk Connected" will be shown here.
Disk Capacity	It displays the total capacity of the USB storage disk.
Free Capacity	It displays the free space of the USB storage disk. Click Refresh at any time to get new status for free capacity.
Index	It displays the number of the client which connects to FTP server.
IP Address	It displays the IP address of the user's host which connects to the FTP server.
Username	It displays the username that user uses to login to the FTP server.

When you insert USB device into the Vigor router, the system will start to find out such device within several seconds.

USB Application >> USB Device Status

Disk	Modem	Printer	Sensor	Refresh
USB Mass Storage Device Status				
Connection Status: Disk Connected				Disconnect USB Disk
Write Protect Status: No				
Disk Capacity: 2009 MB				
Free Capacity: 925 MB Refresh				
USB Disk Users Connected				
Index	Service	IP Address(Port)	Username	
Note: If the write protect switch of USB disk is turned on, the USB disk is in READ-ONLY mode. No data can be written to it.				

VII-2-5 Temperature Sensor

A USB Thermometer is now available. It complements your installed DrayTek router installations which will help you monitor the server or data communications room environment and notify you if the server room or data communications room is overheating.



During summer in particular, it is important to ensure that your server or data communications equipment are not overheating due to cooling system failures.

The inclusion of a USB thermometer in compatible Vigor routers will continuously monitor the temperature of its environment. When a pre-determined threshold is reached you will be alerted by either an email or SMS so you can undertake appropriate action.

Temperature Sensor Settings

USB Application >> Temperature Sensor Setting

Temperature Chart	Temperature Sensor Settings
Display Settings	
Temperature Calibration	<input type="text" value="0.00"/>
Temperature Unit	<input checked="" type="radio"/> Celsius <input type="radio"/> Fahrenheit
Alarm Settings	
<input type="checkbox"/> Enable Syslog Alarm	
Upper temperature limit	<input type="text" value="30.00"/>
Lower temperature limit	<input type="text" value="18.00"/>
<input type="button" value="OK"/>	

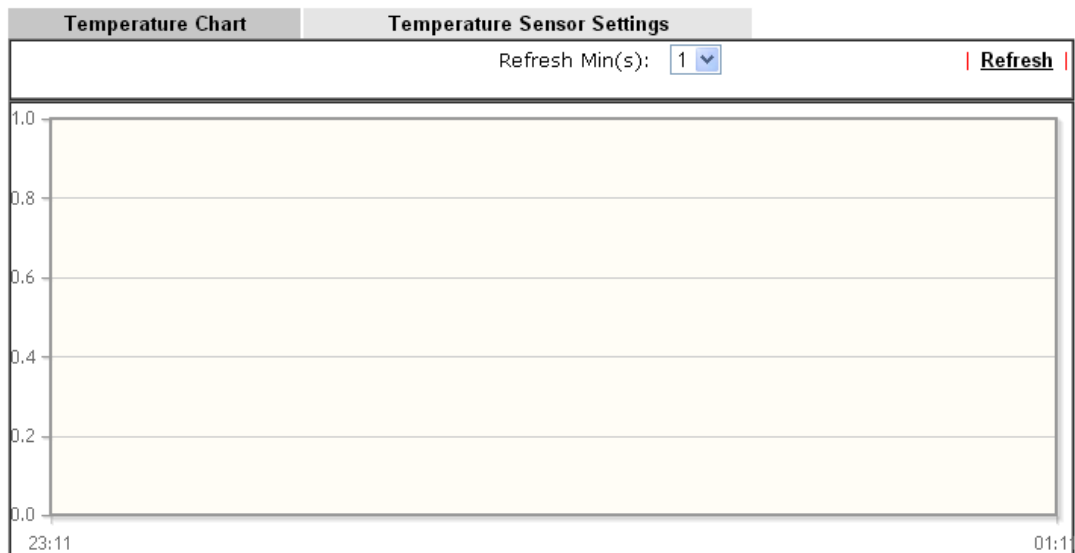
Available settings are explained as follows:

Item	Description
Display Settings	Temperature Calibration - Type a value used for correcting the temperature error. Temperature Unit - Choose the display unit of the temperature. There are two types for you to choose.
Alarm Settings	Enable Syslog Alarm - The temperature log will be recorded on Syslog if it is enabled. Upper temperature limit/Lower temperature limit - 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:

VII-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		Y
Alcatel	Alcatel L100V		Y
Alcatel	Alcatel W100		Y
BandRich	Bandlux C170		Y
BandRich	Bandlux C270		Y
BandRich	Bandlux C321		Y
BandRich	Bandlux C330		Y
BandRich	Bandlux C331		Y
BandRich	Bandlux C502		Y
D-Link	D_LINK DWM221 B1		Y
Huawei	Huawei E169u		Y
Huawei	Huawei E173u-2		Y
Huawei	Huawei E220		Y
Huawei	Huawei E303D		Y
Huawei	Huawei E3131		Y
Huawei	Huawei E3276s-151		Y

VII-2-7 SMB Client Support List

SMB Client Support List provides the test status information for applications with file sharing operated under different platforms.

USB Application >> SMB Client Support List



The following compatibility test lists suggested SMB clients supported by Vigor router.

Platform	Application	Status
Microsoft® Windows® XP	Built in	I
Microsoft® Windows Vista™	Built in	Y
Microsoft® Windows® 7	Built in	Y
Microsoft® Windows® 8	Built in	M
OS X® 10.7.5	Built in	Y
OS X® 10.10	Built in	Y
Android™	AndSMB	Y
Android™	ES File Explorer	Y
Android™	File Expert	Y
Android™	File Manager	Y
Android™	Solid Explorer	Y
Android™	SharesFinder	Y
iOS	eXPlayer	Y
iOS	nPlayer	Y

Y: Tested and is supported.

I: Supported but has some issue.

M: Has not been tested but might be supported.

Application Notes

A-1 How can I get the files from USB storage device connecting to Vigor router?

Files on USB storage device can be reviewed by opening **USB Application >> File Explorer**. If it is necessary for you to delete, copy files on the device or write, paste files to the device, it must be done through SMB server or FTP server.

SMB service is based on the original USB FTP service. You will need to setup USB FTP first. We would like to give brief instructions on USB FTP setup here.

1. Plug the USB device to the USB port on the router. Make sure **Disk Connected** appears on the **Connection Status** as the figure shown below:

USB Application >> USB Disk Status

USB Mass Storage Device Status

Connection Status: Disk Connected	Disconnect USB Disk		
Write Protect Status: No			
Disk Capacity: 2009 MB			
USB Disk Users Connected Refresh			
Index	Service	IP Address(Port)	Username

Note: If the write protect switch of USB disk is turned on, the USB disk is in READ-ONLY mode. No data can be written to it.

2. Then, please open **USB Application >> USB General Settings** to enable SMB service.

USB Application >> USB General Settings

USB General Settings

General Settings	
Simultaneous FTP Connections	<input type="text" value="5"/> (Maximum 6)
Default Charset	<input type="text" value="English"/>
SMB File Sharing Service (Network Neighborhood)	
<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Access Mode	
<input checked="" type="radio"/> LAN Only	<input type="radio"/> LAN And WAN
NetBios Name Service	
Workgroup Name	<input type="text" value="WORKGROUP"/>
Host Name	<input type="text" value="Vigor"/>

Note: 1. If character set is set to "English", only English long file name is supported.
2. Multi-session FTP download will be banned by Router FTP server. If your FTP client has a multi-connection mechanism, such as FileZilla, you should limit client connections to 1 to improve performance.
3. A workgroup name must be different from the host name. The workgroup name can have up to 15 characters and the host name can have up to 15 characters. Names cannot contain any of the following: . ; : " < > * + = / \ | ?.

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.

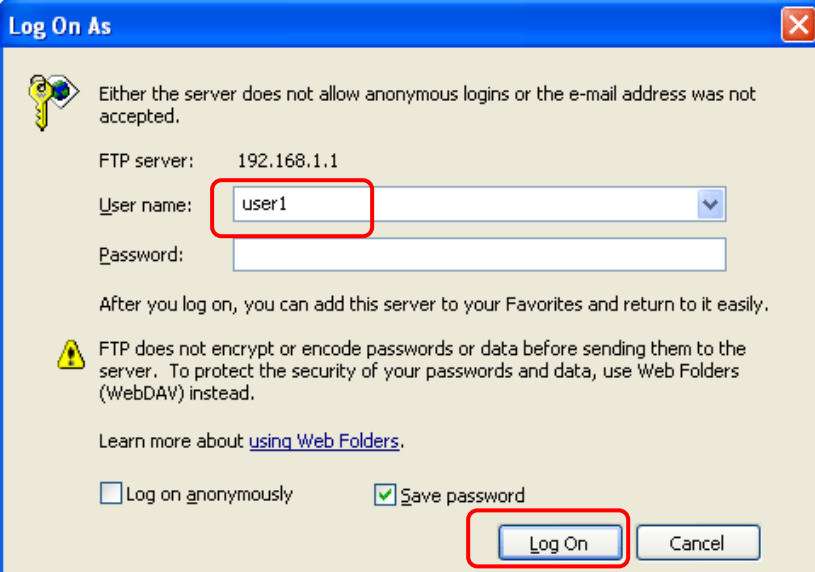
USB Application >> USB User Management

Profile Index: 1

FTP/SMB User	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	<input type="text" value="user1"/>
Password	<input type="password"/> (Maximum 11 Characters)
Confirm Password	<input type="password"/>
Home Folder	<input type="text"/> 
Access Rule	
File	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input type="checkbox"/> Delete
Directory	<input checked="" type="checkbox"/> List <input type="checkbox"/> Create <input type="checkbox"/> Remove

Note: The folder name can only contain the following characters: A-Z a-z 0-9 \$ % ' - _ @ ~ ` ! () and space.

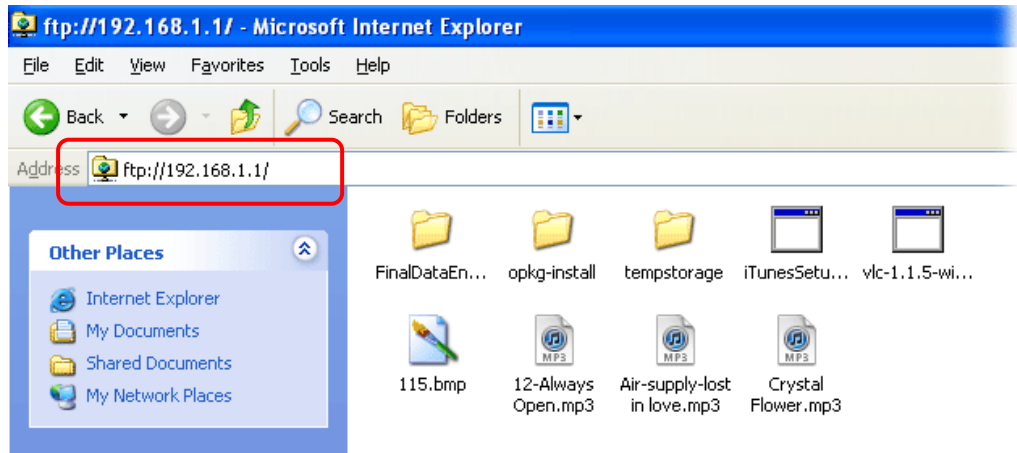
4. Click **OK** to save the configuration.
5. Make sure the FTP service is running properly. Please open a browser and type *ftp://192.168.1.1*. Use the account "user1" to login.



The image shows a Windows-style dialog box titled "Log On As". It contains the following elements:

- A key icon and a message: "Either the server does not allow anonymous logins or the e-mail address was not accepted."
- FTP server: 192.168.1.1
- User name: A dropdown menu with "user1" selected and highlighted by a red box.
- Password: An empty password field.
- A warning icon and message: "FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use Web Folders (WebDAV) instead." Below this is a link: "Learn more about [using Web Folders](#)."
- Checkboxes: "Log on anonymously" (unchecked) and "Save password" (checked).
- Buttons: "Log On" (highlighted by a red box) and "Cancel".

6. When the following screen appears, it means the FTP service is running properly.



7. Return to **USB Application >> USB Disk Status**. The information for FTP server will be shown as below.

USB Application >> USB Disk Status

USB Mass Storage Device Status

Connection Status: **Disk Connected** Disconnect USB Disk
 Write Protect Status: **No**
 Disk Capacity: 2009 MB

USB Disk Users Connected | Refresh |

Index	Service	IP Address(Port)	Username	
1.	FTP	192.168.1.10(1963)	user1	Drop

Now, users in LAN of Vigor2862 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 VIII Troubleshooting



Troubleshooting

This part will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration.

VIII-1 Diagnostics

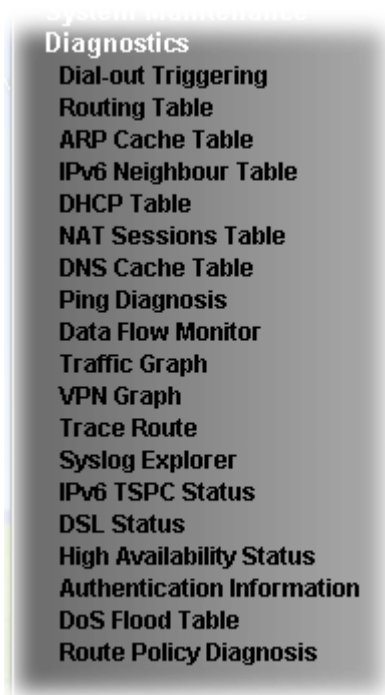
This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

If all above stages are done and the router still cannot run normally, it is the time for you to contact your dealer or DrayTek technical support for advanced help.

Web User Interface

First, take a look at the menu items under Diagnostics. Diagnostic Tools provide a useful way to view or diagnose the status of your Vigor router.



VIII-1-1 Dial-out Triggering

Click **Diagnostics** and click **Dial-out Triggering** to open the web page. The internet connection (e.g., PPPoE) is triggered by a package sending from the source IP address.

Diagnostics >> Dial-out Triggering

Dial-out Triggered Packet Header

| [Refresh](#) |

HEX Format:

```
00 00 00 00 00 00 00-00 00 00 00 00 00-00 00
```

```
00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
```

Decoded Format:

```
0.0.0.0 -> 0.0.0.0
Pr 0 len 0 (0)
```

Available settings are explained as follows:

Item	Description
Decoded Format	It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.

Refresh

Click it to reload the page.

VIII-1-2 Routing Table

Click Diagnostics and click Routing Table to open the web page.

Diagnostics >> View Routing Table

IPv4

| Refresh |

Key	Destination	Gateway	Interface
C~	192.168.1.0/ 255.255.255.0	directly connected	LAN1

Key

C: Connected S: Static R: RIP *: default ~: private

IPv6

| Refresh |

Destination	Interface	Flag	MTU	Metric
FE80::/64	LAN1	U	256	::
FE80::/64	LAN2	U	256	::
FE80::/64	LAN3	U	256	::
FE80::/64	LAN4	U	256	::
FE80::/64	LAN5	U	256	::
FE80::/64	LAN6	U	256	::
FE80::/64	DMZ	U	256	::
FF00::/8	LAN1	U	256	::
FF00::/8	LAN2	U	256	::
FF00::/8	LAN3	U	256	::
FF00::/8	LAN4	U	256	::
FF00::/8	LAN5	U	256	::
FF00::/8	LAN6	U	256	::
FF00::/8	DMZ	U	256	::

Show Detail

Flag

U: Route UP F: Default Route G: Use Next Hop S: Static Route R: RIPng

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

VIII-1-3 ARP Cache Table

Click **Diagnostics** and click **ARP Cache Table** to view the content of the ARP (Address Resolution Protocol) cache held in the router. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.

Diagnostics >> View ARP Cache Table

LAN
WAN

Show: ALL LANS and ALL VLANs

Ethernet ARP Cache Table | [Clear](#) | [Refresh](#) |

IP Address	MAC Address	Netbios Name	Interface	VLAN	Port
192.168.1.5	00-05-5D-	A1000351	LAN1	VLAN0	P1

Show Comment

Available settings are explained as follows:

Item	Description
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.

VIII-1-4 IPv6 Neighbour Table

The table shows a mapping between an Ethernet hardware address (MAC Address) and an IPv6 address. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **IPv6 Neighbour Table** to open the web page.

[Diagnostics >> View IPv6 Neighbour Table](#)

IPv6 Neighbour Table			Refresh
IPv6 Address	Mac Address	Interface	
FF02::2	33-33-00-00-00-02	LAN	
FF02::1:3	33-33-00-01-00-03	LAN	
FE80::3D5E:E74:8751:A44B	e8-9d-87-87-69-2f	LAN	
FF02::1:FF51:A44B	33-33-ff-51-a4-4b	LAN	
FE80::250:7FFF:FEC9:1E79	00-50-7f-c9-1e-79	LAN	
FE80::250:7FFF:FEC8:4305	00-50-7f-c8-43-05	LAN	
FF02::1	33-33-00-00-00-01	LAN	
FF02::1	00-00-00-00-00-00	USB2	
FF02::1:2	00-00-00-00-00-00	USB2	
FE80::9D5C:CA86:5428:3CA7	00-26-2d-fe-63-4f	LAN	
FF02::1:FF0A:673C	33-33-ff-0a-67-3c	LAN	

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

VIII-1-5 DHCP Table

The facility provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **DHCP Table** to open the web page.

Diagnostics >> View DHCP Assigned IP Addresses

Show : ALL LANs

DHCP IP Assignment Table		Other IP Assignment Table		Refresh	
LAN1 : DHCP Server On IP Pool: 192.168.1.10 ~ 192.168.1.209					
Index	IP Address	MAC Address	Leased Time	HOST ID	

LAN1					
1	192.168.1.10	00-50-7F-F1-05-FD	22:08:44		

Show Comment

DHCPv6 IP Assignment Table					Refresh
Index	IPv6 Address	IAID	Link-layer Address	Lease	

Available settings are explained as follows:

Item	Description
Index	It displays the connection item number.
IP Address	It displays the IP address assigned by this router for specified PC.
MAC Address	It displays the MAC address for the specified PC that DHCP assigned IP address for it.
Leased Time	It displays the leased time of the specified PC.
HOST ID	It displays the host ID name of the specified PC.
Refresh	Click it to reload the page.

VIII-1-6 NAT Sessions Table

Click **Diagnostics** and click **NAT Sessions Table** to open the list page.

[Diagnostics >> NAT Sessions Table](#)

NAT Active Sessions Table | [Refresh](#) |

Private IP :Port	#Pseudo Port	Peer IP :Port	Interface
192.168.1.11 2491	52078	24.9.93.189 443	WAN1
192.168.1.11 2493	52080	207.46.25.2 80	WAN1
192.168.1.10 3079	52665	207.46.5.10 80	WAN1

Available settings are explained as follows:

Item	Description
Private IP:Port	It indicates the source IP address and port of local PC.
#Pseudo Port	It indicates the temporary port of the router used for NAT.
Peer IP:Port	It indicates the destination IP address and port of remote host.
Interface	It displays the representing number for different interface.
Refresh	Click it to reload the page.

VIII-1-7 DNS Cache Table

Click **Diagnostics** and click **DNS Cache Table** to open the web page.

The record of domain Name and the mapping IP address for answering the DNS query from LAN will be stored on Vigor router's Cache temporarily and displayed on **Diagnostics >> DNS Cache Table**.

Diagnostics >> DNS Cache Table

IPv4 DNS Cache Table

| [Clear](#) | [Refresh](#) |

Domain Name	IP Address	TTL (s)

IPv6 DNS Cache Table

| [Clear](#) | [Refresh](#) |

Domain Name	IP Address	TTL (s)

Note:

The LAN DNS entry's TTL is static.

When an entry's TTL is larger than s, this entry will be deleted from the table.

OK

Available settings are explained as follows:

Item	Description
Clear	Click this link to remove the result on the window.
Refresh	Click it to reload the page.
When an entry's TTL is larger than....	Check the box the 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.

VIII-1-8 Ping Diagnosis

Click **Diagnostics** and click **Ping Diagnosis** to open the web page.

Diagnostics >> Ping Diagnosis

Ping Diagnosis

IPV4 IPV6

Note: If you want to ping a LAN PC or you don't want to specify which WAN to ping through, please select "Unspecified".

Ping through:

Ping to: IP Address:

Result | [Clear](#) |

or

Diagnostics >> Ping Diagnosis

Ping Diagnosis

IPV4 IPV6

Note: If you want to ping a LAN PC or you don't want to specify which WAN to ping through, please select "Unspecified".

Ping through:


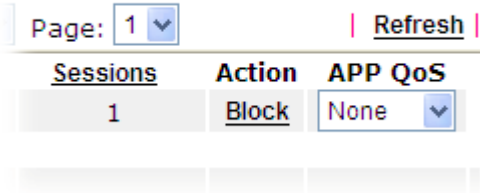
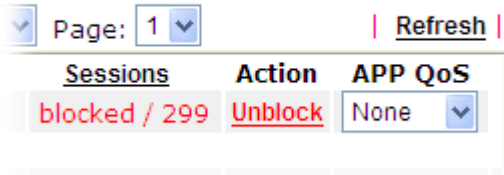
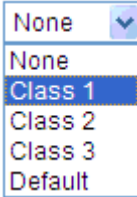
Ping IPv6 Addr:

Result | [Clear](#) |

Available settings are explained as follows:

Item	Description
IPV4 /IPV6	Choose the interface for such function.
Ping through	Use the drop down list to choose the WAN/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.

Available settings are explained as follows:

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: 
Refresh	Click this link to refresh this page manually.
Index	Display the number of the data flow.
IP Address	Display the IP address of the monitored device.
TX rate (kbps)	Display the transmission speed of the monitored device.
RX rate (kbps)	Display the receiving speed of the monitored device.
Sessions	Display the session number that you specified in Limit Session web page.
Action	<p>Block - can prevent specified PC accessing into Internet within 5 minutes.</p>  <p>Unblock -The device with the IP address will be blocked for five minutes. The remaining time will be shown on the session column. Click it to cancel the IP address blocking.</p> 
APP QoS	Use the drop down list to change the priority in data transmission for the specified IP address (host). 
Current /Peak/Speed	Current means current transmission rate and receiving rate for WAN interface. Peak means the highest peak value detected by the router in

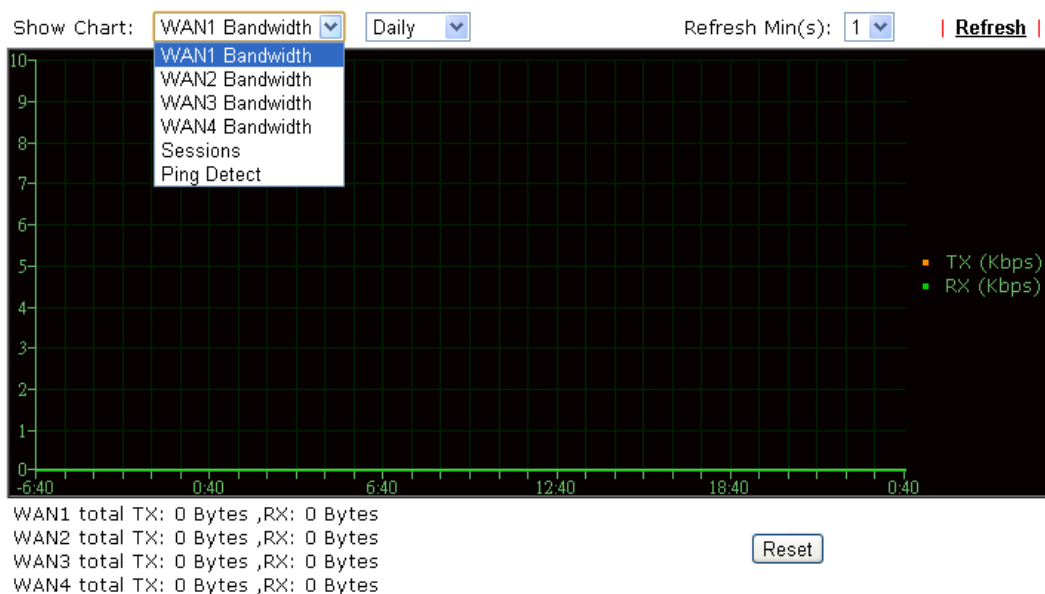
data transmission.

Speed means line speed specified in WAN>>General Setup. If you do not specify any rate at that page, here will display Auto for instead.

VIII-1-10 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to open the web page. Choose WAN1/WAN2/WAN3/WAN4 Bandwidth, Sessions, Ping Detect, 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



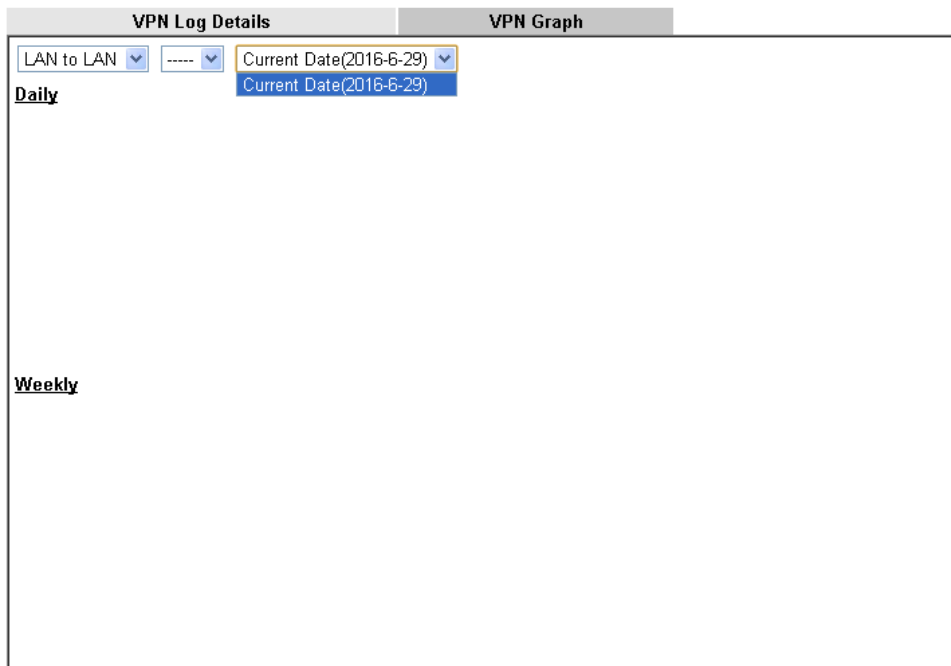
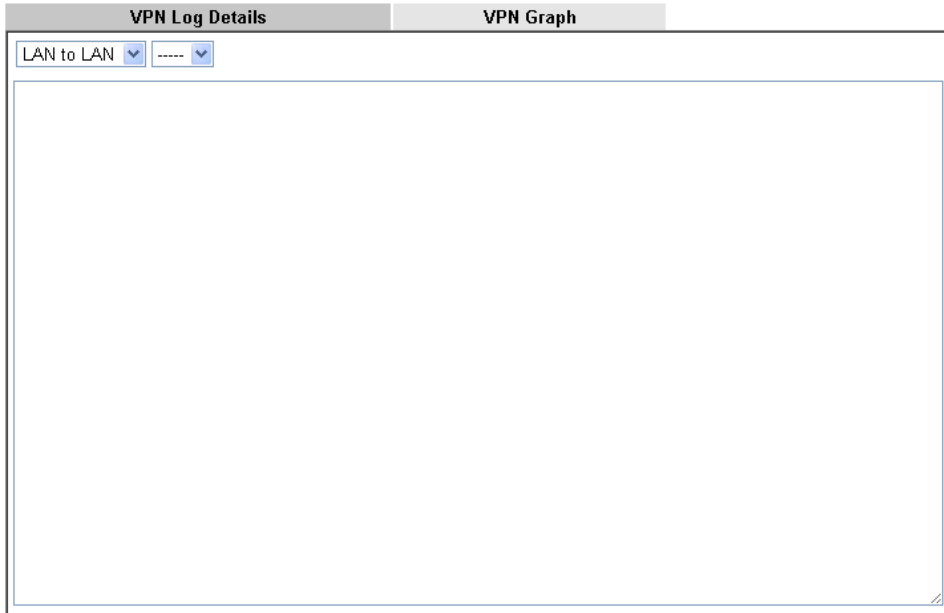
The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1/WAN2/WAN3/LTE/WAN4 Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

For Sessions chart, the numbers displayed on vertical axis represent the numbers of the NAT sessions during the past.

VIII-1-11 VPN Graph

Click **Diagnostics** and click **VPN Graph** to open the web page.

Diagnostics >> VPN Graph



VIII-1-12 Trace Route

Click **Diagnostics** and click **Trace Route** to open the web page. This page allows you to trace the routes from router to the host. Simply type the IP address of the host in the box and click **Run**. The result of route trace will be shown on the screen.

Diagnostics >> Trace Route

Trace Route

IPV4 IPV6

Trace through:

Protocol:

Host / IP Address:

Result | [Clear](#) |

or

Diagnostics >> Trace Route

Trace Route

IPV4 IPV6

Trace Host / IP Address:

Result | [Clear](#) |

Available settings are explained as follows:

Item	Description
IPv4 / IPv6	Click one of them to display corresponding information for it.
Trace through	Use the drop down list to choose the interface that you want to ping through.

Protocol	Use the drop down list to choose the protocol that you want to ping through.
Host/IP Address	It indicates the IP address of the host.
Trace Host/IP Address	It indicates the IPv6 address of the host.
Run	Click this button to start route tracing work.
Clear	Click this link to remove the result on the window.

VIII-1-13 Syslog Explorer


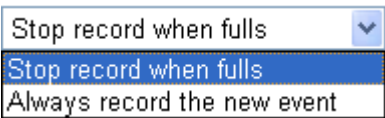
Such page provides real-time syslog and displays the information on the screen.

For Web Syslog

This page displays the time and message for User/Firewall/call/WAN/VPN settings. You can check **Enable Web Syslog**, specify the type of Syslog and choose the display mode you want. Later, the event of Syslog with specified type will be shown for your reference.

Diagnostics >> Syslog Explorer

Available settings are explained as follows:

Item	Description
Enable Web Syslog	Check this box to enable the function of Web Syslog.
Syslog Type	Use the drop down list to specify a type of Syslog to be displayed. 
Export	Click this link to save the data as a file.
Refresh	Click this link to refresh this page manually.
Clear	Click this link to clear information on this page.
Display Mode	There are two modes for you to choose.  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
------------	------------

Note: The syslog will show while the saved syslog file size is over 1MB.

Folder: n/a File: n/a Page: n/a Log Type: n/a

Time	Log Type	Message
------	----------	---------

Available settings are explained as follows:

Item	Description
Time	Display the time of the event occurred.
Log Type	Display the type of the record.
Message	Display the information for each event.

VIII-1-14 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 Status Local Endpoint v4 Address : 114.44.54.220 Local Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b9 Router DNS name : 88886666.broker.freenet6.net Remote Endpoint v4 Address : 81.171.72.11 Remote Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b8 Tspc Prefix : 2001:05c0:1502:0d00:0000:0000:0000:0000 Tspc Prefixlen : 56 Tunnel Broker : amsterdam.freenet6.net Tunnel Status : Connected				

Available settings are explained as follows:

Item	Description
Refresh	Click this link to refresh this page manually.

VIII-1-15 DSL Status

Such page is useful for RD debug or web technician.

Diagnostics >> DSL Status

General		Refresh		
ATU-R Information				
Type:	ADSL2/2+			
Hardware:	Annex A			
Firmware:	05-04-04-04-00-01			
Power Mngt Mode:	DSL_G997_PMS_NA			
Line State:	TRAINING			
Running Mode:				
Vendor ID:	b5004946 544e0000			
ATU-C Information				
Vendor ID:	00000000 00000000 [unknown]			
Line Statistics				
	Downstream		Upstream	
Actual Rate	0	Kbps	0	Kbps
Attainable Rate	0	Kbps	0	Kbps
Path Mode	Fast		Fast	
Interleave Depth	0		0	
Actual PSD	0.0	dB	0.0	dB
	Near End		Far End	
Trellis	ON		ON	
Bitswap	OFF		OFF	

VIII-1-16 High Availability Status

All of the routers under the same DARP (DrayTek Address resolution Protocol) group can be viewed in such page. However, only partial information of the router status will be displayed.

Vigor routers with the following conditions will be treated as the same DARP group:

- HA enabled
- the same Redundancy method
- the same Group ID
- the same Authentication Key
- the same Management Interface

Open [Diagnostics](#)>>[High Availability Status](#).

Diagnostics >> High Availability Status

								Details HA Setup Renew Refresh
Status	Router Name	IP	Role	Stable	WAN	Sync Status	Cached Time	
!	DrayTek	192.168.1.1	Primary	No	All WANs Down - Eth	Ready <input type="button" value="Sync"/>	-	

Note:

1. High Availability Status table displays 10 routers maximum. The local router will always show in the first row of this table.
2. A Status of "!" indicates that an error has occurred, refer to the [Details](#) page for more information.

Available settings are explained as follows:

Item	Description
Details/Back	Details - Click it to display detailed status about HA configuration for the selected router. Back - Return to previous page.
HA Setup	Click it to open Applications>>High Availability for modifying the configuration.
Renew	Click it to get the newest status of other router (except the primary router).
Refresh	Click it to get the newest status of the primary router.
Status	"!" means an error has occurred. Refer to Detailed information and modify HA settings if required.
Router Name	Display the name of the device.
IP	Display the IPv4 address of such router.
Role	"Down" means the function of HA is disabled. "Primary" means such router stands for the primary router in HA. "Secondary" means such router stands for the secondary router in HA.
Stable	"No" means the primary router has not been determined yet. DARP is negotiating. "YES" means the primary router is determined.
WAN	"At Least One UP" means that at least one WAN interface connects to Internet. "All WANs Down" means that no WAN interface connects to Internet.
Sync Status	"Not Ready" means configuration synchronization is unable to execute, or configuration synchronization is disabled, or synchronization initialization executes but fails. "Ready" means configuration synchronization is ready to execute. "Progressing" means configuration synchronization is operating. "Fail" means configuration synchronization executed and failed; or wrong model name. "Equal" means the corresponding settings are equal to the primary router.
Cached Time	Display the time period since the last time to get the newest status of other router (except the primary router).

Click the link of Router Name, IP or Details, the following page will be displayed on the screen.

Diagnostics >> High Availability Status >> Details

[Local Router]		Back HA Setup Renew Refresh		
DrayTek		192.168.1.1(FE80::21D:AAFF:FEF7:C0F0)		
Role	Stable	WAN	Sync Status	Cached Time
Primary	No !	All WANs Down - Eth !	Ready <input type="button" value="Sync"/>	-
Config Sync Status		Not Ready	DHCPv6 Sync Status	Ready
MAC		00:1d:aa:f7:c0:f0	HTTPs Port	443
Model		Vigor2862Vac	Firmware Version	3.8.5_RC5a
Enable High Availability		Off !	Redundancy Method	Active-Standby
Group ID		1	Priority ID	10
Authentication Key		draytek	Management Interface	LAN1
Update DDNS		Off	Protocol	IPv4
Virtual IPv4		Off !		
Virtual IPv6	On	LAN1	FE80::200:5EFF:FE00:101	
		LAN2	FE80::200:5EFF:FE00:101	
		LAN3	FE80::200:5EFF:FE00:101	
		LAN4	FE80::200:5EFF:FE00:101	
		LAN5	FE80::200:5EFF:FE00:101	
		LAN6	FE80::200:5EFF:FE00:101	
		LAN7	FE80::200:5EFF:FE00:101	
Enable Config Sync		Off	Config Sync Interval	0 Day 0 Hour 15 Minute

VIII-1-17 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 Information Log	
test_1	0	test_sales	0

Note:

- 1.This is the authentication list for router's **Internal RADIUS** 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

Authentication User List		Authentication Information Log	
<input type="checkbox"/> Enable			Refresh Clear
	Syslog Type	ALL	Display Mode
		ALL	always record the new event
		Radius	
		802.1X	
		ALL	
	Time		Message

Available settings are explained as follows:

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. <ul style="list-style-type: none">● 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 Vigor2862 series.
Message	Display authentication information done by Vigor2862 series.

VIII-1-18 DoS Flood Table

This page can display content of IP connection detected by DoS Flooding Defense mechanism. It is useful and convenient for network engineers (e.g., MIS engineer) to inspect the network environment to find out if there is any abnormal connection.

Information of IP traced and destination port used for SYN Flood, UDP Flood and ICMP Flood attacks will be detected and shown respectively on different pages.

Moreover, IP address detected and suspected to attack the network system can be blocked shortly by clicking the **Block** button shown on pages of SYN Flood, UDP Flood and ICMP Flood.

Diagnostics >> DoS Flood Table

IPv4

SYN Flood	UDP Flood	ICMP Flood	White/Black IP List	Refresh
Tracing IP		Destination Port		

192.168.1.22	80		<input type="button" value="Block"/>	
192.168.1.205	40005(⊗)		<input type="button" value="Block"/>	

IPv6

SYN Flood	UDP Flood	ICMP Flood	White/Black IP List	Refresh
Tracing IP		Destination Port		



Info

The icon - (⊗) - means there is something wrong (e.g., attacking the system) with that IP address.

However, if an IP address is confirmed to be blocked due to its abnormal behavior, click the **Blocking IP List** tab to block it forever. For example, IP address "192.168.1.99" (displayed on the following web page) will be blocked forever.

Diagnostics >> DoS Flood Table

IPv4

[SYN Flood](#) | [UDP Flood](#) | [ICMP Flood](#) | [White/Black IP List](#) | [Refresh](#)

White Passing IP List:

192.168.1.89

Add
Remove
Clear All

Black Blocking IP List:

192.168.1.99

Add
Remove
Clear All

IPv6

[SYN Flood](#) | [UDP Flood](#) | [ICMP Flood](#) | [White/Black IP List](#) | [Refresh](#)

Tracing IP	Destination Port
<div style="border-top: 1px dashed black; margin-top: 5px;"></div>	

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.

VIII-1-19 Route Policy Diagnosis

With the analysis done by such page, possible path (static route, routing table or policy route) of the packets sent out of the router can be traced.

Diagnostics >> Route Policy Diagnosis

Test how the packets will be routed

- Mode**
- Analyze a single packet
 - Analyze multiple packets by uploading an input file

Packet Information

Protocol

Src IP

Dst IP

Dst Port

Analyze

or

Diagnostics >> Route Policy Diagnosis

Test how the packets will be routed

- Mode**
- Analyze a single packet
 - Analyze multiple packets by uploading an input file

Input File

未選擇檔案

([download](#) an example input file)

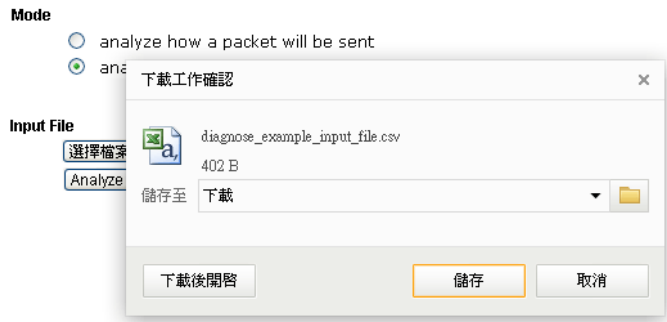
Analyze

Available settings are explained as follows:

Item	Description
Mode	<p>Analyze a single packet - Choose such mode to make Vigor router analyze how a single packet will be sent by a route policy.</p> <p>Analyze multiple packets... - Choose such mode to make Vigor router analyze how multiple packets in a specified file will be sent by a route policy.</p>
Packet Information	Specify the nature of the packets to be analyzed by Vigor router.

ICMP/UDP/TCP/ANY- Specify a protocol for diagnosis.
 Src IP - Type an IP address as the source IP.
 Dst IP - Type an IP address as the destination IP.
 Dst Port - Use the drop down list to specify the destination port.
 Analyze - Click it to perform the job of analyzing. The analyzed result will be shown on the page..

Input File
 It is available when Analyze multiple packets.. is selected as Mode.
 Select - Click the download link to get a blank example file.
 Then, click such button to select that blank ".csv" file for saving the result of analysis.



Analyze - Click it to perform the job of analyzing. The analyzed result will be shown on the page. If required, click export analysis to export the result as a file.

Load Balance/Route Policy >> Diagnose

Mode

analyze how a packet will be sent
 analyze how multiple packets as specified in the input file will be sent

Input File

[選擇檔案](#) [下載](#) (download an example input file)

Analysis

Profile	Input Packet Information			Matched Route		Matched Policy			Final Result	
	Proto	Src IP	Dst IP	Route	Priority	Policy	Priority	Label/Name	Interface	Reason
LA-branch	ICMP	192.168.1.10	10.10.10.10	No Match	N/A	No Match	N/A	N/A	N/A	The packet was dropped because neither "route" or "policy" was matched.
NY-branch	TCP	192.168.1.20	20.20.20.20	No Match	N/A	No Match	N/A	N/A	N/A	The packet was dropped because neither "route" or "policy" was matched.
										The packet was dropped because neither "route" or "policy" was matched.

Note that the analysis was based on the current "load-balance/route policy" settings, we do not guarantee it will be 100% the same as the real case.

VIII-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.

VIII-3 Checking If the Network Connection Settings on Your Computer Is OK or Not

Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is still failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows



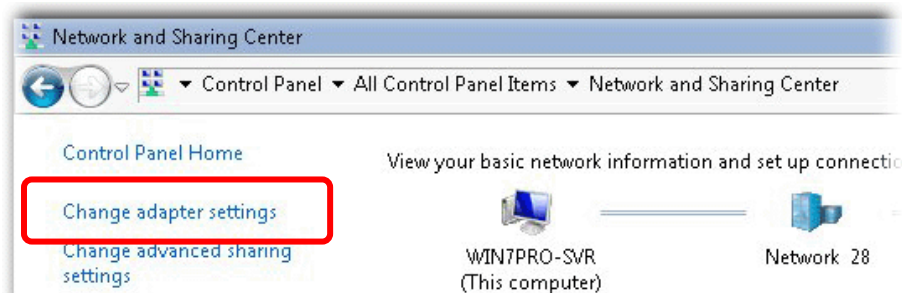
Info

The example is based on Windows 7. As to the examples for other operation systems, please refer to the similar steps or find support notes in www.DrayTek.com.

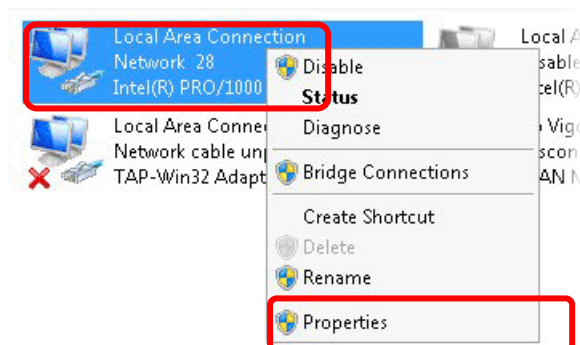
1. Open **All Programs>>Getting Started>>Control Panel**. Click **Network and Sharing Center**.



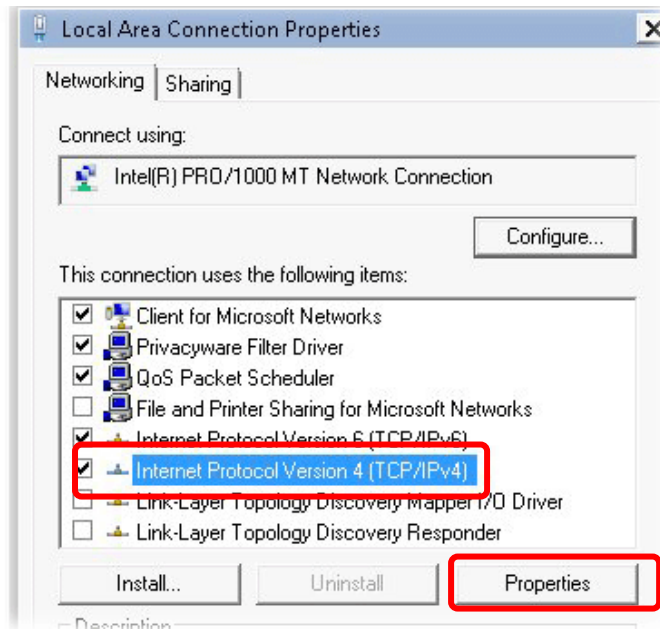
2. In the following window, click **Change adapter settings**.



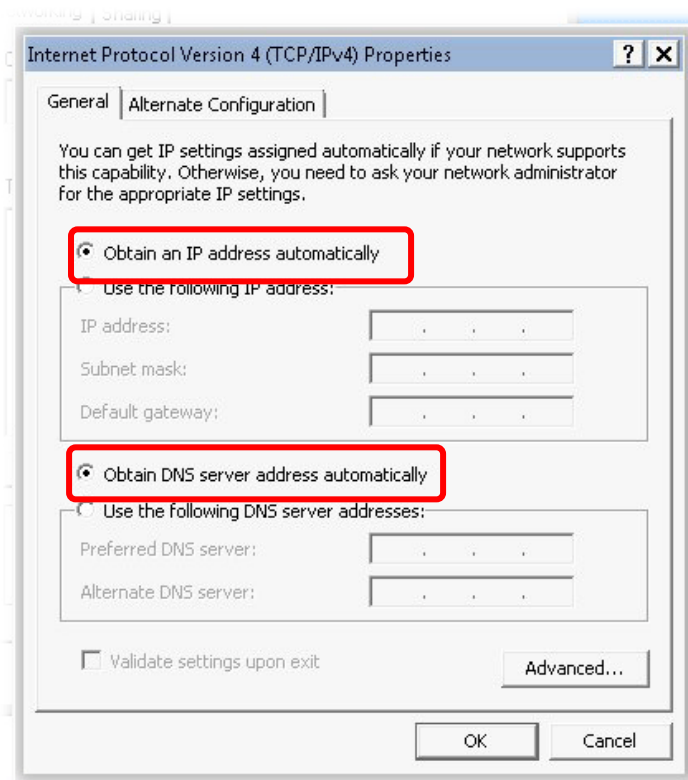
3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



4. Select **Internet Protocol Version 4 (TCP/IP)** and then click **Properties**.

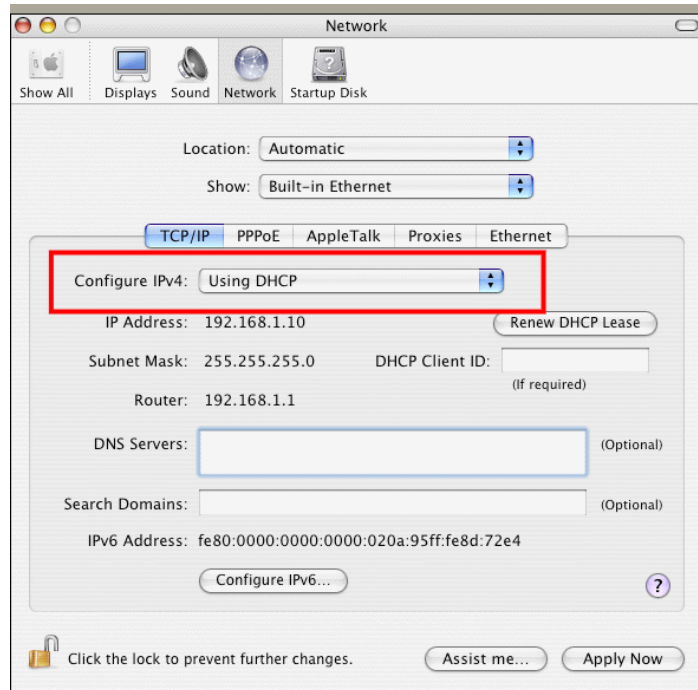


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



For Mac OS

1. Double click on the current used Mac OS on the desktop.
2. Open the **Application** folder and get into **Network**.
3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.



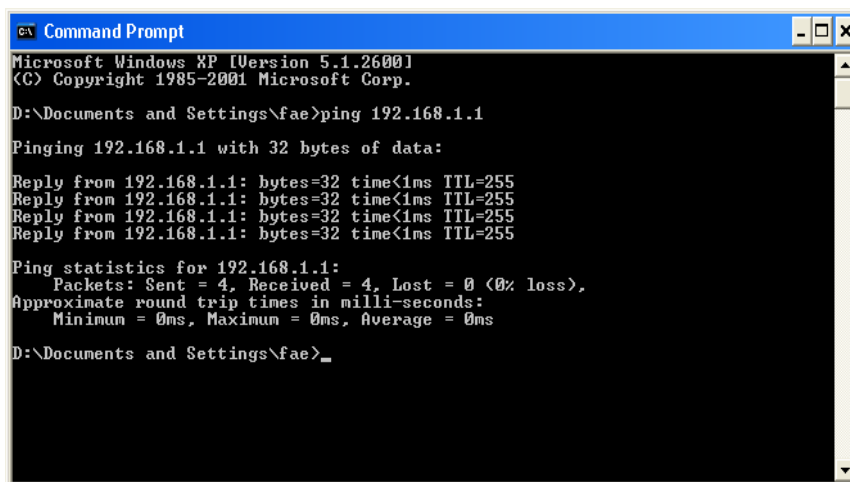
VIII-4 Pinging the Router from Your Computer

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.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fae>_
```

3. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of “Reply from 192.168.1.1:bytes=32 time<1ms TTL=255” will appear.
4. If the line does not appear, please check the IP address setting of your computer.

For Mac OS (Terminal)

1. Double click on the current used 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 ttys1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$ █
```

VIII-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.

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode
WAN1		ADSL / VDSL2	None Details Page IPv6
WAN2		Ethernet	Static or Dynamic IP Details Page IPv6
WAN3		USB	None Details Page IPv6
WAN4		USB	None Details Page IPv6

Note:
1. Device on USB port 1 applies WAN3 configuration.
2. Device on USB port 2 applies WAN4 configuration.

[Advanced](#) You can configure DHCP client options here.

VIII-6 Problems for 3G/4G Network Connection

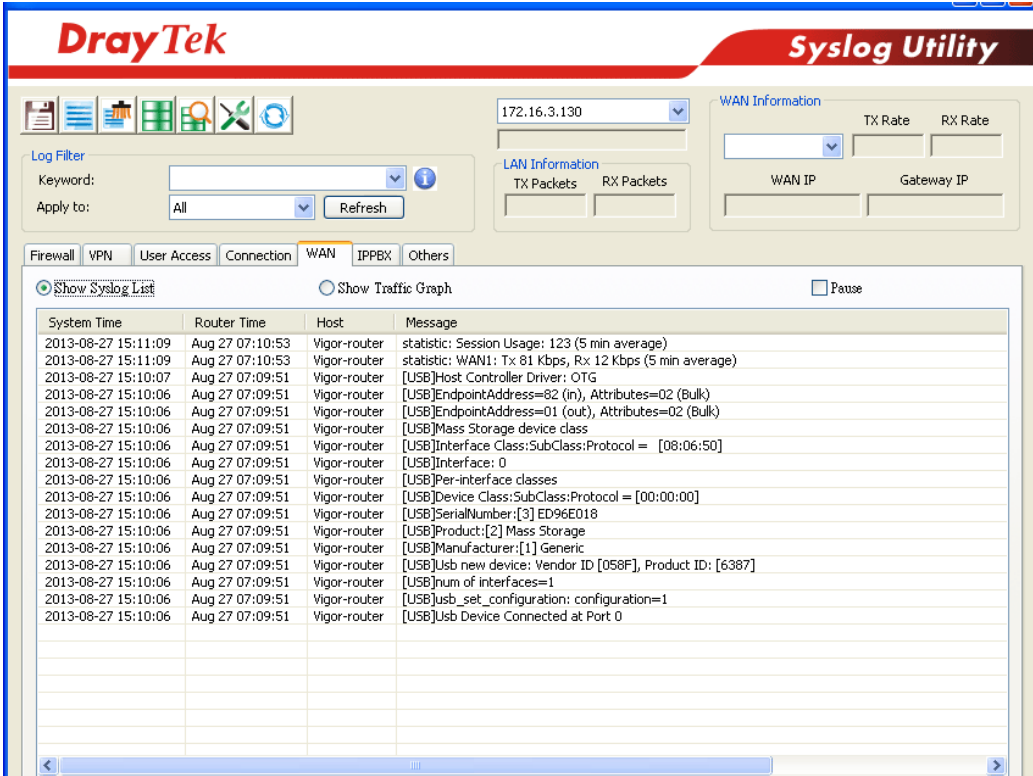
When you have trouble in using 3G/4G network transmission, please check the following:

Check if USB LED lights on or off

You have to wait about 15 seconds after inserting 3G/4G USB Modem into your Vigor2862. 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 Vigor2862.

USB LED lights on but the network connection does not work

Check the PIN Code of SIM card is disabled or not. Please use the utility of 3G/4G USB Modem to disable PIN code and try again. If it still fails, it might be the compliance problem of system. Please open DrayTek Syslog Tool to capture the connection information (WAN Log) and send the page (similar to the following graphic) to the service center of DrayTek.



The screenshot displays the DrayTek Syslog Utility web interface. At the top, the DrayTek logo and 'Syslog Utility' title are visible. Below the title bar, there are navigation icons and a 'Log Filter' section with a 'Keyword' input field and an 'Apply to' dropdown set to 'All'. A 'Refresh' button is also present. The main content area is divided into several sections: 'WAN Information' with fields for IP address (172.16.3.130), TX Rate, RX Rate, WAN IP, and Gateway IP; 'LAN Information' with TX Packets and RX Packets fields; and a 'Syslog List' table. The 'Syslog List' table has columns for System Time, Router Time, Host, and Message. The messages include statistics and USB device connection logs.

System Time	Router Time	Host	Message
2013-08-27 15:11:09	Aug 27 07:10:53	Vigor-router	statistic: Session Usage: 123 (5 min average)
2013-08-27 15:11:09	Aug 27 07:10:53	Vigor-router	statistic: WAN1: Tx 81 Kbps, Rx 12 Kbps (5 min average)
2013-08-27 15:10:07	Aug 27 07:09:51	Vigor-router	[USB]Host Controller Driver: OTG
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]EndpointAddress=82 (in), Attributes=02 (Bulk)
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]EndpointAddress=01 (out), Attributes=02 (Bulk)
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Mass Storage device class
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Interface Class:SubClass:Protocol = [08:06:50]
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Interface: 0
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Per-interface classes
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Device Class:SubClass:Protocol = [00:00:00]
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]SerialNumber:[3] ED96E018
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Product:[2] Mass Storage
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Manufacturer:[1] Generic
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]usb new device: Vendor ID [058F], Product ID: [6387]
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]num of interfaces=1
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]usb_set_configuration: configuration=1
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]usb Device Connected at Port 0

Transmission Rate is not fast enough

Please connect your Notebook with 3G/4G USB Modem to test the connection speed to verify if the problem is caused by Vigor2862. 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.

VIII-7 Backing to Factory Default Setting If Necessary

Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware. Such function is available in **Admin Mode** only.



Info

After pressing factory default setting, you will lose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null.

Software Reset

You can reset the router to factory default via Web page. Such function is available in **Admin Mode** only.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **Reboot Now**. After few seconds, the router will return all the settings to the factory settings.

System Maintenance >> Reboot System

Reboot System

Do you want to reboot your router ?

- Using current configuration
 Using factory default configuration

Reboot Now

Auto Reboot Time Schedule

Index(1-15) in Schedule Setup: , , ,

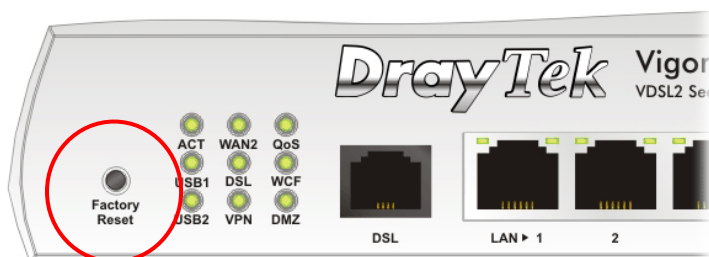
Note: Action and Idle Timeout settings will be ignored.

OK

Cancel

Hardware Reset

While the router is running (ACT LED blinking), press the **Factory Reset** button and hold for more than 5 seconds. When you see the ACT LED blinks rapidly, please release the button. Then, the router will restart with the default configuration.



After restore the factory default setting, you can configure the settings for the router again to fit your personal request.

VIII-8 Contacting DrayTek

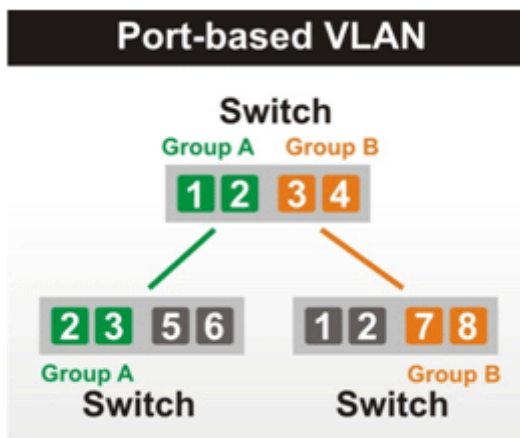
If the router still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@DrayTek.com.

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:

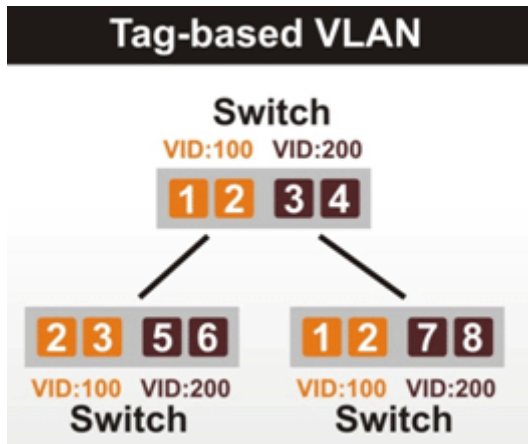
Port-based

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.

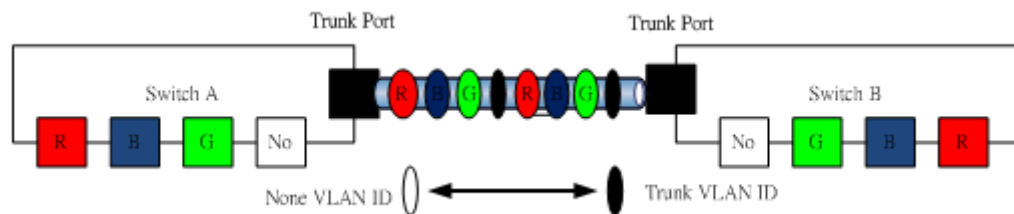
[Note]

Broadband router: Vigor2920/Vigor3200/Vigor2925/Vigo2960/Vigor3900

Modem router: Vigor2850/Vigor2862

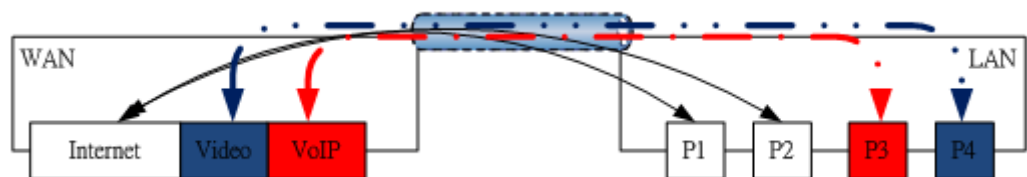
VLAN Packets on Vigor routers

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

Multi-VLAN

General				
Channel	Enable	WAN Type	VLAN Tag	Port-based Bridge
1	Yes	Ethernet(WAN1)	None	
2	Yes	Ethernet(WAN2)	None	
3	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
4	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
5_WAN5	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
6_WAN6	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
7_WAN7	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
8	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5

Detail settings of channel profile

VLAN Settings

VLAN Members

Service Binding & WAN Setup

Multi-VLAN Channel 5: Enable Disable
 WAN Type :

General Settings
 VLAN Header
 VLAN Tag:
 Priority:
 Note:1.Tag value must be set between 1~4095 and unique for each channel.
 2.Only one channel can be untagged (equal to 0) at a time.

Open Port-based Bridge Connection for this Channel
 Physical Members
 P1 P2 P3 P4 P5
 Note:3.P1 is reserved for NAT use,and cannot be configured for bridge mode.

Open WAN Interface for this Channel
 WAN for Router-borne Application:
 WAN Setup:

<p>ISP Access Setup</p> <p>ISP Name <input type="text"/></p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>PPP Authentication <input type="text" value="PAP or CHAP"/></p> <p><input checked="" type="checkbox"/> Always On</p> <p>Idle Timeout <input type="text" value="-1"/> second(s)</p> <p>IP Address From ISP</p> <p>Fixed IP <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP)</p> <p>Fixed IP Address <input type="text"/></p>	<p>WAN IP Network Settings</p> <p><input type="radio"/> Obtain an IP address automatically</p> <p>Router Name <input type="text" value="Vigor"/> *</p> <p>Domain Name <input type="text"/> *</p> <p>*: Required for some ISPs</p> <p><input checked="" type="radio"/> Specify an IP address</p> <p>IP Address <input type="text"/></p> <p>Subnet Mask <input type="text"/></p> <p>Gateway IP Address <input type="text"/></p> <p>DNS Server IP Address</p> <p>Primary IP Address <input type="text" value="8.8.8.8"/></p> <p>Secondary IP Address <input type="text" value="8.8.4.4"/></p>
---	--

LAN

Enable *Port-based VLAN* by checking the option

The option of *Tag-based VLAN*

VLAN Configuration

Enable

VLAN	LAN				Wireless LAN				Subnet	VLAN Tag		
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4		Enable	VID	Priority
VLAN0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0

VLAN Group

Member of *Port-based* or *Tag-based* VLAN

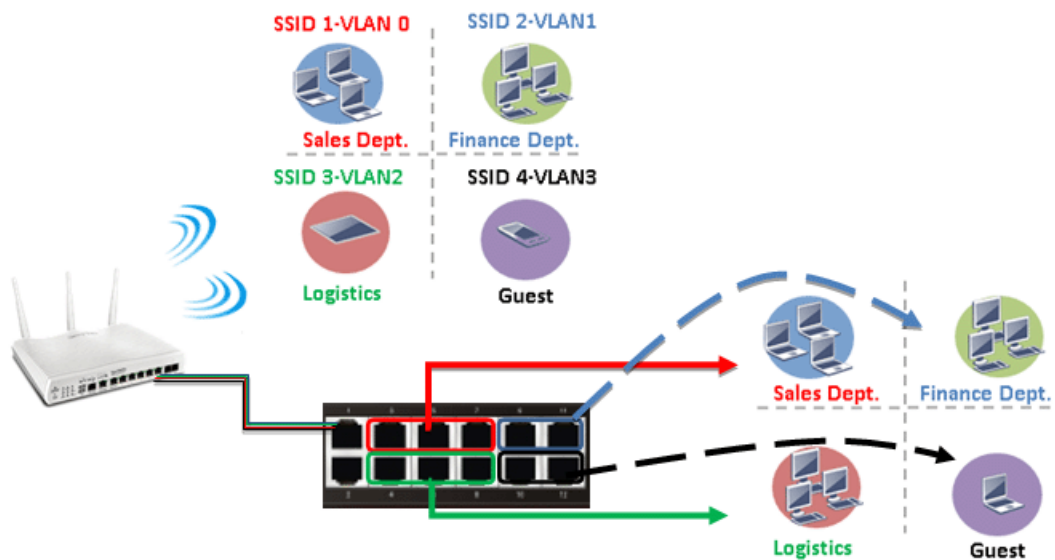
DHCP Pool will be used

VLAN ID assigned

802.1p field

VLAN applications on Vigor router

- Multi Subnet (VLAN of LAN)



Port-based mode

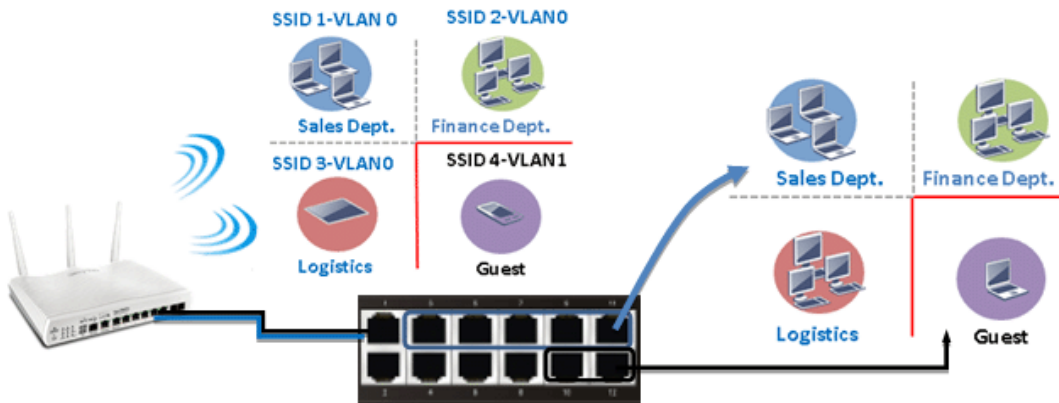
	LAN				Wireless LAN				VLAN Tag			
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
VLAN0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 2	<input type="checkbox"/>	0	0
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	LAN 3	<input type="checkbox"/>	0	0
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	LAN 4	<input type="checkbox"/>	0	0
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0

Tag-based mode

	LAN				Wireless LAN				VLAN Tag			
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
VLAN0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input checked="" type="checkbox"/>	10	0
VLAN1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 2	<input checked="" type="checkbox"/>	20	0
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	LAN 3	<input checked="" type="checkbox"/>	30	0
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	LAN 4	<input checked="" type="checkbox"/>	40	0
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0

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

Enable

	LAN				Wireless LAN				VLAN Tag			
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
VLAN0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	LAN 2	<input type="checkbox"/>	0	0
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0

Tag-based mode

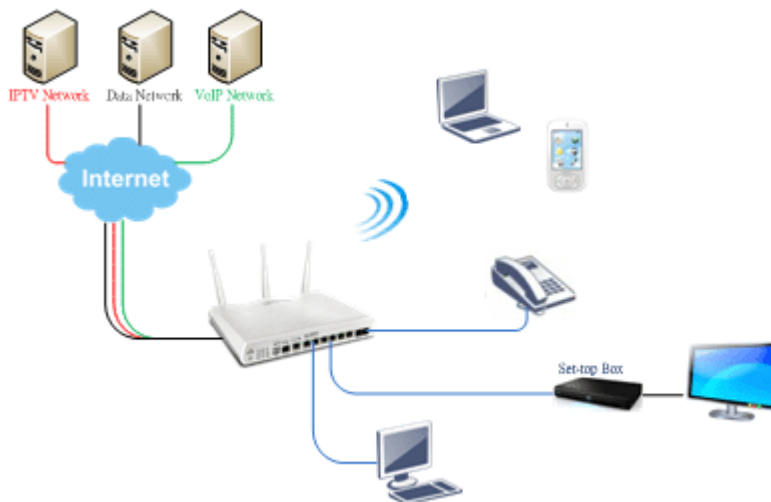
Enable

	LAN				Wireless LAN				VLAN Tag			
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
VLAN0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	LAN 2	<input checked="" type="checkbox"/>	10	0
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0

To deploy a guest network, which serves your guests the internet accessibility, but the traffics have to be isolated from your private network due to the security considerations, it can be done by above settings. However, a switch support VLAN function is need if VLAN Tag enabled.

- Triple Play (Multi-WAN)

NAT mode with VLAN



Following settings, the set-top box (STB) is able to attach with any LAN port. Video streaming which your ISP provided will be played on your monitor.

WAN 1

Enable: Yes No

Display Name:

Physical Mode: Ethernet

Physical Type: Auto negotiation

Line Speed(Kbps):

DownLink:

UpLink:

VLAN Tag insertion: Enable Disable (Please configure Internet Access setting first)

Tag value: (0~4095)

Priority: (0~7)

Active Mode: Always On Load Balance:

1. Setup the VLAN ID on WAN1 profiles if WAN is the primary interface of IPTV service.

2. Open the profile of WAN5 by clicking the ID.

Channel	Enable	WAN Type	VLAN Tag	Port-based Bridge
1	Yes	Ethernet(WAN1)	None	
2	Yes	Ethernet(WAN2)	None	
3	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
4	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
5. WAN5	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
6. WAN6	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
7. WAN7	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
8	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4

Multi-VLAN Channel 5: Enable Disable

WAN Type: Ethernet(WAN1)

General Settings

VLAN Header

VLAN Tag:

Priority:

Note: 1. Tag value must be set between 1~4095 and unique for each channel.
2. Only one channel can be untagged (equal to 0):

P1 P2 P3 P4 P5

Note: 3. P1 is reserved for NAT use, and cannot be configured for bridge mode.

Open Port-based Bridge Connection for this Channel

Physical Members: P1 P2 P3 P4 P5

Note: 3. P1 is reserved for NAT use, and cannot be configured for bridge mode.

3. Setup connection of WAN 5 and bind the service onto it.

NO need to enable Port-based Bridge.

P1 P2 P3 P4 P5

Note: 3. P1 is reserved for NAT use, and cannot be configured for bridge mode.

Open WAN interface for this Channel

WAN for Router-borne Application: IPTV

WAN Setup: Static or Dynamic IP

ISP Access Setup

ISP Name:

Username:

Password:

PPP Authentication: PAP or CHAP

Always On

Idle Timeout: second(s)

IP Address From ISP

Fixed IP (Dynamic IP): Yes No

Fixed IP Address:

WAN IP Network Settings

Obtain an IP address automatically

Router Name: Vigor

Domain Name:

*: Required for some ISPs

Specify an IP address

IP Address:

Subnet:

Mask:

Gateway IP Address:

DNS Server IP Address

Primary IP Address: 8.8.8.8

Secondary IP Address: 8.8.4.4

4. Go to Application >> IGMP to bind it on PVC WAN.

IGMP

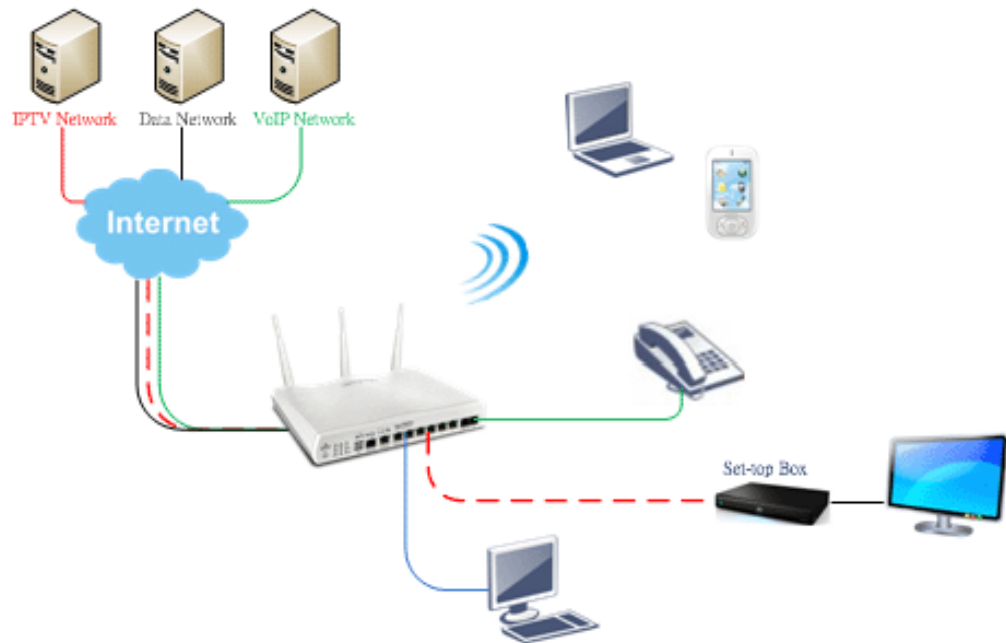
Enable IGMP Proxy PVC

IGMP Proxy is to act as a multicast proxy for will access any multicast group. But this function take no effect when bridge mode is enable.

Enable IGMP Snooping

Enable IGMP Snooping, multicast traffic is only forwarded to ports that have members of that group. Disable IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic.

Bridge mode with VLAN



Multi-VLAN

General				
Channel	Enable	WAN Type	VLAN Tag	Port-based Bridge
1	Yes	Ethernet(WAN1)	None	
2	Yes	Ethernet(WAN2)	None	
3	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
4	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
5	WAN5	No		
6	WAN6	No		
7	WAN7	No		
8	WAN8	No		

Multi-VLAN Channel 3: Enable Disable

WAN Type :

General Settings

VLAN Header

VLAN Tag:

Priority:

Note:1.Tag value must be set between 1~4095 and unique for each channel.
2.Only one channel can be untagged (equal to 0) at a time.

Bridge mode

Enable

Physical Members

P1 P2 P3 P4 P5

Note:3.P1 is reserved for NAT use,and cannot be configured for bridge mode.

Set-top box (STB) or the other kinds of media devices are able to attach with Port4 or Port5 of LAN. Those devices that attached with Port4 or Port5 are able to access the services network directly which your ISP provided.

This page is left blank.

Part IX Telnet Commands

Accessing Telnet of Vigor2862

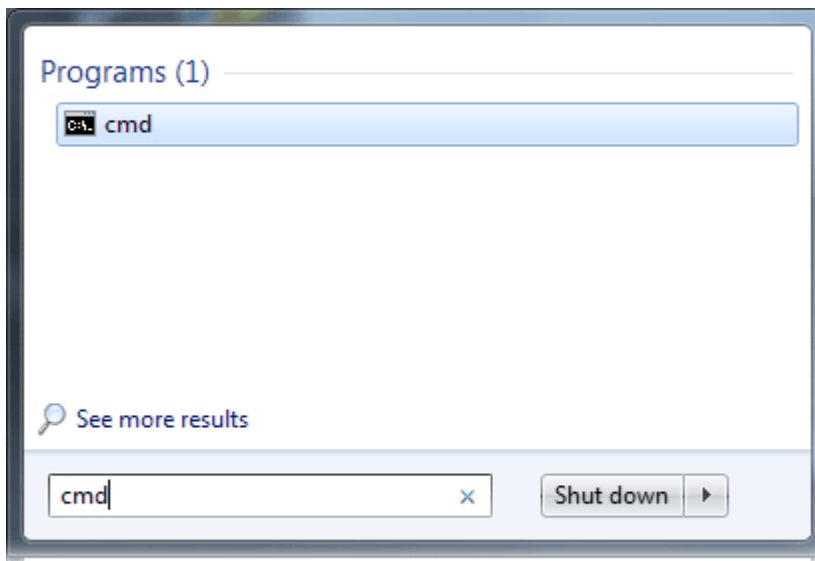
This chapter also gives you a general description for accessing telnet and describes the firmware versions for the routers explained in this manual.



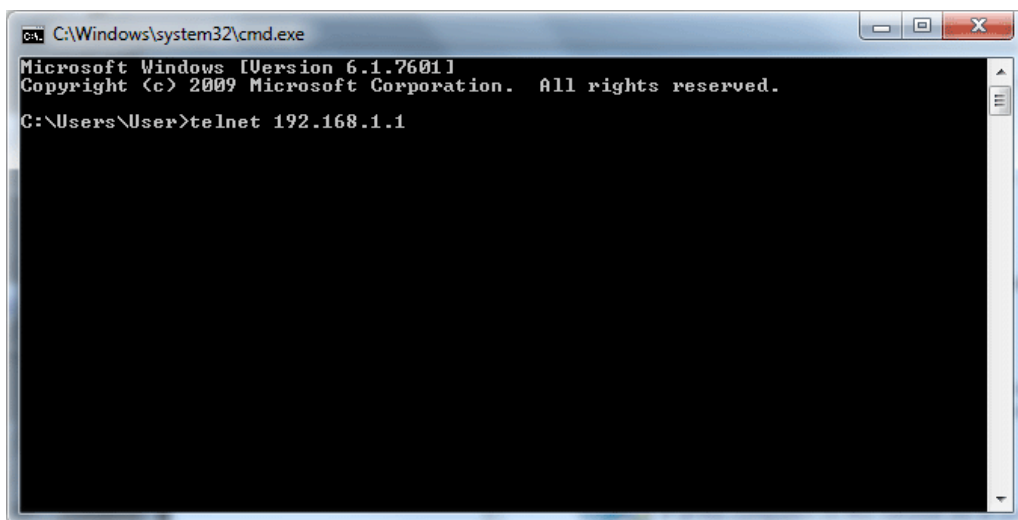
Info

For Windows 7 user, please make sure the Windows Features of Telnet Client has been turned on under Control Panel>>Programs.

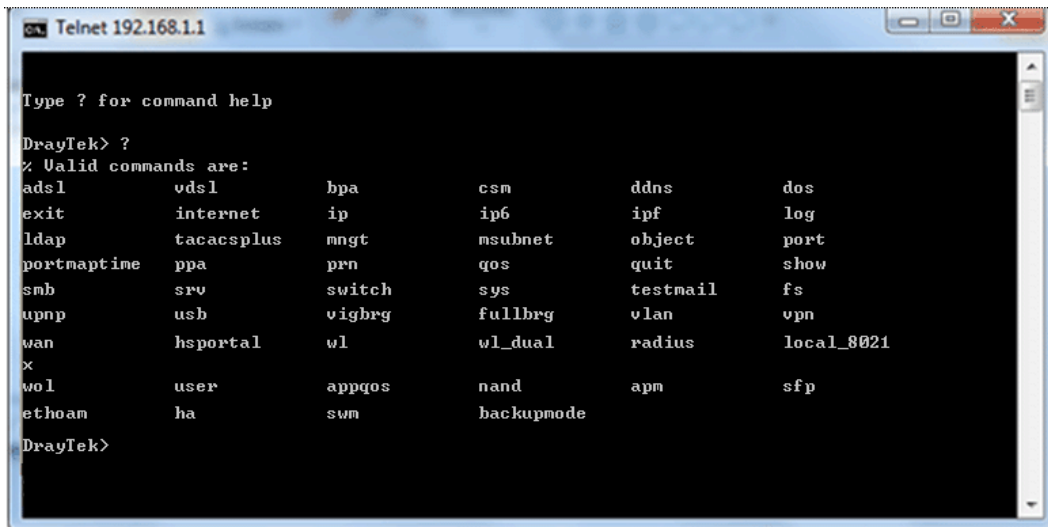
Type cmd and press Enter. The Telnet terminal will be open later.



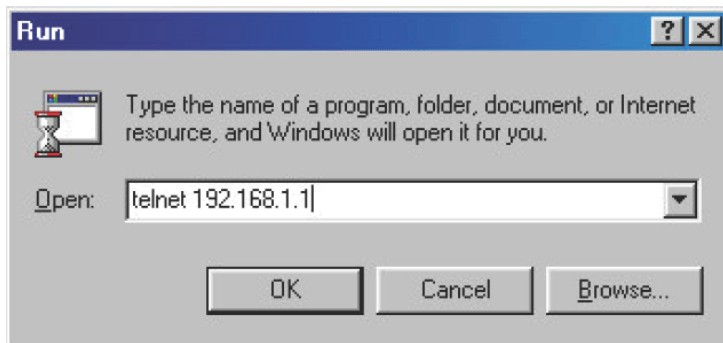
In the following window, type Telnet 192.168.1.1 as below and press Enter. Note that the IP address in the example is the default address of the router. If you have changed the default, enter the current IP address of the router.



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

```
> adsl status
----- ATU-R Info (hw: annex A, f/w: annex Unknown) -----
Running Mode           : T1.413      State           : TRAINING
DS Actual Rate         : 0 bps    US Actual Rate   : 0 bps
DS Attainable Rate     : 0 bps    US Attainable Rate: 0 bps
DS Path Mode          : Fast      US Path Mode     : Fast
DS Interleave Depth    : 0        US Interleave Depth: 0
NE Current Attenuation : 0 dB    Cur SNR Margin   : 0 dB
DS actual PSD          : 0.0 dB    US actual PSD    : 0.0 dB
ADSL Firmware Version  : 05-04-08-00-00-06
----- ATU-C Info -----
Far Current Attenuation : 0 dB    Far SNR Margin   : 0 dB
CO ITU Version[0]      : 00000000    CO ITU Version[1] : 00000000
DSLAM CHIPSET VENDOR   : < ADI >
>
```

Telnet Command: adsl ppp

This command can set the Internet Access mode for the router.

Syntax

`adsl ppp [? | pvc_no vci vpi Encap Proto modu acqIP idle [Username Password]`

Syntax Description

Parameter	Description
?	Display the command syntax of "adsl ppp".
pvc_no	It means the PVC number and the adjustable range is from 0 (Channel-1) to 7(Channel-8).
Encap	Different numbers represent different modes. 0 : VC_MUX, 1: LLC/SNAP, 2: LLC_Bridge, 3: LLC_Route, 4: VCMUX_Bridge 5: VCMUX_Route, 6: IPoE.
Proto	It means the protocol used to connect Internet. Different numbers represent different protocols. 0: PPPoA, 1: PPPoE, 2: MPoA.
Modu	0: T1.413, 2: G.dmt, 4: Multi, 5: ADSL2, 7:ADSL2_AnnexM 8:ADSL2+ 14:ADSL2+_AnnexM.
acqIP	It means the way to acquire IP address. 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.

Example

```
> adsl ppp o 35 8 1 1 4 1 -1 draytek draytek
pvc no.=0
vci=35
vpi=8
encap=LLC(1)
proto=PPPoE(1)
modu=MULTI(4)
```

```
AcquireIP: Dhcp_client(1)
Idle timeout:-1
Username=draytek
Password=draytek
```

Telnet Command: adsl bridge

This command can specify a LAN port (LAN1 to LAN4) for mapping to certain PVC, and the mapping port/PVC will be operated in bridge mode.

Syntax

```
adsl bridge [pvc_no/status/save/enable/disable] [on/off/clear/tag tag_no] [service type]
[px ... ]
```

Syntax Description

Parameter	Description
<i>pvc_no</i>	It means <i>pvc</i> number and must be between 0(Channel 1) to 7(Channel 8).
<i>status</i>	It means to shown the whole bridge status.
<i>save</i>	It means to save the configuration to flash.
<i>enable</i>	It means to enable the Multi-VLAN function.
<i>disable</i>	It means to disable the Multi-VLAN function.
<i>on/off</i>	It means to turn on/off bridge mode for the specific channel.
<i>clear</i>	It means to turn off and clear all the PVC settings.
<i>tag tag_no</i>	No tag: -1 Available number for tag: 0-4095
<i>pri pri_no</i>	The number 0 to 7 can be set to indicate the priority. "7" is the highest.
<i>service type</i>	Two number can be set: 0: for Normal (all the applications will be processed with the same PVC). 1: for the IGMP with different PVC which is used for special ISP.
<i>px...</i>	It means the number of LAN port (x=2~4). Port 1 is locked for NAT.

Example

```
> adsl bridge 4 on p2 p3
PVC Bridge   p1   p2   p3   p4   Service Type   Tag   Pri
-----
   4   ON     0   0   1   0     Normal   -1(OFF)  0
PVC 0 & 1 can't set for bridge mode.
Please use 'save' to save config.
```

Telnet Command: adsl 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
<code>on</code>	DSL is under test mode. DSL debug tool mode is off.
<code>tcpmessage</code>	DSL debug tool mode is on.
<code>tcpmessage_off</code>	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.

Example

```
> adsl reboot
% Adsl is Rebooting...
```

Telnet Command: adsl oamlb

This command is used to test if the connection between CPE and CO is OK or not.

Syntax

```
adsl oamlb [n][type]
```

```
adsl oamlb chklink [on/off]
```

```
adsl oamlb [log_on/log_off]
```

Syntax Description

Parameter	Description
<i>n</i>	It means the total number of transmitted packets.
<i>type</i>	It means the protocol that you can use. 1 - for F4 Seg-to-Seg (VP level) 2 - for F4 End-to-End (VP level) 4 - for F5 Seg-to-Seg (VC level) 5 - for F5 End-to-End (VC level)
<i>chklink</i>	Check the DSL connection.
<i>Log_on/log_off</i>	Enable or disable the OAM log for debug.

Example

```
> adsl oamlb chklink on
OAM checking dsl link is ON.
> adsl oamlb F5 4
Tx cnt=0
Rx Cnt=0
>
```

Telnet Command: adsl vcilimit

This command can cancel the limit for vci value.

Some ISP might set the vci value under 32. In such case, we can cancel such limit manually by using this command. Do not set the number greater than 254.

Syntax

```
adsl vcilimit [n]
```

Syntax Description

Parameter	Description
<i>n</i>	The number shall be between 1 - 254.

Example

```
> adsl vcilimit 33
change VCI limitation from 32 to 33.
```

Telnet Command: adsl annex

This command can display the annex interface of this router.

Example

```
> adsl annex
% hardware is annex B.
% modem code is annex B; built at 01/15,07:34.
```

Telnet Command: adsl automode

This command is used to add or remove ADSL modes (such as ANNEXL, ANNEXM and ANNEXJ) supported by Multimode.

Syntax

`adsl automode [add|remove|set|default|show] [adsl_mode]`

Syntax Description

Parameter	Description
<i>add</i>	It means to add ADSL mode.
<i>remove</i>	It means to remove ADSL mode.
<i>set</i>	It means to use default settings plus the new added ADSL mode.
<i>default</i>	It means to use default settings.
<i>show</i>	It means to display current setting.
<i>adsl_mode</i>	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
<i>startbin</i>	The number is between 0 ~ 4092.
<i>endbin</i>	The number is between 4 ~ 4095.
<i>up</i>	Show upstream information.

Example

```
> adsl showbins 2 30
DOWNSTREAM :
```

Bin	SNR	Gain	Bi	-	Bin	SNR	Gain	Bi	-	Bin	SNR	Gain	Bi	-	Bin	SNR	Gain	Bi
	dB	.1dB	ts			dB	.1dB	ts			dB	.1dB	ts			dB	.1dB	ts
Bin	SNR	Gain	Bi	-	Bin	SNR	Gain	Bi	-	Bin	SNR	Gain	Bi	-	Bin	SNR	Gain	Bi
	dB	.1dB	ts			dB	.1dB	ts			dB	.1dB	ts			dB	.1dB	ts

Telnet Command: adsl optn

This command allows you to configure DSL line feature.

Syntax

adsl optn FUNC [us/ds/bi [value/on/off]]

Syntax Description

Parameter	Description
<i>FUNC</i>	Available settings contain: 'bitswap', 'sra', 'aelem', 'g.vector', 'status', 'trellis', 'retx', 'default'.
<i>us/ds/bi</i>	us: upstream ds: downstream bi: bidirection. 'aelem' and 'g.vector' can be only on/off.
<i>value</i>	The value shall be hex digits. bitswap=0-2, sra=0,2,3,4.
<i>on/off</i>	Type "on" for enabling such function. Type "off" for disabling such function.

Example

```
> adsl optn default
trellis      [US] =      ON, [DS] =      ON.
bitswap      [US] =      0, [DS] =      0.
              [0: default(ON), 1: ON, 2: OFF]
sra          [US] =      0, [DS] =      0.
              [0: default(=3), 2: OFF, 3: ON , 4: DYNAMIC_SOS]
retx         [US] =      ON, [DS] =      ON.
aelem        ON
G.Vector     ON
```

Telnet Command: adsl savecfg

This command can save the configuration into FLASH with a file format of cfg.

Example

```
> adsl savecfg
% Xdsl Cfg Save OK!
```

Telnet Command: adsl vendorid

This command allows you to configure user-defined CPE vendor ID.

Syntax

`adsl vendorid [status/on/off/ set vid0 vid1]`

Syntax Description

Parameter	Description
<i>status</i>	Display current status of user-defined vendor ID.
<i>on</i>	Enable the user-defined function.
<i>off</i>	Disable the user-defined function.
<i>set vid0 vid1</i>	It means to set user-defined vendor ID with vid0 and vid1. The vendor ID shall be set with HEX format, ex: 00fe7244: 79612f21.

Example

```
> adsl vendorid status
% User define CPE Vendor ID is OFF
% vid0:vid1 = 0x00fe7244:79612f21
> adsl vendorid on set vid0 vid1
% User define CPE Vendor ID is ON
```

Telnet Command: adsl atm

This command can set QoS parameter for ATM.

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
<i>pvc_no</i>	It means <i>pvc</i> number and must be between 0(Channel 1) to 7(Channel 8).
<i>PCR</i>	It means Peak Cell Rate for upstream. The range for the number is "1" to "2539".
<i>max</i>	It means to get the highest speed for the upstream.
<i>SCR</i>	It means Sustainable Cell Rate.
<i>MBS</i>	It means Maximum Burst Size.
<i>status</i>	It means to display PCR/SCR/MBS setting.

Example

```
> adsl atm pcr 1 200 max
% PCR is 200 for pvc 1.

> adsl atm pcr status
pvc  channel      PCR
-----
```

```

0      1      0
1      2      200
2      3      0
3      4      0
4      5      0
5      6      0
6      7      0
7      8      0
> adsl atm mbs 2 300 max
% MBS is 300 for 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
<i>pvc_x</i>	It means the PVC number for the source.
<i>pvc_y</i>	It means the PVC number that the source PVC will be bound to.
<i>status</i>	Display a table for PVC binding group.
<i>-1</i>	It means to clear specific PVC binding.

Example

```

> adsl pvcbinding 3 5
set done. bind pvc3 to pvc5.

```

The above example means PVC3 has been bound to PVC5.

```

> adsl pvcbinding 3 -1
clear pvc-1 binding

```

The above example means the PVC3 binding group has been removed.

Telnet Command: adsl inventory

This command is used to display information about CO or CPE.

Syntax

`adsl inventory [co/cpe]`

Syntax Description

Parameter	Description
<i>co</i>	It means DSLAM (Digital Subscriber Line Access Multiplexer) or CO (Central Office).
<i>cpe</i>	It means CPE (Customer Premise Equipment).

Example

```

> adsl inventory co
xDSL inventory info only available in showtime.

```

```

> adsl inventory cpe
G.994 vendor ID           : 0XB5004946544E5444
  G.994.1 country code    : 0XB500
  G.994.1 provider code   : IFTN
  G.994.1 vendor info     : 0X5444
System vendor ID         : 0XB5004946544E0000
  System country code     : 0XB500
  System provider code    : IFTN
  System vendor info     : 0X000
Version number           : 3.8.2_RC4a_STD
Version number(16 octets) : 0X332E382E325F524334615F5354440000
Self-test result         : PASS
Transmission mode capability : 0X40004004C010400
>

```

Telnet Command: vdsl status

This command is used to display current status of VDSL setting.

Syntax

`vdsl status [more | counts | hlog | qln | snr | bandinfo | olr]`

Example

```

> vdsl status
----- ATU-R Info (hw: annex A, f/w: annex A/B/C) -----
Running Mode           :                State           : TRAINING
DS Actual Rate         :                US Actual Rate   :                0 bps
DS Attainable Rate     :                US Attainable Rate :                0 bps
DS Path Mode           :                US Path Mode     :                Fast
DS Interleave Depth    :                US Interleave Depth :                0
NE Current Attenuation :                Cur SNR Margin       :                0 dB
DS actual PSD          :                US actual PSD     :                0.0 dB
NE CRC Count           :                FE CRC Count      :                0
NE ES Count            :                FE ES Count       :                0
Xdsl Reset Times       :                Xdsl Link Times   :                0
ITU Version[0]         : b5004946             ITU Version[1]       : 544e0000
VDSL Firmware Version  : 05-04-08-00-00-06
Power Management Mode  : DSL_G997_PMS_NA
Test Mode              : DISABLE
----- ATU-C Info -----
Far Current Attenuation :                Far SNR Margin       :                0 dB
CO ITU Version[0]       : 00000000             CO ITU Version[1]   : 00000000
DSLAM CHIPSET VENDOR   : < unknown >
>

```

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
<i>on</i>	DSL is under test mode. DSL debug tool mode is off.

<code>tcpmessage</code>	DSL debug tool mode is on.
<code>tcpmessage_off</code>	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 vdsl2/2+ 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
<code>startbin</code>	The number is between 0 ~ 4092.
<code>endbin</code>	The number is between 4 ~ 4095.
<code>up</code>	Show upstream information.

Example

```

> vdsl showbins 2 30
DOWNSTREAM :
-----
Bin  SNR  Gain Bi - Bin  SNR  Gain Bi - Bin  SNR  Gain Bi - Bin  SNR  Gain Bi
dB   .1dB ts      dB   .1dB ts      dB   .1dB ts      dB   .1dB ts
-----
Bin  SNR  Gain Bi - Bin  SNR  Gain Bi - Bin  SNR  Gain Bi - Bin  SNR  Gain Bi
dB   .1dB ts      dB   .1dB ts      dB   .1dB ts      dB   .1dB ts

```

Telnet Command: 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
<i>FUNC</i>	Available settings contain: 'bitswap', 'sra', 'aelem', 'g.vector', 'status', 'trellis', 'retx', 'default'.
<i>us/ds/bi</i>	us: upstream ds: downstream bi: bidirection. 'aelem' and 'g.vector' can be only on/off.
<i>value</i>	The value shall be hex digits. bitswap=0-2, sra=0,2,3,4.
<i>on/off</i>	Type "on" for enabling such function. Type "off" for disabling such function.

Example

```

> vdsl optn default
trellis      [US] =    ON, [DS] =    ON.
bitswap     [US] =    0, [DS] =    0.
             [0: default(ON), 1: ON, 2: OFF]
sra         [US] =    0, [DS] =    0.
             [0: default(=3), 2: OFF, 3: ON , 4: DYNAMIC_SOS]
retx        [US] =    ON, [DS] =    ON.
aelem       ON
G.Vector    ON

```

Telnet Command: 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
<code>status</code>	Display current status of user-defined vendor ID.
<code>on</code>	Enable the user-defined function.
<code>off</code>	Disable the user-defined function.
<code>set vid0 vid1</code>	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
<code>co</code>	It means DSLAM (Digital Subscriber Line Access Multiplexer) or CO (Central Office).
<code>cpe</code>	It means CPE (Customer Premise Equipment).

Example

```
> 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
  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: bpa

This command allows to configure a network setting specified for Australia's ISP.

Syntax

`bpa m [-<command> <parameter> / ...]`

Syntax Description

Parameter	Description
<i>m</i>	Available settings are 1 and 2.
-a <enable>	1/0 to enable/disable this entry
-n <UserName>	contact UserName(max. 24 characters)
-p <PassWord>	contact PassWord (max. 24 characters)
-s <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)
-l <List>	List all settings configured.

Example

```
> 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
<i>INDEX</i>	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.
<i>NAME</i>	It means to specify a name for the CSM profile, less than 15 characters.
<i>setdefault</i>	Reset to default settings.

Example

```
> csm appe prof -i 1 -n games  
The name of APPE Profile 1 was setted.
```

Telnet Command: csm appe set

It is used to configure group settings for IM/P2P/Protocol and Others in APP Enforcement Profile.

```
csm appe set -i INDEX [-v GROUP| -e AP_IDX | -d AP_IDX| -a AP_IDX [ACTION]]
```

Syntax Description

Parameter	Description
<i>INDEX</i>	Specify the index number of CSM profile, from 1 to 32.
-v	View the IM/P2P/Protocol and Others configuration of the CSM profile.
-e	Enable to block specific application.
-d	Disable to block specific application.
-a	Set the action of specific application
<i>GROUP</i>	Specify the category of the application. Available options are: IM, P2P, Protocol and Others.
<i>AP_IDX</i>	Each application has independent index number for identification in CLI command. Specify the index number of the application here. If you have no idea of the index number, do the following (Take IM as an example): Type “csm appe set -l 1 -v IM”, the system will list all of the index numbers of the applications categorized under IM.
<i>ACTION</i>	Specify the action of the application, 0 or 1. 0: Block. All of the applications meet the CSM rule will be blocked. 1: Pass. All of the applications meet the CSM rule will be passed.

Example

```
>csm appe set -i 1 -a 1 1
Profile 1 - : <NULL> action set to Pass.
>
```

Telnet Command: csm appe show

It is used to display group (IM/P2P/Protocol and Others) information APP Enforcement Profile.
csm appe show [-a/-i/-p/-t/-m]

Syntax Description

Parameter	Description
-a	View the configuration status for All groups.
-i	View the configuration status of IM group.
-p	View the configuration status of P2P group.
-t	View the configuration status of protocol group.
-m	View the configuration status of Others group.

Example

```
>csm appe show -t

      Type      Index          Name          Version  Advance
Advanced Option: (M)essage, (F)ile Transfer, (G)ame, (C)onference, and (O)ther
Activities
-----
      PROTOCOL      52          DB2
      PROTOCOL      53          DNS
      PROTOCOL      54          FTP
      PROTOCOL      55          HTTP          1.1
      PROTOCOL      56          IMAP          4.1
      PROTOCOL      57      IMAP STARTTLS  4.1
      PROTOCOL      58          IRC          2.4.0          .....
```

Telnet Command: csm appe config

It is used to display the configuration status (enabled or disabled) for IM/P2P/Protocol/Other applications.

csm appe config -v *INDEX* [-i/-p/-t/-m]

Syntax Description

Parameter	Description
<i>INDEX</i>	Specify the index number of CSM profile, from 1 to 32.
-i	View the configuration status of IM group.
-p	View the configuration status of P2P group.
-t	View the configuration status of protocol group.
-m	View the configuration status of Others group.

Example

```
> csm appe config -v 1 -m
```

Group	Type	Index	Name	Enable	A
vance Enable					
Advance abbreviation: Message, File Transfer, Game, Conference, and Other					
Advance abbreviation: : M, F, G, C, and O					

OTHERS	TUNNEL	75	DNSCrypt	Disable	
OTHERS	TUNNEL	76	DynaPass	Disable	
OTHERS	TUNNEL	77	FreeU	Disable	
OTHERS	TUNNEL	78	HTTP Proxy	Disable	
OTHERS	TUNNEL	79	HTTP Tunnel	Disable	
OTHERS	TUNNEL	80	Hamachi	Disable	
OTHERS	TUNNEL	81	MS Teredo	Disable	
OTHERS	TUNNEL	82	MS Teredo	Disable	
OTHERS	TUNNEL	83	PGPNet	Disable	
OTHERS	TUNNEL	84	Ping Tunnel	Disable	
.					
.					
.					

Total 66 APPs					
>					

Telnet Command: csm appe interface

It is used to configure APPE signature download interface.

csm appe interface *[AUTO/WAN#]*

Syntax Description

Parameter	Description
<i>AUTO</i>	Vigor router specifies WAN interface automatically.
<i>WAN</i>	Specify the WAN interface for signature downloading.

Example

<pre>> csm appe interface wan1</pre> <p>Download interface is set as "WAN1" now.</p> <pre>> csm appe interface auto</pre> <p>Download interface is set as "auto-selected" now.</p>
--

Telnet Command: csm appe email

It is used to set notification e-mail for APPE signature based on the settings configured in System Maintenance>>SysLog/Mail Alert Setup (in which, the box of APPE Signature is checked under Enable E-Mail Alert).

csm appe email [-e/-d/-s]

Syntax Description

Parameter	Description
-e	Enable notification e-mail mechanism.
-d	Disable notification e-mail mechanism.
-s	Send an example e-mail.

Example

```
> csm appe email -e
Enable APPE email.
```

Telnet Command: csm ucf

It is used to configure settings for URL control filter profile.

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

Syntax Description

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)
-p	Set the priority (defined by the number specified in VALUE) for the profile.

<i>VALUE</i>	Number 0 to 3 represent different conditions. 0: It means Bundle: Pass. 1: It means Bundle: Block. 2: It means Either: URL Access Control First. 3: It means Either: Web Feature First.
<i>-l</i>	It means the log type of the profile. They are: P: Pass, B: Block, A: All, N: None
<i>MSG</i>	It means to specify the Administration Message, less then 255 characters
<i>uac</i>	It means to set URL Access Control part.
<i>wf</i>	It means to set Web Feature part.

Example

```
> csm ucf obj 1 -n game -l B
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
  Action:[pass]
[ ]Prevent web access from IP address.
  No  Obj NO.   Object Name
-----
  No  Grp NO.   Group Name
-----
```

Telnet Command: csm ucf obj INDEX uac

It means to configure the settings regarding to URL Access Control (uac).

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
```

Syntax Description

Parameter	Description
<i>INDEX</i>	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.
-e	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.
-o	Set the keyword object.
KEY_WORD_Object_Index	Specify the index number of the object profile.
-g	Set the keyword group.
KEY_WORD_Group_Index	Specify the index number of the group profile.

Example

```

> csm ucf obj 1 uac -i E
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
Action:[pass]
[v]Prevent web access from IP address.
  No  Obj NO.   Object Name
-----
  No  Grp NO.   Group Name
-----

> csm ucf obj 1 uac -a B
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
Action:[block]
[v]Prevent web access from IP address.
  No  Obj NO.   Object Name
-----
  No  Grp NO.   Group Name
-----

```

Telnet Command: csm ucf obj INDEX wf

It means to configure the settings regarding to Web Feature (wf).

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
<i>INDEX</i>	It means to specify the index number of CSM profile, from 1 to 8.
<i>-v</i>	It means to view the protocol configuration of the CSM profile.
<i>-e</i>	It means to enable the restriction of web feature.
<i>-d</i>	It means to disable the restriction of web feature.
<i>-a</i>	Set the action of web feature, P or B. B: Block. The web access meets the web feature will be blocked. P: Pass. The web access meets the web feature will be passed.
<i>-s</i>	It means to enable the the Web Feature configuration. Features available for configuration are: c: Cookie p: Proxy u: Upload
<i>-u</i>	It means to cancel the web feature configuration.
<i>-f</i>	It means to set the file extension object index number.
<i>File_Extension_Object_index</i>	Type the index number (1 to 8) for the file extension object.

Example

```
> csm ucf obj 1 wf -s c
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
Action:[block]
[v] Prevent web access from IP address.
No  Obj NO.   Object Name
-----
No  Grp NO.   Group Name
-----
```

```
[ ] Enable Restrict Web Feature
Action:[pass]
File Extension Object Index : [0]           Profile Name : []
[V] Cookie [ ] Proxy [ ] Upload
```

Telnet Command: csm wcf

It means to configure the settings regarding to web control filter (wcf).

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
```

Syntax Description

Parameter	Description
<i>show</i>	It means to display the web content filter profiles.
<i>Look</i>	It means to display the license information of WCF.
<i>Cache</i>	It means to set the cache level for the profile.
<i>Server WCF_SERVER</i>	It means to set web content filter server.
<i>Msg MSG</i>	It means de set the administration message. MSG means the content (less than 255 characters) of the message itself.
<i>setdefault</i>	It means to return to default settings for all of the profile.
<i>obj</i>	It means to specify the object profile.
<i>INDEX</i>	It means to specify the index number of web content filter profile, from 1 to 8.
<i>- v</i>	It means to view the web content filter profile.
<i>-a</i>	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.
<i>-n</i>	It means to set the profile name.
<i>PROFILE_NAME</i>	It means to specify the name of the profile (less than 16 characters)
<i>-I</i>	It means the log type of the profile. They are:

	P: Pass, B: Block, A: All, N: None
<i>-o</i>	Set the keyword object.
<i>KEY_WORD_Object_Index</i>	Specify the index number of the object profile.
<i>-g</i>	Set the keyword group.
<i>KEY_WORD_Group_Index</i>	Specify the index number of the group profile.
<i>-w</i>	It means to set the action for the black and white list. E: Enable, D: Disable, P: Pass, B: Block
<i>-s</i>	It means to choose the items under CATEGORY or WEB_GROUP.
<i>-u</i>	It means to discard items under CATEGORY or WEB_GROUP.
WEB_GROUP	Child_Protection, Leisure, Business, Chating, Computer Internet, Other
CATEGORY	Includes: Alcohol & Tobacco, Criminal Activity, Gambling, Hate & Intoleranc, Illegal Drug, Nudity, Pornography/Sexually Explicit, Weapons, Violence, School Cheating, Sex Education, Tasteless, Child Abuse Imges, Entertainment, Games, Sports, Travel, Leisure & Recreation, Fashin & Beauty, Business, Job Search, Web-based Emai, Chat, Instant Messaging, Anonymizers, Forums & Newsgroups, Computers & Technology, Download Sites, Streaming Media & Downloads, Phishing & Fraud, Search Engines & Portals, Social Networking, Spam Sites, Malware, Botnets, Hacking, Illegal Software, Information Security, Peer-to-eer, Advertisements & Pop-Ups, Arts, Transportation, Compromised, Dating & Personals, , Education, Finance, Government, Health & Medcine, News, Non-profits & NGOs, Personal Sites, Politics, Real Estate, Rligion, Restaurants & Dining, Shopping, Translators, General, Cults, Greetig cards, Image Sharing, Network Errors, Parked Domains, Private IP Addresses)

Example

```
> csm wcf obj 1 -n test_wcf
Profile Index: 1
Profile Name:[test_wcf]
[ ]White/Black list
Action:[block]
  No  Obj NO.   Object Name
  ---  -
  No  Grp NO.   Group Name
  ---  -
Action:[block]
Log:[block]
-----
child Protection Group:
  [v]Alcohol & Tobacco      [v]Criminal & Activity   [v]Gambling
  [v]Hate & Intolerance     [v]Illegal Drug         [v]Nudity
  [v]Pornography & Sexually explicit [v]Violence
[v]Weapons

  [v]School Cheating       [v]Sex Education        [v]Tasteless
  [v]Child Abuse Images
-----
leisure Group:
  [ ]Entertainment         [ ]Games                 [ ]Sports
  [ ]Travel                 [ ]Leisure & Recreation [ ]Fashion & Beauty
.
.
>
```

Telnet Command: csm dnsf

It means to configure the settings regarding to DNS filter.

```
csm dnsf enable ON/OFF
csm dnsf syslog N/P/B/A
csm dnsf service WCF_PROFILE
csm dnsf service_ucf UCF_PROFILE
csm dnsf time CACHE_TIME
csm dnsf blockpage show/on/off
csm dnsf profile_show
csm dnsf profile_edit INDEX
csm dnsf profile_edit INDEX -n PROFILE_NAME
csm dnsf profile_edit INDEX -I N/P/B/A
csm dnsf profile_edit INDEX -w WCF_PROFILE
csm dnsf profile_edit INDEX -u UCF_PROFILE
```

Syntax Description

Parameter	Description
<i>enable</i>	Enable or disable DNS Filter. ON: enable. OFF: disable.
<i>syslog</i>	Determine the content of records transmitting to Syslog. P: Pass. Records for the packets passing through DNS filter will be sent to Syslog. B: Block. Records for the packets blocked by DNS filter will be sent to Syslog. A: All. Records for the packets passing through or blocked by DNS filter will be sent to Syslog. N: None. No record will be sent to Syslog.
<i>service WCF_PROFILE</i>	WCF_PROFILE: Specify a WCF profile as the base of DNS filtering. Type a number to indicate the index number of WCF profile (1 is first profile, 2 is second profile, and so on ...).
<i>time CACHE_TIME</i>	CACHE_TIME: It means to set the time for cache to live (available values are 1 to 24; 1 is one hour, 2 is two hours, and so on ...) for DNS filter.
<i>blockpage</i>	DNS sends block page for redirect port. When a web page is blocked by DNS filter, the router system will send a message page to describe that the page is not allowed to be visited. ON: Enable the function of displaying message page. OFF: Disable the function of displaying message page. SHOW: Display the function of displaying message page is ON or OFF.
<i>profile_show</i>	Display the table of the DNS filter profile.
<i>profile_edit</i>	Modify the content of the DNS filter profile.
<i>-n PROFILE_NAME</i>	PROFILE_NAME: Type the name of the DNS filter profile that you want to modify.
<i>-I N P B A</i>	Specify the log type of the profile. P: Pass. B: Block. A: All. N: None.
<i>-w WCF_PROFILE</i>	WCF_PROFILE: Type the index number of the WCF profile.
<i>-u UCF_PROFILE</i>	UCF_PROFILE: Type the index number of the UCF profile.
<i>-c CACHE_TIME</i>	-c means to set the cache time for DNS filter. CACHE_TIME: It means to set the time for cache to live (available values are 1 to 24; 1 is one hour, 2 is two hours, and so on ...) for DNS filter.

Example

```
> csmf dnsf service 2
dns service set up!!!
>csmf dnsf service 3
wcf profile 3 is empty.....
>csmf 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
<i>Update in minutes</i>	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]]

Syntax Description

Parameter	Description
-V	It means to view the configuration of DoS defense system.
-D	It means to deactivate the DoS defense system.
-A	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 portscan.
THRESHOLD	It means the packet rate (packet/second) that a flooding attack will be detected. Set a value larger than 20.

<i>TIMEOUT</i>	It means the time (seconds) that a flooding attack will be blocked. Set a value larger than 5.
<i>-a</i>	It means to enable the defense function for all attacks listed in ATTACK_0.
<i>-e</i>	It means to enable defense function for a specific attack(s).
<i>ATTACK_0</i>	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.
<i>-d</i>	It means to disable the defense function for a specific attack(s).

Example

```
>dos -A
The Dos Defense system is Activated
>dos -s synflood 50 10
Synflood is enabled! Threshold=50 <pke/sec> timeout=10 <pke/sec>
```

Telnet Command: exit

Type this command will leave telnet window.

Telnet Command: Internet

This command allows you to configure detailed settings for WAN connection.

Syntax

internet *-W n -M n [-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
<i>-M n</i>	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
<i><command><parameter> ...]</i>	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
<i>-S <isp name></i>	It means to set ISP Name (max. 23 characters).
<i>-P <on/off></i>	It means to enable PPPoE Service.
<i>-u <username></i>	It means to set username (max. 49 characters) for Internet accessing.
<i>-p <password></i>	It means to set password (max. 49 characters) for Internet accessing.
<i>-a n</i>	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
<i>-t n</i>	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>	It means that PPPoE server will assign an IP address specified here for CPE (PPPoE client). If you type 0.0.0.0 as the <ip address>, ISP will assign suitable IP address for you. However, if you type an IP address here, the router will use that one as a fixed IP.
-w <ip address>	It means to assign WAN IP address for such connection. Please type an IP address here for WAN port.
-n <netmask>	It means to assign netmask for WAN connection. You have to type 255.255.255.xxx (x is changeable) as the netmask for WAN port.
-g <gateway>	It means to assign gateway IP for such WAN connection.
-V	It means to view Internet Access profile.
-C <sim pin code>	Set (PPP mode) SIM PIN code (max. 15 characters).
-O <init string>	Set (PPP mode) Modem Initial String (max. 47 characters).
-T <init string2>	Set (PPP mode) Modem Initial String2 (max. 47 characters)
-D <dial string>	Set (PPP mode) Modem Dial String (max. 31 characters).
-v <service name>	Set (PPP mode) Service Name (max. 23 characters).
-m <ppp username>	Set (PPP mode) PPP Username (max. 63 characters).
-o <ppp password>	Set (PPP mode) PPP Password (max. 62 characters).
-e n	Set (PPP mode) PPP Authentication Type. n= 0: PAP/CHAP (default), 1: PAP Only
-q n	(PPP mode) Index(1-15) in Schedule Setup-One
-x n	(PPP mode) Index(1-15) in Schedule Setup-Two
-y n	(PPP mode) Index(1-15) in Schedule Setup-Three
-z n	(PPP mode) Index(1-15) in Schedule Setup-Four
-Q <mode>	Set (PPP mode or DHCP mode) WAN Connection Detection Mode. <mode> 0: ARP Detect; 1: Ping Detect
-I <ping ip>	Set (PPP mode or DHCP mode) WAN Connection Detection Ping IP. <ping ip>= ppp.qqq.rrr.sss: WAN Connection Detection Ping IP
-L n	Set (PPP mode) WAN Connection Detection TTL (1-255) value.
-E <sim pin code>	Set (DHCP mode) SIM PIN code (max. 19 characters).
-G <mode>	Set (DHCP mode) Network Mode. <mode> 0: 4G/3G/2G; 1: 4G Only; 2: 3G Only; 3: 2G Only
-N <apn name>	Set (DHCP mode) APN Name (max. 47 characters)
-U n	(DHCP mode) MTU(1000-1440)

Example

```
>internet -M 1 -S tcom -u username -p password -a 0 -t -1 -i 0.0.0.0
WAN1 Internet Mode set to PPPoE/PPPoA
```

```

WAN1 ISP Name set to tcom
WAN1 Username set to username
WAN1 Password set successful
WAN1 PPP Authentication Type set to PAP/CHAP
WAN1 Idle timeout set to always-on
WAN1 Gateway IP set to 0.0.0.0
> internet -V
WAN1 Internet Mode:PPPoE
ISP Name: tcom
Username: username
Authentication: PAP/CHAP
Idle Timeout: -1
WAN IP: Dynamic IP

```

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
<i>Enable</i>	Enable the function.
<i>Disable</i>	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
<i>?</i>	Display an IP address which allows users set as the public subnet IP address.
<i>public subnet IP address</i>	Specify an IP address. The system will set the one that you specified as the public subnet IP address.

Example

```

> ip pubaddr ?
% ip addr <public subnet IP address>

```

```
% Now: 192.168.0.1
> ip pubaddr 192.168.2.5
% Set public subnet IP address done !!!
```

Telnet Command: ip pubmask

This command allows users to set the mask for IP routed subnet of your router.

Syntax

```
ip pubmask ?
ip pubmask <public subnet mask>
```

Syntax Description

Parameter	Description
?	Display an IP address which allows users set as the public subnet mask.
<i>public subnet IP address</i>	Specify a subnet mask. The system will set the one that you specified as the public subnet mask.

Example

```
> ip pubmask ?
% ip pubmask <public subnet mask>
% Now: 255.255.255.0

> ip pubmask 255.255.0.0
% Set public subnet mask done !!!
```

Telnet Command: ip aux

This command is used for configuring WAN IP Alias.

Syntax

```
ip aux add [IP] [Join to NAT Pool][wanX]
ip aux remove [index]
```

Syntax Description

Parameter	Description
<i>add</i>	It means to create a new WAN IP address.
<i>remove</i>	It means to delete an existed WAN IP address.
<i>IP</i>	It means the auxiliary WAN IP address.
<i>Join to NAT Pool</i>	0 (disable) or 1 (enable).
<i>wanX</i>	Add or remove an address for WAN interface.
<i>index</i>	Type the index number of the table displayed on your screen.

Example

```
> ip aux add 192.168.1.65 1
% 192.168.1.65 has added in index 2.
```

```

> ip aux ?%% ip aux add [IP] [Join to NAT Pool]
%% ip aux remove [Index]

%%      Where IP = Auxiliary WAN IP Address.
%%      Join to NAT Pool = 0 or 1.
%%      Index = The Index number of table.

Now auxiliary WAN1 IP Address table:
Index no.      Status  IP address      NAT IP pool
-----
  1           Disable 0.0.0.0 Yes
  2           Enable 192.168.1.65   Yes

```

When you type *ip aux?*, the current auxiliary WAN IP Address table will be shown as the following:

Index no.	Status	IP address	IP pool
1	Enable	172.16.3.229	Yes
2	Enable	172.16.3.56	No
3	Enable	172.16.3.113	No

Telnet Command: ip addr

This command allows users to set/add a specified LAN IP your router.

Syntax

`ip addr [IP address]`

Syntax Description

Parameter	Description
<i>IP address</i>	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
<i>IP netmask</i>	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.

Syntax Description

Parameter	Description
<i>IP address</i>	It means the LAN IP address.
<i>MAC address</i>	It means the MAC address of your router.
<i>LAN or WAN</i>	It indicates the direction for the arp function.
<i>0/1/2/3/4/5</i>	0: disable to accept illegal source mac address 1: enable to accept illegal source mac address 2: disable to accept illegal dest mac address 3: enable to accept illegal dest mac address 4: Decline VRRP mac into arp table 5: Accept VRRP mac into arp table status: display the setting status.
<i>Time</i>	Available settings will be 10, 20, 30, ... 2550 seconds.

Example

```
> ip arp accept status
Accept illegal source mac arp: disable

Accept illegal dest mac arp: disable

Accept VRRP mac into arp table: disable
> ip arp status
[ARP Table]
  Index IP Address      MAC Address      Netbios Name
  1    192.168.1.113    00-05-5D-E4-D8-EE  A1000351
```

Telnet Command: ip dhcpc

This command is available for WAN DHCP.

Syntax

`ip dhcpc option`

`ip dhcpc option -h/l`

`ip dhcpc option -d [idx]`

`ip dhcpc option -e [1 or 0] -w [wan unumber] -c [option number] -v [option value]`

`ip dhcpc option -e [1 or 0] -w [wan unumber] -c [option number] -x "[option value]"`

`ip dhcpc option -u [idx unumber]`

`ip dhcpc release [wan number]`

`ip dhcpc renew [wan number]`

`ip dhcpc status`

Syntax Description

Parameter	Description
<i>option</i>	It is an optional setting for DHCP server. -h: display usage -l: list all custom set DHCP options -d: delete custom dhcp client option by index number -e: enable/disable option feature, 1:enable, 0:disable -w: set WAN number (e.g., 1=WAN1) -c: set option number: 0-255 -v: set option value by string -x: set option value by raw byte (hex) -u: update by index number
<i>release</i>	It means to release current WAN IP address.
<i>renew</i>	It means to renew the WAN IP address and obtain another new one.
<i>status</i>	It displays current status of DHCP client.

Example

```
>ip dhcpc status
I/F#3 DHCP Client Status:
```

```

DHCP Server IP      : 172.16.3.7
WAN Ipm             : 172.16.3.40
WAN Netmask         : 255.255.255.0
WAN Gateway         : 172.16.3.1
Primary DNS         : 168.95.192.1
Secondary DNS       : 0.0.0.0
Leased Time         : 259200
Leased Time T1      : 129600
Leased Time T2      : 226800
Leased Elapsed      : 259194
Leased Elapsed T1   : 129594
Leased Elapsed T2   : 226794

```

Telnet Command: ip ping

This command allows users to ping IP address of WAN1/WAN2/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
<i>IP address</i>	It means the WAN IP address.
<i>WAN1/PVC3/PVC4/PVC5</i>	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 tracet

This command allows users to trace the routes from the router to the host.

Syntax

```
ip tracet [Host/IP address] [WAN1/WAN2/WAN3/WAN4/WAN5] [Udp/Icmp]
```

Syntax Description

Parameter	Description
<i>IP address</i>	It means the target IP address.
<i>WAN1/WAN2</i>	It means the WAN port that the above IP address passes through.
<i>Udp/Icmp</i>	It means the UDP or ICMP.

Example

```
>ip tracert 22.128.2.62 WAN1
Traceroute to 22.128.2.62, 30 hops max
 1  172.16.3.7  10ms
 2  172.16.1.2  10ms
 3  Request Time out.
 4  168.95.90.66  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
<i>IP address</i>	Type the WAN or LAN IP address of the remote device.
<i>Port</i>	Type a port number (e.g., 23). Available settings: 0 ~65535.

Example

```
> ip telnet 172.17.3.252 23
>
```

Telnet Command: ip rip

This command allows users to set the RIP (routing information protocol) of IP.

Syntax

`ip rip [0/1/2]`

Syntax Description

Parameter	Description
<i>0/1/2</i>	0 means disable; 1 means first subnet and 2 means second subnet.

Example

```
> 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
<i>ifno</i>	It means the connection interface. 1: WAN1,2: WAN2, 3: PVC3,4: PVC4,5: PVC5 Note: PVC3 -PVC5 are virtual WANs.
<i>-e</i>	It means to disable or enable RIP setting for specified WAN interface. 1: Enable the function of setting RIP of WAN IP. 0: Disable the function.

Example

```
> ip wanrip ?
Valid ex:ip wanrip <ifno> -e <0/1>
<ifno> 1: WAN1,2: WAN2
       3: PVC3,4: PVC4,5: PVC5
-e <0/1> 0: disable, 1: enable
Now status:
WAN[1] Rip Protocol disable
WAN[2] Rip Protocol disable
WAN[3] Rip Protocol disable
WAN[4] Rip Protocol disable
WAN[5] Rip Protocol disable
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
<i>add</i>	It means to add an IP address as static route.
<i>del</i>	It means to delete specified IP address.
<i>status</i>	It means current status of static route.
<i>dst</i>	It means the IP address of the destination.
<i>netmask</i>	It means the netmask of the specified IP address.
<i>gateway</i>	It means the gateway of the connected router.
<i>ifno</i>	It means the connection interface. 3=WAN1 5=WAN3,6=WAN4,7=WAN5 However, WAN3, WAN4, WAN5 are router-borne WANs
<i>rtype</i>	It means the type of the route. default : default route; static: static route.
<i>cnc</i>	It means current IP range for CNC Network.
<i>default</i>	Set WAN1/WAN2/off as current default route.
<i>clean</i>	Clean all of the route settings. 1: Enable the function. 0: Disable the function.

Example

```
> ip route add 172.16.2.0 255.255.255.0 172.16.2.4 3 static
> ip route status

Codes: C - connected, S - static, R - RIP, * - default, ~ - private
C~      192.168.1.0/ 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
<i>set</i>	It means to enable proxy server.
<i>reset</i>	It means to disable proxy server.
<i>wan</i>	It means to specify WAN interface for IGMP service.
<i>t_home</i>	It means to specify t_home proxy server for using.
<i>On/off/show/help</i>	It means to turn on/off/display or get more information of the T_home service.
<i>query</i>	It means to set IGMP general query interval. The default value is 125000 ms.
<i>ppp</i>	0 - No need to set IGMP with PPP header. 1 - Set IGMP with PPP header.
<i>status</i>	It means to display current status for proxy server.

Example

```
> 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
<i>mac</i>	It means the MAC address of the device that you want to specify

Example

```
>ip dmz ?
% ip dmz <mac>, now : 00-00-00-00-00-00
> ip dmz 11-22-33-44-55-66
> ip dmz ?
% ip dmz <mac>, now : 11-22-33-44-55-66
>
```

Telnet Command: ip 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]`

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on session limit for each IP.
<i>off</i>	It means to turn off session limit for each IP.
<i>default [num]</i>	It means to set the default number of session num limit.
<i>Defaultlp2p [num]</i>	It means to set the default number of session num limit for p2p.
<i>status</i>	It means to display the current settings.
<i>show</i>	It means to display all session limit settings in the IP range.
<i>timer [num]</i>	It means to set when the IP session block works. The unit is second.

<i>[block/unblock][IP]</i>	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.
<i>add</i>	It means to add the session limits in an IP range.
<i>del</i>	It means to delete the session limits in an IP range.
<i>IP1-IP2</i>	It means the range of IP address specified for this command.
<i>num</i>	It means the number of the session limits, e.g., 100.
<i>p2pnum</i>	It means the number of the session limits, e.g., 50 for P2P.

Example

```
>ip session default 100
> ip session add 192.168.1.5-192.168.1.100 100 50
> ip session on
> ip session status

IP range:
  192.168.1.5 - 192.168.1.100 : 100

Current ip session limit is turn on

Current default session number is 100
```

Telnet Command: ip bandwidth

This command allows users to set maximum bandwidth limit number for the specified IP.

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]

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on the IP bandwidth limit.
<i>off</i>	It means to turn off the IP bandwidth limit.
<i>default [tx_rate][rx_rate]</i>	It means to set default tx and rx rate of bandwidth limit. The range is from 0 - 65535 Kpbs.
<i>status</i>	It means to display the current settings.
<i>show</i>	It means to display all the bandwidth limits settings within the IP range.
<i>add</i>	It means to add the bandwidth within the IP range.
<i>del</i>	It means to delete the bandwidth within the IP range.
<i>IP1-IP2</i>	It means the range of IP address specified for this command.

<i>tx</i>	It means to set transmission rate for bandwidth limit.
<i>rx</i>	It means to set receiving rate for bandwidth limit.
<i>shared</i>	It means that the bandwidth will be shared for the IP range.

Example

```

> ip bandwidth default 200 800
> ip bandwidth add 192.168.1.50-192.168.1.100 10 60
> ip bandwidth status

IP range:
  192.168.1.50 - 192.168.1.100 : Tx:10K Rx:60K

Current ip Bandwidth limit is turn off

Auto adjustment is off

```

Telnet Command: ip bindmac

This command allows users to set IP-MAC binding for LAN host.

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

```

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on IP bindmac policy. Even the IP is not in the policy table, it can still access into network.
<i>off</i>	It means to turn off all the bindmac policy.
<i>strict_on</i>	It means that only those IP address in IP bindmac policy table can access into network.
<i>show</i>	It means to display the IP address and MAC address of the pair of binded one.
<i>add</i>	It means to add one ip bindmac.
<i>del</i>	It means to delete one ip bindmac.
<i>IP</i>	It means to type the IP address for binding with specified MAC address.
<i>MAC</i>	It means to type the MAC address for binding with the IP address specified.
<i>Comment</i>	It means to type words as a brief description.
<i>All</i>	It means to delete all the IP bindmac settings.

Example

```
> ip bindmac add 192.168.1.46 00:50:7f:22:33:55 just for test
> ip bindmac show
ip bind mac function is turned ON
IP : 192.168.1.46 bind MAC : 00-50-7f-22-33-55 Comment : just
```

Telnet Command: ip maxnatuser

This command is used to set the maximum number of NAT users.

Syntax

ip maxnatuser *user no*

Syntax Description

Parameter	Description
<i>User no</i>	A number specified here means the total NAT users that Vigor router supports. 0 - It means no limitation.

Example

```
> ip maxnatuser 100
% Max NAT user = 100
```

Telnet Command: ip policy_rt

This command is used to set the IP policy route profile.

Syntax

ip policy_rt [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
<command><parameter>[...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
General Setup for Policy Route	
-i [value]	Specify an index number for setting policy route profile. Value: 1 to 60. "-1" means to get a free policy index automatically.
-e [0/1]	0: Disable the selected policy route profile. 1: Enable the selected policy route profile.
-o [value]	Determine the operation of the policy route. Value: add - Create a new policy route profile. del - Remove an existed policy route profile. edit - Modify an existed policy route profile. flush - Reset policy route to default setting.
-1 [any/range]	Specify the source IP mode. Range: Indicate a range of IP addresses. Any: It means any IP address will be treated as source IP address.
-2 [any/ip_range/ip_subnet/domain]	Specify the destination IP mode. Any: No need to specify an IP address for any IP address will be treated as destination IP address. ip_range: Indicates a range of IP addresses. ip_subnet: Indicates the IP subnet. domain: Indicates the domain name.
-3 [any/range]	Specify the destination port mode. Range: Indicate a range of port number.

	Any: It means any port number can be used as destination port.
<i>-G [default/specific]</i>	Specify the gateway mode.
<i>-L [default/specific]</i>	Specify the failover gateway mode.
<i>-s [value]</i>	Indicate the source IP start. Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.1.0)
<i>-S [value]</i>	Indicate the source IP end. Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.1.100)
<i>-d [value]</i>	Indicate the destination IP start. Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.2.0)
<i>-D [value]</i>	Indicate the destination IP end. Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.2.100)
<i>-p [value]</i>	Indicate the destination port start. Value: Type a number (1 ~ 65535) as the port start (e.g., 1000).
<i>-P [value]</i>	Indicate the destination port end. Value: Type a number (1 ~ 65535) as the port end (e.g., 2000).
<i>-y [value]</i>	Indicate the priority of the policy route profile. Value: Type a number (0 ~ 250). The default value is "150".
<i>-I [value]</i>	Indicate the interface specified for the policy route profile. Value: Available interfaces include, LAN1 ~ LAN8, IP_Routed_Subnet, DMZ_Subnet, WAN1 ~ WAN5, VPN_PROFILE_1 ~ VPN_PROFILE_100, WAN_1_IP_ALIAS_1 ~ WAN_4_IP_ALIAS_8
<i>-g [value]</i>	Indicate the gateway IP address. Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.3.1)
<i>-I [value]</i>	Indicate the failover IP address. Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.4.1)
<i>-t [value]</i>	It means "protocol". Value: Available settings include "TCP", "UDP", "TCP/UDP", "ICMP" and "Any".
<i>-n [0/1]</i>	Indicates the function of "Force NAT". 0: Disable the function. 1: Enable the function.
<i>-a [0/1]</i>	Indicates to enable the function of failover. 0: Disable the function. 1: Enable the function.
<i>-f [value]</i>	It means to specify the interface for failover. Value: Available interfaces include, NO_FAILOVER, Default_WAN, Policy1 ~ Policy60 LAN1 ~ LAN8 IP_Routed_Subnet, DMZ_Subnet, WAN1 ~ WAN5, VPN_PROFILE_1 ~ VPN_PROFILE_100, WAN_1_IP_ALIAS_1 ~ WAN_4_IP_ALIAS_8
<i>-b [value]</i>	It means "failback".

	Value: Available settings include, 0: Disable the function of "failback". 1: Enable the function of "failback". -v: View current failback setting.
Diagnose for Policy Route	
<i>-s [value]</i>	It means "source IP". Value: Available settings include: Any: It indicates any IP address can be used as source IP address. "xxx.xxx.xxx.xxx": The type format (e.g, 192.168.1.0).
<i>-d [value]</i>	It means "destination IP". Value : Available settings include: Any: It indicates any IP address can be used as destination IP address. "xxx.xxx.xxx.xxx": Specify an IP address.
<i>-p [value]</i>	It means "destination port". Value: Specify a number or type Any (indicating any number).
<i>-t [value]</i>	It means "protocol". Value: Available settings include "ICMP", "TCP", "UDP" and "Any".

Example

```
> ip policy_rt diagnose -s 192.168.1.100 -d any -p any -t ICMP

-----
      Matched Route  (Priority)
-----
* No_Match

-----
      Matched Policy (Priority)
-----
* Policy_1 (200)

* Conclusion:The packet was dropped because the send-to interface
of the mat
ched policy "policy 1" was inactive and there was no failover setting
> ip policy_rt -i -1 -o add -1 range -s 192.168.1.10 -S 192.168.1.20 -2
ip_range -d 202.211.100.10 -D 202.211.100.20 -g 202.211.100.1 -I WAN2
```

Telnet Command: ip dnsforward

This command is used to set LAN DNS profile for conditional DNS forwarding.

`ip dnsforward [-<command> <parameter> | ...]`

Syntax Description

Parameter	Description
<i>[<command> <parameter> ...]</i>	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
<i>-a <IP Address></i>	Set forwarded DNS server IP Address.
<i>-d <DNS server mapping index number></i>	Delete the selected LAN DNS profile.
<i>-e <0/1></i>	0: disable such function. 1: enable such function.

<i>-i <profile setting index number></i>	Type the index number of the profile.
<i>-l</i>	List the content of LAN DNS profile (including domain name, IP address and message).
<i>-n <domain name></i>	Set domain name.
<i>-p <profile name></i>	Set profile name for LAN DNS.
<i>-r</i>	Reset the settings for selected profile.

Example

```

> ip dnsforward -i 1 -n ftp.drayTek.com
% Configure Set1's DomainName:ftp.drayTek.com
> ip dnsforward -i 1 -a 172.16.1.1
% Configure Set1's IP:172.16.1.1
> ip dnsforward -i 1 -l
% Idx: 1
% State: Disable
% Profile: test
% Domain Name: ftp.drayTek.com
% DNS Server IP: 172.16.1.1
>

```

Telnet Command: ip6 addr

This command allows users to set the IPv6 address for your router.

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
<i>-s</i>	It means to add a static ipv6 address.
<i>-d</i>	It means to delete an ipv6 address.
<i>-a</i>	It means to show current address(es) status.
<i>-u</i>	It means to show only unicast addresses.
<i>prefix</i>	It means to type the prefix number of IPv6 address.
<i>prefix-length</i>	It means to type a fixed value as the length of the prefix.
<i>LAN/WAN1/WAN2/iface#</i>	It means to specify LAN or WAN interface for such address.

Example

```

> ip6 addr -a
LAN
Unicast Address:
  FE80::250:7FFF:FE00:0/64 (Link)
Multicast Address:

```

```
FF02::2
FF02::1:FF00:0
FF02::1
```

Telnet Command: ip6 dhcp req_opt

This command is used to configure option-request settings for DHCPv6 client.

Syntax

```
ip6 dhcp req_opt [LAN/WAN1/WAN2/iface#] [-<command> <parameter>| ... ]
```

Syntax Description

Parameter	Description
<i>req_opt</i>	It means option-request.
<i>LAN/WAN1/WAN2/iface#</i>	It means to specify LAN or WAN interface for such address.
<i>[<command> <parameter> ...]</i>	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
<i>-a</i>	It means to show current DHCPv6 status.
<i>-s</i>	It means to ask the SIP.
<i>-S</i>	It means to ask the SIP name.
<i>-d</i>	It means to ask the DNS setting.
<i>-D</i>	It means to ask the DNS name.
<i>-n</i>	It means to ask NTP.
<i>-i</i>	It means to ask NIS.
<i>-I</i>	It means to ask NIS name.
<i>-p</i>	It means to ask NISP.
<i>-P</i>	It means to ask NISP name.
<i>-b</i>	It means to ask BCMCS.
<i>-B</i>	It means to ask BCMCS name.
<i>-r</i>	It means to ask refresh time.
<i>Parameter</i>	1: the parameter related to the request will be displayed. 0: the parameter related to the request will not be displayed.

Example

```
> ip6 dhcp req_opt WAN2 -S 1
> ip6 dhcp req_opt WAN2 -r 1
> ip6 dhcp req_opt WAN2 -a
% Interface WAN2 is set to request following DHCPv6 options:
%   sip name
>
```

Telnet Command: ip6 dhcp client

This command allows you to use DHCPv6 protocol to obtain IPv6 address from server.

Syntax

```
ip6 dhcp client [WAN1/WAN2/iface#] [-<command> <parameter>| ... ]
```


Syntax Description

Parameter	Description
<i>client</i>	It means the dhcp client settings.
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-a	It means to show current DHCPv6 status.
-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

Example

```

> ip6 dhcp client WAN2 -p 2008::1
> ip6 dhcp client WAN2 -a
  Interface WAN2 has following DHCPv6 client settings:
    DHCPv6 client enabled
    request IA_PD whose IAID equals to 2008
> ip6 dhcp client WAN2 -n 1023456
> ip6 dhcp client WAN2 -a
  Interface WAN2 has following DHCPv6 client settings:
    DHCPv6 client enabled
    request IA_NA whose IAID equals to 2008
> system reboot

```

Telnet Command: ip6 dhcp server

This command allows you to configure DHCPv6 server.

Syntax

ip6 dhcp server [-<command> <parameter>| ...]

Syntax Description

Parameter	Description
<i>server</i>	It means the dhcp server settings.
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-a	It means to show current DHCPv6 status.
-i<pool_min_addr>	It means to set the start IPv6 address of the address pool.
-x<pool_max_addr>	It means to set the end IPv6 address of the address pool.
-d<addr>	It means to set the first DNS IPv6 address.
-D<addr>	It means to set the second DNS IPv6 address.
-c<parameter>	It means to send rapid commit to server. 1: Enable

	0: Disable
-e<parameter>	It means to enable or disable the DHCPv6 server. 1: Enable 0: Disable

Example

```
> ip6 dhcp server -d FF02::1
> ip6 dhcp server -i ff02::1
> ip6 dhcp server -x ff02::3
> ip6 dhcp server -a
% Interface LAN has following DHCPv6 server settings:
%   DHCPv6 server disabled
%   maximum address of the pool: FF02::3
%   minimum address of the pool: FF02::1
%   1st DNS IPv6 Addr: FF02::1
```

Telnet Command: ip6 internet

This command allows you to configure settings for accessing Internet.

Syntax

ip6 internet -W n -M n [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
-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> <parameter> ...]	The available commands with parameters are listed below. [...] 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>	It means to set Username.

	<username>= type a name as the username (maximum 63 characters).
-p <password>	It means to set Password. <password> = type a password (maximum 63 characters).
-s <server>	It means to set Tunnel Server IP. <server>= IPv4 address or URL (maximum 63 characters).
-d <server>	It means to set the primary DNS Server IP. <server>= type an IPv6 address for first DNS server.
-D <server>	It means to set the secondary DNS Server IP. <server>= type an IPv6 address for second DNS server.
-t <dhcp/ra/none>	It means to set IPv6 PPP WAN test mode for DHCP or RADVD. <dhcp/ra/none>= type IPv6 address.
-V	It means to view IPv6 Internet Access Profile.
-o	It means to set AICCU always on. 1=On, 0=Off

Example

```
> 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.

Example

```
> ip6 neigh -s 2001:2222:3333::1111 00:50:7F:11:ac:22:WAN2
    Neighbour 2001:2222:3333::1111 successfully added!
> ip6 neigh -a
```

I/F	ADDR	MAC	STATE
LAN	FF02::1	33-33-00-00-00-01	CONNECTED
WAN2	2001:5C0:1400:B::10B8	00-00-00-00-00-00	CONNECTED
WAN2	2001:2222:3333::1111	00-00-00-00-00-00	CONNECTED
WAN2	2001:2222:6666::1111	00-00-00-00-00-00	CONNECTED
WAN2	::	00-00-00-00-00-00	CONNECTED
LAN	::		NONE

```
>
```

Telnet Command: ip6 neigh

This command allows you to add a proxy neighbour.

Syntax

```
ip6 neigh -s inet6_addr [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 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.

Example

```
> ip6 route -s FE80::250:7FFF:FE12:500 16 FE80::250:7FFF:FE12:100 LAN
%      Route FE80::250:7FFF:FE12:500/16 successfully added!
> ip6 route -a LAN
```

PREFIX/PREFIX-LEN	_EXPIRES_	_NEXT-HOP_	I/F	METRIC	STATE	FLAGS
FE80::/128	0	::	LAN	0	UNICAST	U
FE80::250:7FFF:FE00:0/128	0	::	LAN	0	UNICAST	U
FE80::/64	0		LAN	256	UNICAST	U
FE80::/16	0	FE80::250:7FFF:FE12:100	LAN	1024	UNICAST	UGA
FF02::1/128	0	FF02::1	LAN	0	UNICAST	UC
FF00::/8	0		LAN	256	UNICAST	U
::/0	0		LAN	-1	UNREACHABLE	!

Telnet Command: ip6 ping

This command allows you to ping an IPv6 address or a host.

Syntax

`ip6 ping [IPv6 address/Host] [LAN/WAN1/WAN2]`

Syntax Description

Parameter	Description
<i>IPv6 address/Host</i>	It means to specify the IPv6 address or host for ping.
<i>LAN/WAN1/WAN2</i>	It means to specify LAN or WAN interface for such address.

Example

```
> ip6 ping 2001:4860:4860::8888 WAN2

Pinging 2001:4860:4860::8888 with 64 bytes of Data:

Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms

Packets: Sent = 5, Received = 5, Lost = 0 <% loss>
>
```

Telnet Command: ip6 tracert

This command allows you to trace the routes from the router to the host.

Syntax

`ip6 tracert [IPv6 address/Host]`

Syntax Description

Parameter	Description
<i>IPv6 address/Host</i>	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
 7 2001:4860::8:0:2DAF      330 ms
 8 2001:4860::2:0:66E      340 ms
 9 Request timed out.      *
10 2001:4860:4860::8888    350 ms
Trace complete.
>
```

Telnet Command: ip6 tspan

This command allows you to display TSPC status.

Syntax

`ip6 tspan [ifno]`

Syntax Description

Parameter	Description
<i>ifno</i>	It means the connection interface. Ifno=1 (means WAN1) Info=2 (means WAN2)

Example

```
> ip6 tspan 2
Local Endpoint v4 Address : 111.243.177.223
Local Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b9
Router DNS name : 88866666.broker.freenet6.net
Remote Endpoint v4 Address :81.171.72.11
Remote Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b8
Tspan Prefixlen : 56
Tunnel Broker: Amsterdam.freenet.net
```

```
Status: Connected
>
```

Telnet Command: ip6 radvd

This command allows you to enable or disable RADVD server.

Syntax

`ip6 radvd -s [1|0] [lifetime]`

`ip6 radvd -V`

Syntax Description

Parameter	Description
<code>-s</code>	It means to enable or disable the default lifetime of the RADVD server. 1: Enable the RADVD server. 0: Disable the RADVD server.
<code>Lifetime</code>	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.
<code>-V</code>	It means to show the RADVD configuration.
<code>-r</code>	It means RA default test.
<code>-r [num]</code>	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]`

Syntax Description

Parameter	Description
<code>list</code>	It means to show the setting information of the access list.
<code>status</code>	It means to show the status of IPv6 management.
<code>add</code>	It means to add an IPv6 address which can be used to execute

	management through Internet.
<i>index</i>	It means the number (1, 2 and 3) allowed to be configured for IPv6 management.
<i>prefix</i>	It means to type the IPv6 address which will be used for accessing Internet.
<i>prefix-length</i>	It means to type a fixed value as the length of the prefix.
<i>remove</i>	It means to remove (delete) the specified index number with IPv6 settings.
<i>flush</i>	It means to clear the IPv6 access table.
<i>http/telnet/ping/https/ssh</i>	These protocols are used for accessing Internet.
<i>on/off</i>	It means to enable (on) or disable (off) the Internet accessing through http/telnet/ping.

Example

```

> ip6 mngt list add 1 FE80::250:7FFF:FE12:1010 128
> ip6 mngt list add 2 FE80::250:7FFF:FE12:1020 128
> ip6 mngt list add 3 FE80::250:7FFF:FE12:2080 128
> ip6 mngt list
% IPv6 Access List :
Index  IPv6 Prefix      Prefix Length
=====
1      FE80::250:7FFF:FE12:1010      128
2      FE80::250:7FFF:FE12:1020      128
3      FE80::250:7FFF:FE12:2080      128

> ip6 mngt status
% IPv6 Remote Management :
telnet : off,  http : off,    ping : off

```

Telnet Command: ip6 online

This command allows you to check the online status of IPv6 LAN /WAN.

Syntax

ip6 online [ifno]

Syntax Description

Parameter	Description
<i>ifno</i>	It means the connection interface. 0=LAN1 1=WAN1 2=WAN2

Example

```

> 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
% IPv6 DNS Server: :: Static
% 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
<i>ifno</i>	It means the connection interface. 1=WAN1 2=WAN2
<i>add</i>	It means to add an IPv6 address which can be used to execute management through Internet.
<i>prefix</i>	It means to type the IPv6 address which will be used for accessing Internet.
<i>prefix-length</i>	It means to type a fixed value as the length of the prefix.
<i>remove</i>	It means to remove (delete) the specified index number with IPv6 settings.
<i>show</i>	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
<i>Options</i>	There are several options provided here, such as <code>-v</code> , <code>-c [SET_NO]</code> , <code>-d [SET_NO]</code> ,... and etc.
<i>SET_NO</i>	It means to specify the index number (from 1 to 12) of filter set.
<i>RULE_NO</i>	It means to specify the index number (from 1 to 7) of filter rule set.
<code>-v</code>	Type <code>"-v"</code> to view the configuration of general set.
<code>-c [SET_NO]</code>	It means to setup Call Filter, e.g., <code>-c 2</code> . The range for the index number you can type is <code>"0"</code> to <code>"12"</code> (0 means "disable").
<code>-d [SET_NO]</code>	It means to setup Data Filter, e.g., <code>-d 3</code> . The range for the index number you can type is <code>"0"</code> to <code>"12"</code> (0 means "disable").
<code>-l [VALUE]</code>	It means to setup Log Flag, e.g., <code>-l 2</code> Type <code>"0"</code> to disable the log flag. Type <code>"1"</code> to display the log of passed packet. Type <code>"2"</code> to display the log of blocked packet. Type <code>"3"</code> to display the log of non-matching packet.
<code>-p [VALUE]</code>	It means to setup actions for packet not matching any rule, e.g., <code>-p 1</code> Type <code>"0"</code> to let all the packets pass; Type <code>"1"</code> to block all the packets.
<code>-M [P2P_NO]</code>	It means to configure IM/P2P for the packets not matching with any rule, e.g., <code>-M 1</code> Type <code>"0"</code> to let all the packets pass; Type <code>"1"</code> to block all the packets.
<code>-U [URL_NO]</code>	It means to configure URL content filter for the packets not matching with any rule, e.g., <code>-U 1</code> Type <code>"0"</code> to let all the packets pass; Type <code>"1"</code> to block all the packets.
<code>-a [AD_SET]</code>	It means to configure the advanced settings.
<code>-f [VALUE]</code>	It means to accept large incoming fragmented UDP or ICMP packets.
<code>-E [VALUE]</code>	It means to set the maximum count for session limitation.
<code>-F [VALUE]</code>	It means to configure the load-balance policy.
<code>-Q [VALUE]</code>	It means to set the QoS class.

Example

```
> ipf set -c 1 #set call filter start from set 1
Setting saved.

> ipf set -d 2 #set data filter start from set 2
Setting saved.
> ipf set -v

Call Filter: Enable (Start Filter Set = 1)
Data Filter: Enable (Start Filter Set = 2)
```

```

Log Flag      : None

Actions for packet not matching any rule:
  Pass or Block      : Pass
  CodePage           : ANSI(1252)-Latin I
  Max Sessions Limit: 60000
  Current Sessions  : 0
  Mac Bind IP        : Non-Strict
  QOS Class          : None
  APP Enforcement    : None
  URL Content Filter: None
  Load-Balance policy : Auto-select
-----
CodePage                : ANSI(1252)-Latin I
Window size             : 65535
Session timeout         : 1440
DrayTek Banner          : Enable
-----
Apply IP filter to VPN incoming packets      : Enable
Accept large incoming fragmented UDP or ICMP packets: Enable
-----
Strict Security Checking
  [ ] APP Enforcement
>

```

Telnet Command: ipf rule

This command is used to set filter rule for firewall.

Syntax

`ipf rule s r [-<command> <parameter> | ...`

`ipf rule s r -v`

Syntax Description

Parameter	Description
<i>s</i>	Such word means Filter Set, range form 1-12.
<i>r</i>	Such word means Filter Rule, range from 1-7.
<Command><parameter>	The following lists all of the available commands with parameters.
-e	It means to enable or disable the rule setting. 0- disable 1- enable
-s o:g <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 Address> <End IP Address> / <Address Mask>	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

	<p>type).</p> <p>0 - Subnet Address</p> <p>1 - Single Address</p> <p>2 - Any Address</p> <p>3 - Range Address</p> <p>Example:</p> <p>Set Subnet Address => -s u 0 192.168.1.10 255.255.255.0</p> <p>Set Single Address => -s u 1 192.168.1.10</p> <p>Set Any Address => -s u 2</p> <p>Set Range Address => -s u 3 192.168.1.10 192.168.1.15</p>
<i>-d u <Address Type> <Start IP Address> <End IP Address> / <Address Mask></i>	<p>It means to configure destination IP address including address type, start IP address, end IP address and address mask.</p> <p>u - It means "user defined".</p> <p><i>Address Type</i> - Type the number (representing different address type).</p> <p>0 - Subnet Address</p> <p>1 - Single Address</p> <p>2 - Any Address</p> <p>3 - Range Address</p> <p>Example:</p> <p>Set Subnet Address => -d u 0 192.168.1.10 255.255.255.0</p> <p>Set Single Address => -d u 1 192.168.1.10</p> <p>Set Any Address => -d u 2</p> <p>Set Range Address => -d u 3 192.168.1.10 192.168.1.15</p>
<i>-d o:g <obj></i>	<p>It means to specify destination IP object and IP group.</p> <p>o - indicates "object".</p> <p>g - indicates "group"</p> <p><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.</p>
<i>-S o:g <obj></i>	<p>It means to specify Service Type object and IP group.</p> <p>o - indicates "object".</p> <p>g - indicates "group"</p> <p><obj> - indicates index number of object or index number of group. Available settings range from 1-96. For example, "-S 0 1" means the first service type object profile.</p>
<i>-S u <protocol> <source_port_value> <destination_port_value></i>	<p>It means to configure advanced settings for Service Type, such as protocol and port range.</p> <p>u - it means "user defined".</p> <p><protocol> - It means TCP(6),UDP(17), TCP/UDP(255).</p> <p><source_port_value> -</p> <p>1 - Port OP, range is 0-3. 0:=, 1:!=, 2:>, 3:<</p> <p>3 - Port range of the Start Port Number, range is 1-65535.</p> <p>5 - Port range of the End Port Number, range is 1-65535.</p> <p><destination_port_value>:</p> <p>2 - Port OP, range is 0-3, 0:==, 1:!=, 2:>, 3:<</p> <p>4 - Port range of the Start Port Number, range is 1-65535.</p> <p>6 - Port range of the End Port Number, range is 1-65535.</p>
<i>-F</i>	<p>It means the Filter action you can specify.</p> <p>0 -Pass Immediately,</p> <p>1 - Block Immediately,</p>

	2 - Pass if no further match, 3 - Block if no further match.
<i>-q</i>	It means the classification for QoS. 1- Class 1, 2 - Class 2, 3 - Class 3, 4 - Other
<i>-l</i>	It means load balance policy. Such function is used for "debug" only.
<i>-E</i>	It means to enable APP Enforcement.
<i>-a<index></i>	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.
<i>-u<index></i>	It means to specify which URL Content Filter profile will be applied. <index> - Available settings range from 0 ~ 8. "0" means no profile will be applied.
<i>-c</i>	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
<i>-C <Windows Size> <Session_Timeout></i>	It means to set Window size and Session timeout (Minute). <Windows Size> - Available settings range from 1 ~ 65535. <Session_Timeout> - Make the best utilization of network resources.
<i>-v</i>	It is used to show current filter/rule settings.

Example

```
> 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>

Direction   : LAN -> WAN
Source IP   : Group1,
Destination IP: Group2,
Service Type : TCP/UDPGroupl,
Fragments   : Don't Care

Pass or Block      : Block Immediately
Branch to Other Filter Set: None
Max Sessions Limit : 32000
Current Sessions   : 0
Mac Bind IP        : Non-Strict
Qos Class          : None
APP Enforcement    : None
URL Content Filter : None
Load-Balance policy : Auto-select
Log                : 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]`

Syntax Description

Parameter	Description
<code>-r</code>	It means to refresh the flowtrack.
<code>-e</code>	It means to enable or disable the flowtrack. 0: Disable 1: Enable
<code>-f</code>	It means to show the sessions state of flowtrack. If you do not

	specify any IP address, then all the session state of flowtrack will be displayed.
<i>-b</i>	It means to show all of IP sessions state.
<i>-i [IP address]</i>	It means to specify IP address (e.g., -i 192.168.2.55).
<i>-p[value]</i>	It means to type a port number (e.g., -p 1024). Available settings are 0 ~ 65535.
<i>-t [value]</i>	It means to specify a protocol (e.g., -t tcp). Available settings include: <i>tcp</i> <i>udp</i> <i>icmp</i>

Example

```
>ipf flowtrack set -r
Refresh the flowstate ok
> ipf flowtrack view -f
Start to show the flowtrack sessions state:

ORIGIN>> 192.168.1.11:59939 ->      8.8.8.8: 53 ,ifno=0
REPLY >>      8.8.8.8: 53 -> 192.168.1.11:59939 ,ifno=3
          proto=17, age=93023180(3920), flag=203
ORIGIN>> 192.168.1.11:15073 ->      8.8.8.8: 53 ,ifno=0
REPLY >>      8.8.8.8: 53 -> 192.168.1.11:15073 ,ifno=3
          proto=17, age=93025100(2000), flag=203
ORIGIN>> 192.168.1.11: 7247 ->      8.8.8.8: 53 ,ifno=0
REPLY >>      8.8.8.8: 53 -> 192.168.1.11: 7247 ,ifno=3
          proto=17, age=93020100(7000), flag=203
End to show the flowtrack sessions state
```

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]
```

Syntax Description

Parameter	Description
<i>-c</i>	It means to show the latest call log.
<i>-f</i>	It means to show the IP filter log.
<i>-F</i>	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
<i>-h</i>	It means to show this usage help.
<i>-p</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.

Example

```

> log -w
25:36:25.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
    Client IP      = 0.0.0.0
    Your IP        = 0.0.0.0
    Next server IP = 0.0.0.0
    Relay agent IP = 0.0.0.0
25:36:33.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
    Client IP      = 0.0.0.0
    Your IP        = 0.0.0.0
    Next server IP = 0.0.0.0
    Relay agent IP = 0.0.0.0
25:36:41.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
    Client IP      = 0.0.0.0
    Your IP        = 0.0.0.0
    Next server IP = 0.0.0.0
    Relay agent IP = 0.0.0.0
25:36:49.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
    Client IP      = 0.0.0.0
    Your IP        = 0.0.0.0
    Next server IP = 0.0.0.0
    Relay agent IP = 0.0.0.0
25:36:57.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
    Client IP      = 0.0.0.0
    Your IP        = 0.0.0.0
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
```

Telnet Command: mngt ftpport

This command allows users to set FTP port for management.

Syntax

mngt ftpport *[FTP port]*

Syntax Description

Parameter	Description
<i>FTP port</i>	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
<i>Http port</i>	It means to enter the number for HTTP port. The default setting is 80.

Example

```
> mngt httpport 80
% Set web server port to 80 done.
```

Telnet Command: mngt httpsport

This command allows users to set HTTPS port for management.

Syntax

mngt httpsport [*Https port*]

Syntax Description

Parameter	Description
<i>Https port</i>	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
<i>Telnet port</i>	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
<i>ssh port</i>	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
<i>enable</i>	It means to activate FTP server function.
<i>disable</i>	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
<i>on</i>	All PING packets will be forwarded from LAN PC to Internet.
<i>off</i>	All PING packets will be blocked from LAN PC to Internet.
<i>viewlog</i>	It means to display a log of ping action, including source MAC and source IP.
<i>clearlog</i>	It means to clear the log of ping action.

Example

```
> mngt noping off
No Ping Packet Out is OFF!!
```

Telnet Command: mngt defenseworm

This command can block specified port for passing through the router.

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
<i>on</i>	It means to activate the function of defense worm packet out.
<i>off</i>	It means to inactivate the function of defense worm packet out.
<i>add port</i>	It means to add a new TCP port for block.
<i>del port</i>	It means to delete a TCP port for block.
<i>viewlog</i>	It means to display a log of defense worm packet, including source MAC and source IP.
<i>clearlog</i>	It means to remove the log of defense worm packet.

Example

```
> mngt defenseworm add 21
Add TCP port 21
Block TCP port list: 135, 137, 138, 139, 445, 21
> mngt defenseworm del 21
Delete TCP port 21
Block TCP port list: 135, 137, 138, 139, 445
```

Telnet Command: mngt rmtcfg

This command can allow the system administrators to login from the Internet. By default, it is not allowed.

Syntax

```
mngt rmtcfg [status]
mngt rmtcfg [enable]
mngt rmtcfg [disable]
mngt rmtcfg [http/https/ftp/telnet/ssh/tr069] [on/off]
```

Syntax Description

Parameter	Description
-----------	-------------

<i>status</i>	It means to display current setting for your reference.
<i>enable</i>	It means to allow the system administrators to login from the Internet.
<i>disable</i>	It means to deny the system administrators to login from the Internet.
<i>http/https/ftp/telnet/ssh/t r069</i>	It means to specify one of the servers/protocols for enabling or disabling.
<i>on/off</i>	on - enable the function. off - disable the function.

Example

```
> mngt rmtcfg ftp on
Enable server fail
Remote configure function has been disabled
please enable by enter mngt rmtcfg enable

> mngt rmtcfg enable
%% Remote configure function has been enabled.
> mngt rmtcfg ftp on
%% FTP server has been enabled.
```

Telnet Command: mngt lanaccess

This command allows users to manage accessing into Vigor router through LAN port.

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
<i>-e[0/1]</i>	It means to enable/disable the function. 0-disable the function. 1-enable the function.
<i>-s[value]</i>	It means to specify service offered. Available values include: FTP, HTTP, HTTPS, TELNET, SSH, None, All
<i>-i[value]</i>	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.
<i>-f</i>	It means to flush all of the settings.
<i>-d</i>	It means to restore the factory default settings.
<i>-v</i>	It means to view current settings.
<i>-h</i>	It means to get the usage of such command.

Example

```
> mngt lanaccess -e 1
> mngt lanaccess -s FTP,TELNET
> mngt lanaccess -i LAN3
>> mngt lanaccess -v
Current LAN Access Control Setting:
* Enable:Yes
* Service:
  - FTP:Yes
  - HTTP:No
  - HTTPS:No
  - TELNET:Yes
  - SSH:No
* Subnet:
  - LAN 2: disabled
  - LAN 3: enabled
  - LAN 4: disabled
  - LAN 5: disabled
  - LAN 6: disabled
  - DMZ: disabled
  - IP Routed Subnet: disabled
```

Note: the settings do NOT apply to LAN1, LAN1 is always allowed to access the router

Telnet Command: mngt echoicmp

This command allows users to reject or accept PING packets from the Internet.

Syntax

```
mngt echoicmp [enable]
```

```
mngt echoicmp [disable]
```

Syntax Description

Parameter	Description
<i>enable</i>	It means to accept the echo ICMP packet.
<i>disable</i>	It means to drop the echo ICMP packet.

Example

```
> mngt echoicmp enable
%% Echo ICMP packet enabled.
```

Telnet Command: mngt accesslist

This command allows you to specify that the system administrator can login from a specific host or network. A maximum of three IPs/subnet masks is allowed.

Syntax

```
mngt accesslist list
```

mngt accesslist add [*index*][*ip addr*][*mask*]

mngt accesslist remove [*index*]

mngt accesslist flush

Syntax Description

Parameter	Description
<i>list</i>	It can display current setting for your reference.
<i>add</i>	It means adding a new entry.
<i>index</i>	It means to specify the number of the entry.
<i>ip addr</i>	It means to specify an IP address.
<i>mask</i>	It means to specify the subnet mask for the IP address.
<i>remove</i>	It means to delete the selected item.
<i>flush</i>	It means to remove all the settings in the access list.

Example

```
> mngt accesslist add 1 192.168.1.89 255.255.255.0
%% Set OK.
> mngt accesslist list
%% Access list :
  Index IP address      Subnet mask
=====
  1      192.168.1.89    255.255.255.0
```

Telnet Command: mngt snmp

This command allows you to configure SNMP for management.

Syntax

mngt snmp [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-e <1/2>	1: Enable the SNMP function. 2: Disable the SNMP function.
-g<Community name>	It means to set the name for getting community by typing a proper character. (max. 23 characters)
-s <Community name>	It means to set community by typing a proper name. (max. 23 characters)
-m <IP address>	It means to set one host as the manager to execute SNMP function. Please type in IPv4 address to specify certain host.
-t <Community name>	It means to set trap community by typing a proper name. (max. 23 characters)
-n <IP address>	It means to set the IPv4 address of the host that will receive the trap community.
-T <seconds>	It means to set the trap timeout <0-999>.

-V	It means to list SNMP setting.
----	--------------------------------

Example

```
> mngt snmp -e 1 -g draytek -s DK -m 192.168.1.1 -t trapcom -n 10.20.3.40
-T 88
SNMP Agent Turn on!!!
Get Community set to draytek
Set Community set to DK
Manager Host IP set to 192.168.1.1
Trap Community set to trapcom
Notification Host IP set to 10.20.3.40
Trap Timeout set to 88 seconds
```

Telnet Command: msubnet switch

This command is used to configure multi-subnet.

Syntax

`msubnet switch [2/3/4/5/6][On/Off]`

Syntax Description

Parameter	Description
<i>2/3/4/5/6</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6
<i>On/Off</i>	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]`

Syntax Description

Parameter	Description
<i>2/3/4/5/6</i>	It means LAN interface. 2=LAN2

	3=LAN3 4=LAN4 5=LAN5 6=LAN6
<i>IP address</i>	Type the private IP address for the specified LAN interface.

Example

```
> 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
<i>2/3/4/5/6</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6
<i>IP address</i>	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
<i>2/3/4/5/6</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4

	5=LAN5 6=LAN6
--	------------------

Example

```
> msubnet status 2
% LAN2      Off: 0.0.0.0/0.0.0.0, PPP Start IP: 0.0.0.60
% DHCP server: Off
% Dhcp Gateway: 0.0.0.0, Start IP: 0.0.0.10, Pool Count: 50
```

Telnet Command: msubnet dhcps

This command allows you to enable or disable DHCP server for the subnet.

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

Parameter	Description
2/3/4/5/6	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6
On/Off	On - It means the subnet will be configured for NAT usage.

Off - It means the subnet will be configured for Routing usage.

Example

```
> > 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
<i>2/3/4/5/6</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6
<i>Gateway IP</i>	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
<i>2/3/4/5/6</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5

	6=LAN6
<i>IP counts</i>	Specify a total number of IP address allowed for each LAN interface. The available range is from 0 to 220.

Example

```
> msubnet ipcnt 2 15
This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet talk

This command is used to establish a route between two LAN interfaces.

Syntax

`msubnet talk [1/2/3/4/5/6] [1/2/3/4/5/6] [On/Off]`

Syntax Description

Parameter	Description
<i>1/2/3/4/5/6</i>	It means LAN interface. 1=LAN1 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6
<i>On/Off</i>	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> <On/Off>
% where 1:LAN1, 2:LAN2, 3:LAN3, 4:LAN4, 5:LAN5, 6:LAN6
% Now:
%           LAN1  LAN2  LAN3  LAN4  LAN5  LAN6
% LAN1           V
% LAN2          V   V
% LAN3                   V
% LAN4                       V
% LAN5                           V
% LAN6                               V
>
```

Telnet Command: msubnet startip

This command is used to configure a starting IP address for DHCP.

Syntax

`msubnet startip [2/3/4/5/6] [Gateway IP]`

Syntax Description

Parameter	Description
<i>2/3/4/5/6</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6
<i>Gateway IP</i>	Type an IP address as the starting IP address for a subnet.

Example

```
> ms subnet 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.
> ms subnet startip ?
% ms subnet 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: ms subnet 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
<i>2/3/4/5/6</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6
<i>Start IP</i>	Type an IP address as the starting IP address for PPP connection.

Example

```
> ms subnet 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 <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]

Syntax Description

Parameter	Description
<i>2/3/4/5/6</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6
<i>WINS IP</i>	Type the IP address as the WINS IP.

Example

```
> > 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
<i>2/3/4/5/6</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6
<i>WINS IP</i>	Type the IP address as the WINS IP.

Example

```
> > msubnet secWINS 2 192.168.3.89
% Set LAN2 Dhcp Secondary WINS IP done !!!

> msubnet secWINS ?
% msubnet secWINS <2/3/4/5/6> <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
<i>2/3/4/5/6</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6
<i>TFTP server name</i>	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
<i>interface</i>	Available settings include LAN1~LAN6, IP_Routed_Subnet, and DMZ.
<i>value</i>	1000 ~ 1508 (Bytes), default: 1500 (Bytes)

Example

```

> 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)
LAN3 MTU:           1500 (Bytes)
LAN4 MTU:           1500 (Bytes)
LAN5 MTU:           1500 (Bytes)
LAN6 MTU:           1500 (Bytes)
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*]

Syntax Description

Parameter	Description
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number of the specified object profile.
-v	It means to view the information of the specified object profile. Example: <i>object ip obj 1 -v</i>
-n <i>NAME</i>	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: <i>object ip obj 9 -n bruce</i>
-i <i>INTERFACE</i>	It means to define an interface for the IP object. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=3, means WAN Example: <i>object ip obj 8 -i 0</i>

<i>-s INVERT</i>	It means to set invert selection for the object profile. INVERT=0, means disabling the function. INVERT=1, means enabling the function. Example: <i>object ip obj 3 -s 1</i>
<i>-a TYPE</i>	It means to set the address type and IP for the IP object profile. TYPE=0, means Mask TYPE=1, means Single TYPE=2, means Any TYPE=3, means Rang Example: <i>object ip obj 3 -a 2</i>
<i>[START_IP]</i>	When the TYPE is set with 2, you have to type an IP address as a starting point and another IP address as end point. Type an IP address.
<i>[END/MASK_IP]</i>	Type an IP address (different with START_IP) as the end IP address.

Example

```
> object ip obj 1 -n marketing
> object ip obj 1 -a 1 192.168.1.45
> object ip obj 1 -v
IP Object Profile 1
Name :[marketing]
Interface:[Any]
Address type:[single]
Start ip address:[192.168.1.45]
End/Mask ip address:[0.0.0.0]
Invert Selection:[0]
```

Telnet Command: object 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

Syntax Description

Parameter	Description
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number of the specified group profile.
<i>-v</i>	It means to view the information of the specified group profile. Example: <i>object ip grp 1 -v</i>
<i>-n NAME</i>	It means to define a name for the IP group. NAME: Type a name with less than 15 characters. Example: <i>object ip grp 8 -n bruce</i>
<i>-i INTERFACE</i>	It means to define an interface for the IP group.

	<p>INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=2, means WAN Example: <i>object ip grp 3 -i 0</i></p>
<i>-a IP_OBJ_INDEX</i>	<p>It means to specify IP object profiles for the group profile. Example: <i>:object ip grp 3 -a 1 2 3 4 5</i> The IP object profiles with index number 1,2,3,4 and 5 will be group under such profile.</p>

Example

```

> object ip grp 2 -n First
IP Group Profile 2
Name      :[First]
Interface:[Any]
Included ip object index:
[0:][0]
[1:][0]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]

> object ip grp 2 -i 1
> object ip grp 2 -a 1 2
IP Group Profile 2
Name      :[First]
Interface:[Lan]
Included ip object index:
[0:][1]
[1:][2]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]

```

Telnet Command: object ipv6 obj

This command is used to create an IP object profile.

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
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number of the specified object profile.
-v	It means to view the information of the specified object profile. Example: <i>object ip obj 1 -v</i>
-n <i>NAME</i>	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: <i>object ip obj 9 -n bruce</i>
-i <i>INTERFACE</i>	It means to define an interface for the IP object. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=3, means WAN Example: <i>object ip obj 8 -i 0</i>
-s <i>INVERT</i>	It means to set invert selection for the object profile. INVERT=0, means disabling the function. INVERT=1, means enabling the function. Example: <i>object ip obj 3 -s 1</i>
-a <i>TYPE</i>	It means to set the address type and IP for the IP object profile. TYPE=0, means Mask TYPE=1, means Single TYPE=2, means Any TYPE=3, means Rang Example: <i>object ip obj 3 -a 2</i>
[<i>START_IP</i>]	When the TYPE is set with 2, you have to type an IP address as a starting point and another IP address as end point. Type an IP address.
[<i>END/MASK_IP</i>]	Type an IP address (different with <i>START_IP</i>) as the end IP address.

Example

```
> object ip obj 1 -n marketing
> object ip obj 1 -a 1 192.168.1.45
> object ip obj 1 -v
IP Object Profile 1
Name    :[marketing]
```

```

Interface:[Any]
Address type:[single]
Start ip address:[192.168.1.45]
End/Mask ip address:[0.0.0.0]
Invert Selection:[0]

```

Telnet Command: object ipv6 grp

This command is used to integrate several IP objects under an IP group profile.

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
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number of the specified group profile.
<i>-v</i>	It means to view the information of the specified group profile. Example: <i>object ip grp 1 -v</i>
<i>-n NAME</i>	It means to define a name for the IP group. NAME: Type a name with less than 15 characters. Example: <i>object ip grp 8 -n bruce</i>
<i>-i INTERFACE</i>	It means to define an interface for the IP group. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=2, means WAN Example: <i>object ip grp 3 -i 0</i>
<i>-a IP_OBJ_INDEX</i>	It means to specify IP object profiles for the group profile. Example: <i>:object ip grp 3 -a 1 2 3 4 5</i> The IP object profiles with index number 1,2,3,4 and 5 will be group under such profile.

Example

```

> object ip grp 2 -n First
IP Group Profile 2
Name   :[First]
Interface:[Any]
Included ip object index:
[0:][0]
[1:][0]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]

```

```

[7:][0]

> object ip grp 2 -i 1
> object ip grp 2 -a 1 2
IP Group Profile 2
Name      :[First]
Interface:[Lan]
Included ip object index:
[0:][1]
[1:][2]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]

```

Telnet Command: object service obj

This command is used to create service object profile.

Syntax

object service obj setdefault

object service obj INDEX -v

object service obj INDEX -n NAME

object service obj INDEX -p PROTOCOL

object service obj INDEX -s CHK [START_P] [END_P]

object service obj INDEX -d CHK [START_P] [END_P]

Syntax Description

Parameter	Description
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number of the specified service object profile.
<i>-v</i>	It means to view the information of the specified service object profile. Example: <i>object service obj 1 -v</i>
<i>-n NAME</i>	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: <i>object service obj 9 -n bruce</i>
<i>-i PROTOCOL</i>	It means to define a PROTOCOL for the service object profile. PROTOCOL =0, means any PROTOCOL =1, means ICMP PROTOCOL =2, means IGMP PROTOCOL =6, means TCP PROTOCOL =17, means UDP PROTOCOL =255, means TCP/UDP Other values mean other protocols. Example: <i>object service obj 8 -i 0</i>
<i>CHK</i>	It means the check action for the port setting. 0=equal(=), when the starting port and ending port values are the

	<p>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.</p> <p>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.</p> <p>2=larger(>), the port number greater than this value is available..</p> <p>3=less(<), the port number less than this value is available for this profile.</p>
<code>-s CHK [START_P] [END_P]</code>	<p>It means to set source port check and configure port range (1-65565) for TCP/UDP.</p> <p>END_P, type a port number to indicate source port.</p> <p>Example: <code>object service obj 3 -s 0 100 200</code></p>
<code>-d CHK [START_P] [END_P]</code>	<p>It means to set destination port check and configure port range (1-65565) for TCP/UDP.</p> <p>END_P, type a port number to indicate destination port.</p> <p>Example: <code>object service obj 3 -d 1 100 200</code></p>

Example

```

> object service obj 1 -n limit
> object service obj 1 -p 255
> object service obj 1 -s 1 120 240
> object service obj 1 -d 1 200 220
> object service obj 1 -v
Service Object Profile 1
Name      :[limit]
Protocol  :[255]
Source port check action:[!=]
Source port range:[120~240]
Destination port check action:[!=]
Destination port range:[200~220]

```

Telnet Command: object service grp

This command is used to integrate several service objects under a service group profile.

Syntax

```

object service grp setdefault
object service grp INDEX -v
object service grp INDEX -n NAME
object service grp INDEX -a SER_OBJ_INDEX

```

Syntax Description

Parameter	Description
<code>setdefault</code>	It means to return to default settings for all profiles.
<code>INDEX</code>	It means the index number of the specified group profile.
<code>-v</code>	It means to view the information of the specified group profile. Example: <code>object service grp 1 -v</code>
<code>-n NAME</code>	It means to define a name for the service group.

	NAME: Type a name with less than 15 characters. Example: <i>object service grp 8 -n bruce</i>
<i>-a SER_OBJ_INDEX</i>	It means to specify service object profiles for the group profile. Example: <i>:object service grp 3 -a 1 2 3 4 5</i> The service object profiles with index number 1,2,3,4 and 5 will be group under such profile.

Example

```
>object service grp 1 -n Grope_1
Service Group Profile 1
Name   :[Grope_1]
Included service object index:
[0:][0]
[1:][0]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]

> object service grp 1 -a 1 2
Service Group Profile 1
Name   :[Grope_1]
Included service object index:
[0:][1]
[1:][2]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]
```

Telnet Command: object kw

This command is used to create keyword profile.

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
```

Syntax Description

Parameter	Description
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>show PAGE</i>	It means to show the contents of the specified profile.

	PAGE: type the page number.
<i>show</i>	It means to show the contents for all of the profiles.
<i>INDEX</i>	It means the index number of the specified keyword profile.
<i>-v</i>	It means to view the information of the specified keyword profile.
<i>-n NAME</i>	It means to define a name for the keyword profile. NAME: Type a name with less than 15 characters.
<i>-a CONTENTS</i>	It means to set the contents for the keyword profile. Example: <i>object kw obj 40 -a test</i>

Example

```
> object kw obj 1 -n children
Profile 1
Name  :[children]
Content:[]
> object kw obj 1 -a gambling
Profile 1
Name  :[children]
Content:[gambling]

> object kw obj 1 -v
Profile 1
Name  :[children]
Content:[gambling]
```

Telnet Command: object fe

This command is used to create File Extension Object profile.

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`

Syntax Description

Parameter	Description
<i>show</i>	It means to show the contents for all of the profiles.
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number (from 1 to 8) of the specified file extension object profile.
<i>-v</i>	It means to view the information of the specified file extension object profile.
<i>-n NAME</i>	It means to define a name for the file extension object profile. NAME: Type a name with less than 15 characters.
<i>-e</i>	It means to enable the specific <i>CATEGORY</i> or <i>FILE_EXTENSION</i> .

<code>-d</code>	It means to disable the specific CATEGORY or FILE_EXTENSION
<code>CATEGORY/FILE_EXTENSION</code>	<p>CATEGORY: Image, Video, Audio, Java, ActiveX, Compression, Execution Example: <code>object fe obj 1 -e Image</code></p> <p>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: <code>object fe obj 1 -e .bmp</code></p>

Example

```

> object fe obj 1 -n music
> object fe obj 1 -e Audio
> object fe obj 1 -v
Profile Index: 1
Profile Name:[music]

-----
Image category:
[ ].bmp [ ].dib [ ].gif [ ].jpeg [ ].jpg [ ].jpg2 [ ].jp2 [ ].pct
[ ].pcx [ ].pic [ ].pict [ ].png [ ].tif [ ].tiff
-----
Video category:
[ ].asf [ ].avi [ ].mov [ ].mpe [ ].mpeg [ ].mpg [v].mp4 [ ].qt
[ ].rm [v].wmv [ ].3gp [ ].3gpp [ ].3gpp2 [ ].3g2
-----
Audio category:
[v].aac [v].aiff [v].au [v].mp3 [v].m4a [v].m4p [v].ogg [v].ra
[v].ram [v].vox [v].wav [v].wma
-----
Java category:
[ ].class [ ].jad [ ].jar [ ].jav [ ].java [ ].jcm [ ].js [ ].jse
[ ].jsp [ ].jtk
-----
ActiveX category:
[ ].alx [ ].apb [ ].axs [ ].ocx [ ].olb [ ].ole [ ].tlb [ ].viv
[ ].vrm
-----
Compression category:
[ ].ace [ ].arj [ ].bzip2 [ ].bz2 [ ].cab [ ].gz [ ].gzip [ ].rar
[ ].sit [ ].zip

```

```
-----
-----
Execution category:
[ ].bas [ ].bat [ ].com [ ].exe [ ].inf [ ].pif [ ].reg [ ].scr
```

Telnet Command: port

This command allows users to set the speed for specific port of the router.

Syntax

port [1, 2, 3, 4, 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, status]	
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: portmuptime

This command allows you to set a time of keeping the session connection for specified protocol.

Syntax

portmuptime [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
<i>[<command> <parameter> ...]</i>	The available commands with parameters are listed below. <i>[...]</i> means that you can type in several commands in one line.
<i>-t <sec></i>	It means "TCP" protocol. <sec>: Type a number to set the TCP session timeout.
<i>-u <sec></i>	It means "UDP" protocol. <sec>: Type a number to set the UDP session timeout.
<i>-i <sec></i>	It means "IGMP" protocol. <sec>: Type a number to set the IGMP session timeout.
<i>-w <sec></i>	It means "TCP WWW" protocol. <sec>: Type a number to set the TCP WWW session timeout.
<i>-s <sec></i>	It means "TCP SYN" protocol. <sec>: Type a number to set the TCP SYN session timeout.
<i>-f</i>	It means to flush all portmaps (useful for diagnostics).
<i>-l <List></i>	List all settings.

Example

```
> portmuptime -t 86400 -u 300 -i 10
> portmuptime -l
----- Current setting -----
TCP Timeout      : 86400 sec.
UDP Timeout      : 300 sec.
IGMP Timeout     : 10 sec.
TCP WWW Timeout : 60 sec.
TCP SYN Timeout  : 60 sec.
```

Telnet Command: ppa

This command allows you to configure PPA mode.

ppa [-<command> <parameter> | ...]

ppa n [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
<i>[<command> <parameter> ...]</i>	The available commands with parameters are listed below. <i>[...]</i> means that you can type in several commands in one line.
<i>-m <mode></i>	Specify a mode. 1=auto 2=manual(traffic) 3=manual(qos) 4=manual(specific hosts) 0=disable
<i>-p <proto></i>	Specify a protocol. proto - 1-TCP; 2-UDP; 3-Both.
<i>-b 1/0</i>	Enable/disable TWO-way hardware acceleration.
<i>-M enable/disable</i>	Enable/disable the multicast hardware acceleration.
<i>-S</i>	Show multicast table in HW acceleration

-V	Show PPA_WAN_Table and PPA_LAN_Table for reference.
-C	Clean all settings.
-X	Show hardware acceleration information.
-k	Clean the PPA table.
ppa n - used in QoS or specific host	
-l <rule>	Specify an index number of rule profile for QoS mode.
-h <host>	Type an IP address for Specific Host mode.
-s <start port>	Specify a starting port number for Specific Host mode.
-e <end port>	Specify an ending port number for Specific Host mode

Example

```

> ppa -m 1 -p 1 -b 0
Set ok! The PPA mode is Auto

% You need to set the Manual mode first !

%TWO way accleration is disable

> ppa -v
% PPA mode is Auto
%PPA Protocol TCP 1, UDP 0
%PPA two way disable
%PPA time is 10
%PPA range is 192
%PPA LAN entries 0
%PPA WAN entries 0
DrayTek> ppa -x
WAN1 status : Enable
WAN1 phy_type : ADSL
WAN1 session check = NULL
WAN2 status : Enable
WAN2 phy_type : ETHERNET
WAN2 session check = hw_acc_for_ether_XDSL

```

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

usblp_ptr=0
UsbPrintReady=0, UsbIsPrinting=0

```

Telnet Command: qos setup

This command allows user to set general settings for QoS.

Syntax

`qos setup [-<command> <parameter> | ...]`

Syntax Description

Parameter	Description
<code>[<command> <parameter> ...]</code>	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
<code>-h</code>	Type it to display the usage of this command.
<code>-m <mode></code>	It means to define which traffic the QoS control settings will apply to and enable QoS control. 0: disable. 1: in, apply to incoming traffic only. 2: out, apply to outgoing traffic only. 3: both, apply to both incoming and outgoing traffic. Default is enable (for outgoing traffic).
<code>-i <bandwidth></code>	It means to set inbound bandwidth in kbps (Ethernet WAN only) The available setting is from 1 to 100000.
<code>-o <bandwidth></code>	It means to set outbound bandwidth in kbps (Ethernet WAN only). The available setting is from 1 to 100000.
<code>-r <index:ratio></code>	It means to set ratio for class index, in %.
<code>-u <mode></code>	It means to enable bandwidth control for UDP. 0: disable 1: enable Default is disable.
<code>-p <ratio></code>	It means to enable bandwidth limit ratio for UDP.
<code>-t <mode></code>	It means to enable/disable Outbound TCP ACK Prioritize. 0: disable 1: enable
<code>-V</code>	Show all the settings.
<code>-D</code>	Set all to factory default (for all WANs).
<code>[...]</code>	It means that you can type in several commands in one line.

Example

```
> 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> | ... ]
```

Syntax Description

Parameter	Description
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-h	Type it to display the usage of this command.
-c <no>	Specify the inde number for the class. Available value for <no> contains 1, 2 and 3. The default setting is class 1.
-n <name>	It means to type a name for the class.
-a	It means to add rule for specified class.
-e <no>	It means to edit specified rule. <no>: type the index number for the rule.
-d <no>	It means to delete specified rule. <no>: type the index number for the rule.
-m <mode>	It means to enable or disable the specified rule. 0: disable, 1: enable
-l <addr>	Set the local address. <i>Addr1</i> - It means Single address. Please specify the IP address directly, for example, "-l 172.16.3.9". <i>addr1:addr2</i> - It means Range address. Please specify the IP addresses, for example, "-l 172.16.3.9: 172.16.3.50." <i>addr1:subnet</i> - It means the subnet address with start IP address. Please type the subnet and the IP address, for example, "-l 172.16.3.9:255.255.0.0". <i>any</i> - It means Any address. Simple type "-" to specify any address for this command.
-r <addr>	Set the remote address. <i>addr1</i> - It means Single address. Please specify the IP address directly, for example, "-l 172.16.3.9". <i>addr1:addr2</i> - It means Range address. Please specify the IP addresses, for example, "-l 172.16.3.9: 172.16.3.50."

	<p><i>addr1:subnet</i> - It means the subnet address with start IP address. Please type the subnet and the IP address, for example, "<i>-l 172.16.3.9:255.255.0.0</i>".</p> <p><i>any</i> - It means Any address. Simple type "<i>-l</i>" to specify any address for this command.</p>
<i>-p <DSCP id></i>	Specify the ID.
<i>-s <Service type></i>	<p>Specify the service type by typing the number. The available types are listed as below:</p> <p>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:NNTTP 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</p>
<i>-S <d/s></i>	Show the content for specified DSCP ID/Service type.
<i>-V <1/2/3></i>	Show the rule in the specified class.
<i>[...]</i>	It means that you can type in several commands in one line.

Example

```
> qos class -c 2 -n draytek -a -m 1 -l 192.168.1.50:192.168.1.80

Following setting will set in the class2
class 2 name set to draytek
Add a rule in class2
Class2 the 1 rule enabled
Set local address type to Range, 192.168.1.50:192.168.1.80
```

Telnet Command: qos type

This command allows user to configure protocol type and port number for QoS.

Syntax

`qos type [-a <service name> | -e <no> | -d <no>].`

Syntax Description

Parameter	Description
<i>-a <name></i>	It means to add rule.
<i>-e <no></i>	It means to edit user defined service type. "no" means the index number. Available numbers are 1-40.
<i>-d <no></i>	It means to delete user defined service type. "no" means the index number. Available numbers are 1-40.
<i>-n <name></i>	It means the name of the service.
<i>-t <type></i>	<p>It means protocol type.</p> <p>6: tcp(default) 17: udp 0: tcp/udp <1-254>: other</p>
<i>-p <port></i>	It means service port. The typing format must be [start:end] (ex., 510:330).
<i>-l</i>	List user defined types. "no" means the index number. Available numbers are 1-40.

Example

```
> qos type -a draytek -t 6 -p 510:1330

service name set to draytek
service type set to 6:TCP
Port type set to Range
Service Port set to 510 ~ 1330
>
```

Telnet Command: quit

This command can exit the telnet command screen.

Telnet Command: show lan

This command displays current status of LAN IP address settings.

Example

```
> show lan
The LAN settings:
      ip          mask      dhcp  star_ip      pool  gateway
-----
[V]LAN1 192.168.1.1 255.255.255.0 [V] 192.168.1.10 200
192.168.1.1
[X]LAN2 192.168.2.1 255.255.255.0 [V] 192.168.2.10 100
192.168.2.1
[X]LAN3 192.168.3.1 255.255.255.0 [V] 192.168.3.10 100
192.168.3.1
[X]LAN4 192.168.4.1 255.255.255.0 [V] 192.168.4.10 100
192.168.4.1
[X]LAN5 192.168.5.1 255.255.255.0 [V] 192.168.5.10 100
192.168.5.1
[X]LAN6 192.168.6.1 255.255.255.0 [V] 192.168.6.10 100
192.168.6.1
[X]Route 192.168.0.1 255.255.255.0 [V] 0.0.0.0 0 192.168.0.1
```

Telnet Command: show dmz

This command displays current status of DMZ host.

Example

```
> show dmz
%      WAN1 DMZ mapping status:
Index  Status  WAN1 aux IP    Private IP
-----
1      Disable 172.16.3.221
2      Disable 192.168.1.65
```

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

```
> show openport
%%     Openport settings:
Index  Status  Comment          Local IP Address
*****
No data entry.
```

Telnet Command: show nat

This command displays current status of NAT.

Example

```
> show nat
Port Redirection Running Table:

Index  Protocol  Public Port  Private IP    Private Port
1      0          0           0.0.0.0       0
2      0          0           0.0.0.0       0
3      0          0           0.0.0.0       0
4      0          0           0.0.0.0       0
5      0          0           0.0.0.0       0
6      0          0           0.0.0.0       0
7      0          0           0.0.0.0       0
8      0          0           0.0.0.0       0
9      0          0           0.0.0.0       0
10     0          0           0.0.0.0       0
```

11	0	0	0.0.0.0	0
12	0	0	0.0.0.0	0
13	0	0	0.0.0.0	0
14	0	0	0.0.0.0	0
15	0	0	0.0.0.0	0
16	0	0	0.0.0.0	0
17	0	0	0.0.0.0	0
18	0	0	0.0.0.0	0
19	0	0	0.0.0.0	0
20	0	0	0.0.0.0	0
--- MORE --- ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]				

Telnet Command: show portmap

This command displays the table of NAT Active Sessions.

Example

```
> show portmap
-----
-
Private_IP:Port Pseudo_IP:Port Peer_IP:Port [Timeout/Protocol/Flag]
-----
-
```

Telnet Command: show pmtime

This command displays the reuse time of NAT session.

Level0: It is the default setting.

Level1: It will be applied when the NAT sessions are smaller than 25% of the default setting.

Level2: It will be applied when the NAT sessions are smaller than the eighth of the default setting.

Example

```
> show pmtime
Level0 TCP=86400001 UDP=300001 ICMP=10001
Level1 TCP=600000 UDP=90000 ICMP=7000
Level2 TCP=60000 UDP=30000 ICMP=5000
```

Telnet Command: show session

This command displays current status of current session.

Example

```
> show session
% Maximum Session Number: 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.

Example

```
> 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
Enable:Yes      Line:xDSL      Name:tcom
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
Mode:                  State:TRAINING  TX Block:0      RX Block:0
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 bps
DS Attainable Rate :      0 bps    US Attainable Rate :      0 bps
DS Path Mode      :      Fast    US Path Mode      :      Fast
DS Interleave Depth :      0      US Interleave Depth :      0
NE Current Attenuation :      0 dB    Cur SNR Margin    :      0 dB
DS actual PSD     :      0.0 dB    US actual PSD     :      0.0 dB
ADSL Firmware Version : 05-04-04-04-00-01
----- ATU-C Info -----
Far Current Attenuation :      0 dB    Far SNR Margin    :      0 dB
CO ITU Version[0]      : 00000000    CO ITU Version[1] : 00000000
DSLAM CHIPSET VENDOR  : < ADI >
```

Telnet Command: show statistic

This command displays statistics for WAN interface.

Syntax

show statistic

show statistic reset *[interface]*

Syntax Description

Parameter	Description
<i>reset</i>	It means to reset the transmitted/received bytes to Zero.
<i>interface</i>	It means to specify WAN1 -WAN5 (including multi-PVC) interface for displaying related statistics.

Example

```
> show statistic
WAN1 total TX: 0 Bytes ,RX: 0 Bytes
WAN2 total TX: 0 Bytes ,RX: 0 Bytes
WAN3 total TX: 0 Bytes ,RX: 0 Bytes
WAN4 total TX: 0 Bytes ,RX: 0 Bytes
WAN5 total TX: 0 Bytes ,RX: 0 Bytes
>
```

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-XX]`

`srv dhcp public del [MAC Addr XX-XX-XX-XX-XX-XX/all/ALL]`

Syntax Description

Parameter	Description
<i>start</i>	It means the starting point of the IP address pool for the DHCP server.
<i>IP address</i>	It means to specify an IP address as the starting point in the IP address pool.
<i>cnt</i>	It means the IP count number.
<i>IP counts</i>	It means to specify the number of IP addresses in the pool. The maximum is 10.
<i>status</i>	It means the execution result of this command.
<i>add</i>	It means creating a list of hosts to be assigned.
<i>del</i>	It means removing the selected MAC address.
<i>MAC Addr</i>	It means to specify MAC Address of the host.
<i>all/ALL</i>	It means all of the MAC addresses.

Example

```
Vigor> ip route add 192.168.1.56 255.255.255.0 192.168.1.12 3 default
Vigor> srv dhcp public status
Index  MAC Address
```

Telnet Command: `srv dhcp dns1`

This command allows users to set Primary IP Address for DNS Server in LAN.

Syntax

`srv dhcp dns1 [?]`

`srv dhcp dns1 [DNS IP address]`

Syntax Description

Parameter	Description
<code>?</code>	It means to display current IP address of DNS 1 for the DHCP server.
<code>DNS IP address</code>	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
<code>?</code>	It means to display current IP address of DNS 2 for the DHCP server.
<code>DNS IP address</code>	It means the IP address that you want to use as DNS2. Note: The IP Routed Subnet DNS must be the same as NAT Subnet DNS).

Example

```
> srv dhcp dns2 10.1.1.1
% srv dhcp dns2 <DNS IP address>
% Now: 10.1.1.1
(IP Routed Subnet dns same as NAT Subnet dns)
```


Telnet Command: `srv dhcp frcdnsmanl`

This command can force the router to invoke DNS Server IP address.

Syntax

```
srv dhcp frcdnsmanl [on]
```

```
srv dhcp frcdnsmanl [off]
```

Syntax Description

Parameter	Description
<code>?</code>	It means to display the current status.
<code>on</code>	It means to use manual setting for DNS setting.
<code>Off</code>	It means to use auto settings acquired from ISP.

Example

```
> srv dhcp frcdnsmanl on
% Domain name server now is using manual settings!
> srv dhcp frcdnsmanl off
% Domain name server now is using auto settings!
```

Telnet Command: `srv dhcp gateway`

This command allows users to specify gateway address for DHCP server.

Syntax

```
srv dhcp gateway [?]
```

```
srv dhcp gateway [Gateway IP]
```

Syntax Description

Parameter	Description
<code>?</code>	It means to display current gateway that you can use.
<code>Gateway IP</code>	It means to specify a gateway address used for DHCP server.

Example

```
> srv dhcp gateway 192.168.2.1
This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

Telnet Command: `srv dhcp ipcnt`

This command allows users to specify IP counts for DHCP server.

Syntax

```
srv dhcp ipcnt [?]
```

```
srv dhcp ipcnt [IP counts]
```

Syntax Description

Parameter	Description
<i>?</i>	It means to display current used IP count number.
<i>IP counts</i>	It means the number that you have to specify for the DHCP server.

Example

```
> srv dhcp ipcnt ?
% srv dhcp ipcnt <IP counts>
% Now: 150
```

Telnet Command: `srv dhcp off`

This function allows users to turn off DHCP server. It needs rebooting router, please type "sys reboot" command to reboot router.

Telnet Command: `srv dhcp on`

This function allows users to turn on DHCP server. It needs rebooting router, please type "sys reboot" command to reboot router.

Telnet Command: `srv dhcp relay`

This command allows users to set DHCP relay setting.

Syntax

```
srv dhcp relay servip [server ip]
```

```
srv dhcp relay subnet [index]
```

Syntax Description

Parameter	Description
<i>server ip</i>	It means the IP address that you want to used as DHCP server.
<i>Index</i>	It means subnet 1 or 2. Please type 1 or 2. The router will invoke this function according to the subnet 1 or 2 specified here.

Example

```
> srv dhcp relay servip 192.168.1.46
> srv dhcp relay subnet 2
> srv dhcp relay servip ?
% srv dhcp relay servip <server ip>
% Now: 192.168.1.46
```

Telnet Command: `srv dhcp startip`

Syntax

`srv dhcp startip [?]`

`srv dhcp startip [IP address]`

Syntax Description

Parameter	Description
<code>?</code>	It means to display current used start IP address.
<code>IP address</code>	It means the IP address that you can specify for the DHCP server as the starting point.

Example

```
> srv dhcp startip 192.168.1.53
This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

Telnet Command: `srv dhcp status`

This command can display general information for the DHCP server, such as IP address, MAC address, leased time, host ID and so on.

Example

```
> srv dhcp status
DHCP server: Relay Agent
Default gateway: 192.168.1.1
Index   IP Address      MAC Address      Leased Time      HOST ID
1       192.168.1.113  00-05-5D-E4-D8-EE  17:20:08        A1000351
```

Telnet Command: `srv dhcp leasetime`

This command can set the lease time for the DHCP server.

Syntax

`srv dhcp leasetime [?]`

`srv dhcp leasetime [Lease Time (sec)]`

Syntax Description

Parameter	Description
<code>?</code>	It means to display current leasetime used for the DHCP server.
<code>Lease Time (sec)</code>	It means the lease time that DHCP server can use. The unit is second.

Example

```
> srv dhcp leasetime ?
% srv dhcp leasetime <Lease Time (sec.)>
% Now: 86400
>
```

Telnet Command: `srv dhcp nodetype`

This command can set the node type for the DHCP server.

Syntax

`srv dhcp nodetype <count>`

Syntax Description

Parameter	Description
<code>count</code>	It means to specify a type for node. 1. B-node 2. P-node 4. M-node 8. H-node

Example

```
> srv dhcp nodetype 1
> srv dhcp nodetype ?
%% srv dhcp nodetype <count>
%% 1. B-node 2. P-node 4. M-node 8. H-node
% Now: 1
```

Telnet Command: `srv dhcp primWINS`

This command can set the primary IP address for the DHCP server.

Syntax

```
srv dhcp primWINS [WINS IP address]
```

```
srv dhcp primWINS clear
```

Syntax Description

Parameter	Description
<i>WINS IP address</i>	It means the IP address of primary WINS server.
<i>clear</i>	It means to remove the IP address settings of primary WINS server.

Example

```
> srv dhcp primWINS 192.168.1.88
> srv dhcp primWINS ?
%% srv dhcp primWINS <WINS IP address>
%% srv dhcp primWINS clear
% Now: 192.168.1.88
```

Telnet Command: `srv dhcp secWINS`

This command can set the secondary IP address for the DHCP server.

Syntax

```
srv dhcp secWINS [WINS IP address]
```

```
srv dhcp secWINS clear
```

Syntax Description

Parameter	Description
<i>WINS IP address</i>	It means the IP address of secondary WINS server.
<i>clear</i>	It means to remove the IP address settings of second WINS server.

Example

```
> srv dhcp secWINS 192.168.1.180
> srv dhcp secWINS ?
%% srv dhcp secWINS <WINS IP address>
%% srv dhcp secWINS clear
% Now: 192.168.1.180
```

Telnet Command: `srv dhcp expired_RecycleIP`

This command can set the time to check if the IP address can be assigned again by DHCP server or not.

Syntax

`srv dhcp expRecycleIP <sec time>`

Syntax Description

Parameter	Description
<i>sec time</i>	It means to set the time (5-300 seconds) for checking if the IP can be assigned again or not.

Example

```
Vigor> srv dhcp expRecycleIP 250
% DHCP expired_RecycleIP = 250
```

Telnet Command: `srv dhcp tftp`

This command can set the TFTP server as the DHCP server.

Syntax

`srv dhcp tftp <TFTP server name>`

Syntax Description

Parameter	Description
<i>TFTP server name</i>	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 unumber]`

Syntax Description

Parameter	Description
<i>-h</i>	It means to display usage of this command.
<i>-l</i>	It means to display all the user defined DHCP options.
<i>-d[idx]</i>	It means to delete the option number by specifying its index number.
<i>-e [1 or 0]</i>	It means to enable/disable custom option feature. 1:enable 0:disable
<i>-c</i>	It means to set option number. Available number ranges from 0 to 255.
<i>-v</i>	It means to set option number by typing string.
<i>-a</i>	It means to set the option value by specifying the IP address.
<i>-x</i>	It means to set option number with the format of Hexadecimal characters.
<i>-u</i>	It means to update the option value of the sepecified index.
<i>idx number</i>	It means the index number of the option value.

Example

```

> srv dhcp option -e 1 -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
<i>n</i>	It means to map selected WAN IP to certain host. 1: wan1 2: wan2
<i>m</i>	It means the index number of the DMZ host. Default setting is "1" (WAN 1). It is only available for Static IP mode. If you use other mode, you can set 1 ~ 8 in this field. If WAN IP alias has been configured, then the number of DMZ host can be added more.
<i>[<command> <parameter> ...]</i>	The available commands with parameters are listed below. <i>[...]</i> means that you can type in several commands in one line.
<i>-e</i>	It means to enable/disable such feature. 1:enable 0:disable
<i>-i</i>	It means to specify the private IP address of the DMZ host.
<i>-r</i>	It means to remove DMZ host setting.
<i>-v</i>	It means to display current status.

Example

```
> srv nat dmz 1 1 -i 192.168.1.96
> srv nat dmz -v
%      WAN1 DMZ mapping status:
Index  Status  WAN1 aux IP    Private IP
-----
1      Disable  0.0.0.0 192.168.1.96
```

Telnet Command: `srv nat ipsecpass`

This command allows users to enable or disable IPSec ESP tunnel passthrough and IKE source port (500) preservation.

Syntax

`srv nat ipsecpass [options]`

Syntax Description

Parameter	Description
<i>[options]</i>	The available commands with parameters are listed below.
<i>on</i>	It means to enable IPSec ESP tunnel passthrough and IKE source port (500) preservation.
<i>off</i>	It means to disable IPSec ESP tunnel passthrough and IKE source port (500) preservation.

<i>status</i>	It means to display current status for checking.
---------------	--

Example

```
> srv nat ipsecpass status
%% Status: IPsec ESP pass-thru and IKE src_port:500 preservation is OFF.
```

Telnet Command: `srv nat openport`

This command allows users to set open port settings for NAT server.

Syntax

```
srv nat openport n m [-<command> <parameter> | ... ]
```

Syntax Description

Parameter	Description
<i>n</i>	It means the index number for the profiles. The range is from 1 to 20.
<i>m</i>	It means to specify the sub-item number for this profile. The range is from 1 to 10.
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-a <enable>	It means to enable or disable the open port rule profile. 0: disable 1:enable
-c <comment>	It means to type the description (less than 23 characters) for the defined network service.
-i <local ip>	It means to set the IP address for local computer. Local ip: Type an IP address in this field.
-w <idx>	It means to specify the public IP. 1: WAN1 Default, 2: WAN1 Alias 1, ...and so on.
-p <protocol>	Specify the transport layer protocol. Available values are TCP, UDP and ALL.
-s<start port>	It means to specify the starting port number of the service offered by the local host. The range is from 0 to 65535.
-e<end port>	It means to specify the ending port number of the service offered by the local host. The range is from 0 to 65535.
-v	It means to display current settings.
-r <remove>	It means to delete the specified open port setting. remove: Type the index number of the profile.
-f <flush>	It means to return to factory settings for all the open ports profiles.

Example

```
> srv nat openport 1 1 -a 1 -c games -i 192.168.1.100 -w 1 -p TCP -s
23 -e 83
> srv nat openport -v
```

```

%% Status: Enable
%% Comment: games
%% Private IP address: 192.168.1.100
Index  Protocol      Start Port    End Port
*****
  1.    TCP          23           83

%% Status: Disable
%% Comment:
%% Private IP address: 0.0.0.0
Index  Protocol      Start Port    End Port
*****

%% Status: Disable
%% Comment:
%% Private IP address: 0.0.0.0
Index  Protocol      Start Port    End Port
*****
>

```

Telnet Command: `srv nat portmap`

This command allows users to set port redirection table for NAT server.

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`

Syntax Description

Parameter	Description
<i>Add[idx]</i>	It means to add a new port redirection table with an index number. Available index number is from 1 to 10.
<i>serv name</i>	It means to type one name as service name.
<i>proto</i>	It means to specify TCP or UDP as the protocol.
<i>pub port</i>	It means to specify which port can be redirected to the specified Private IP and Port of the internal host.
<i>pri ip</i>	It means to specify the private IP address of the internal host providing the service.
<i>pri port</i>	It means to specify the private port number of the service offered by the internal host.
<i>wan1/wan2</i>	It means to specify WAN interface for the port redirection.
<i>del [idx]</i>	It means to remove the selected port redirection setting.
<i>disable [idx]</i>	It means to inactivate the selected port redirection setting.
<i>enable [idx]</i>	It means to activate the selected port redirection setting.
<i>flush</i>	It means to clear all the port mapping settings.

table

It means to display Port Redirection Configuration Table.

Example

```
> srv nat portmap add 1 game tcp 80 192.168.1.11 100 wan1
> srv nat portmap table
```

NAT Port Redirection Configuration Table:

Index	Service Name	Protocol	Public Port	Private IP	Private Port
1	game	6	80	192.168.1.11	100
-1					
2		0	0		0
3		0	0		0
4		0	0		0
5		0	0		0
6		0	0		0
7		0	0		0
8		0	0		0
9		0	0		0
10		0	0		0
11		0	0		0
12		0	0		0
13		0	0		0
14		0	0		0
15		0	0		0
16		0	0		0
17		0	0		0
18		0	0		0
19		0	0		0
20		0	0		0

Protocol: 0 = Disable, 6 = TCP, 17 = UDP

Telnet Command: `srv nat status`

This command allows users to view NAT Port Redirection Running Table.

Example

```
> srv nat status
```

NAT Port Redirection Running Table:

Index	Protocol	Public Port	Private IP	Private Port
1	6	80	192.168.1.11	100
2	0	0	0.0.0.0	0
3	0	0	0.0.0.0	0
4	0	0	0.0.0.0	0

5	0	0	0.0.0.0	0
6	0	0	0.0.0.0	0
7	0	0	0.0.0.0	0
8	0	0	0.0.0.0	0
9	0	0	0.0.0.0	0
10	0	0	0.0.0.0	0
11	0	0	0.0.0.0	0
12	0	0	0.0.0.0	0
13	0	0	0.0.0.0	0
14	0	0	0.0.0.0	0
15	0	0	0.0.0.0	0
16	0	0	0.0.0.0	0
17	0	0	0.0.0.0	0
18	0	0	0.0.0.0	0
19	0	0	0.0.0.0	0
20	0	0	0.0.0.0	0
--- MORE --- ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]				

Telnet Command: `srv nat showall`

This command allows users to view a summary of NAT port redirection setting, open port and DMZ settings.

Example

```
> srv nat showall ?
Index  Proto  WAN IP:Port          Private IP:Port      Act
*****
****
R01    TCP    0.0.0.0:80         192.168.1.11:100    Y
O01    TCP    0.0.0.0:23~83     192.168.1.100:23~83 Y
D01    All    0.0.0.0           192.168.1.96       Y

R:Port Redirection, O:Open Ports, D:DMZ
```

Telnet Command: `switch -i`

This command is used to obtain the TX (transmitted) or RX (received) data for each connected switch.

Syntax

`switch -i [switch_idx_no] [option]`

Syntax Description

Parameter	Description
<i>switch_idx_no</i>	It means the index number of the switch profile.
<i>option</i>	The available commands with parameters are listed below. <i>cmd</i> <i>acc</i>

	<i>traffic [on/off/status/tx/rx]</i>
<i>cmd</i>	It means to send command to the client.
<i>acc</i>	It means to set the client authentication account and password.
<i>traffic [on/off/status/tx/rx]</i>	It means to turn on/off or display the data transmission from the client.

Example

```
> switch -i 1 traffic on
External Device NO. 1 traffic statistic function is enable
```

Telnet Command: switch on

This command is used to turn on the auto discovery for external devices.

Example

```
> switch on
Enable Extrnal Device auto discovery!
```

Telnet Command: switch off

This command is used to turn off the auto discovery for external devices.

Example

```
> switch off
Disable External Device auto discovery!
```

Telnet Command: switch list

This command is used to display the connection status of the switch.

Example

```
> switch list?
No.      Mac                IP           status   Dur Time   Model_Name
-----
[1] 00-50-7f-cd-07-48 192.168.1.3  On-Line  00:01:01
Vigor2920 Series
```

Telnet Command: switch clear

This command is used to reset the switch table and reboot the router.

Syntax

switch clear [*idx*]

Syntax Description

Parameter	Description
<i>idx</i>	It means the index number of each item shown on the table. The range is from 1 to 8.
<i>-f</i>	It means to clear all of the data.

Example

```
> switch clear 1
Switch Data clear successful

> switch clear -f
Switch Data clear successful
```

Telnet Command: switch query

This command is used to enable or disable the switch query.

Example

```
> switch query on
Extern Device status query is Enable

> switch query off
Extern Device status query is Disable
```

Telnet Command: sys admin

This command is used for RD engineer to access into test mode of Vigor router.

Telnet Command: sys adminuser

This command is used to create user account 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
<i>option</i>	Available options includes: Local [0-1] LDAP [0-1] edit [INDEX] delete [INDEX] view [INDEX]
<i>Local [0-1]</i>	0 - Disable the local user. 1 - Enable the local user.
<i>LDAP [0-1]</i>	0 - Disable the LDAP. 1 - Enable the LDAP.
<i>edit [INDEX] username password</i>	Edit an existed user account or create a new local user account. [INDEX] - 1 ~8. There are eight profiles to be added / edited. Username - Type a new name for local user. Password - Type a password for local user.
<i>delete [INDEX]</i>	Delete a local user account.
<i>view [INDEX]</i>	Show the user account/password detail information.

Example

```
> > sys adminuser Local 1
```

```

Local User has enabled!
> sys adminuser 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
<code>-e <enable></code>	It is used to disable/enable bonjour service (0: disable, 1: enable).
<code>-h <enable></code>	It is used to disable/enable http (web) service (0: disable, 1: enable).
<code>-t <enable></code>	It is used to disable/enable telnet service (0: disable, 1: enable).
<code>-f <enable></code>	It is used to disable/enable FTP service (0: disable, 1: enable).
<code>-s <enable></code>	It is used to disable/enable SSH service (0: disable, 1: enable).
<code>-p <enable></code>	It is used to disable/enable printer service (0: disable, 1: enable).
<code>-6 <enable></code>	It is used to disable/enable IPv6 (0: disable, 1: enable).

Example

```

> sys bonjour -s 1
>

```

Telnet Command: sys cfg

This command reset the router with factory default settings. When a user types this command, all the configuration will be reset to default setting.

Syntax

sys cfg default

sys cfg status

Syntax Description

Parameter	Description
<i>default</i>	It means to reset current settings with default values.
<i>status</i>	It means to display current profile version and status.

Example

```
> sys cfg status
Profile version: 3.0.0   Status: 1 (0x491e5e6c)
> sys cfg default
>
```

Telnet Command: sys cmdlog

This command displays the history of the commands that you have typed.

Example

```
> sys cmdlog
% Commands Log: (The lowest index is the newest !!!)
 [1] sys cmdlog
 [2] sys cmdlog ?
 [3] sys ?
 [4] sys cfg status
 [5] sys cfg ?
```

Telnet Command: sys ftpd

This command displays current status of FTP server.

Syntax

sys ftpd *on*

sys ftpd *off*

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on the FTP server of the system.
<i>off</i>	It means to turn off the FTP server of the system.

Example

```
> sys ftpd on
% sys ftpd turn on !!!
```


Telnet Command: sys domainname

This command can set and remove the domain name of the system when DHCP mode is selected for WAN.

Syntax

sys domainname [*wan1/wan2*] [*Domain Name Suffix*]

sys domainname [*wan1/wan2*] clear

Syntax Description

Parameter	Description
<i>wan1/wan2</i>	It means to specify WAN interface for assigning a name for it.
<i>Domain Name Suffix</i>	It means the name for the domain of the system. The maximum number of characters that you can set is 40.
<i>clear</i>	It means to remove the domain name of the system.

Example

```
> sys domainname wan1 clever
> sys domainname wan2 intellegent
> sys domainname ?
% sys domainname <wan1/wan2> <Domain Name Suffix (max. 40 characters)>
% sys domainname <wan1/wan2> clear
% Now: wan1 == clever, wan2 ==intelligent
>
```

Telnet Command: sys iface

This command displays the current interface connection status (UP or Down) with IP address, MAC address and Netmask for the router.

Example

```
> sys iface
Interface 0 Ethernet:
Status: UP
IP Address: 192.168.1.1      Netmask: 0xFFFFFFFF00 (Private)
IP Address: 0.0.0.0        Netmask: 0xFFFFFFFF
MAC: 00-50-7F-00-00-00
Interface 4 Ethernet:
Status: DOWN
IP Address: 0.0.0.0        Netmask: 0x00000000
MAC: 00-50-7F-00-00-02
Interface 5 Ethernet:
Status: DOWN
IP Address: 0.0.0.0        Netmask: 0x00000000
MAC: 00-50-7F-00-00-03
Interface 6 Ethernet:
Status: DOWN
IP Address: 0.0.0.0        Netmask: 0x00000000
MAC: 00-50-7F-00-00-04
```

```

Interface 7 Ethernet:
Status: DOWN
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-05
Interface 8 Ethernet:
Status: DOWN
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-06

Interface 9 Ethernet:
Status: DOWN
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-07
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
>

```

Telnet Command: sys name

This command can set and remove the name for the router when DHCP mode is selected for WAN.

Syntax

`sys name [wan1] [ASCII string]`

`sys name [wan1] clear`

Syntax Description

Parameter	Description
<i>wan1</i>	It means to specify WAN interface for assigning a name for it.
<i>ASCII string</i>	It means the name for router. The maximum character that you can set is 20.

Example

```

> sys name wan1 drayrouter
> sys name ?
% sys name <wan1/wan2> <ASCII string (max. 20 characters)>
% sys name <wan1/wan2> clear
% Now: wan1 == drayrouter, wan2 ==

```

Note: Such name can be used to recognize router's identification in SysLog dialog.

Telnet Command: sys passwd

This command allows users to set password for the administrator.

`sys passwd [ASCII string]`

Syntax Description

Parameter	Description
<i>ASCII string</i>	It means the password for administrator. The maximum character that you can set is 23.

Example

```
> sys passwd admin123
>
```

Telnet Command: sys reboot

This command allows users to restart the router immediately.

Example

```
> sys reboot
>
```

Telnet Command: sys autoreboot

This command allows users to restart the router automatically within a certain time.

Syntax

`sys autoreboot [on/off/hour(s)]`

Syntax Description

Parameter	Description
<i>on/off</i>	On - It means to enable the function of auto-reboot. Off - It means to disable the function of auto-reboot.
<i>hours</i>	It means to set the time schedule for router reboot. For example, if you type "2" in this field, the router will reboot with an interval of two hours.

Example

```
> sys autoreboot on
autoreboot is ON
> sys autoreboot 2
autoreboot is ON
autoreboot time is 2 hour(s)
```

Telnet Command: sys commit

This command allows users to save current settings to FLASH. Usually, current settings will be saved in SRAM. Yet, this command will save the file to FLASH.

Example

```
> sys commit
```

```
>
```

Telnet Command: sys tftpd

This command can turn on TFTP server for upgrading the firmware.

Example

```
> sys tftpd
% TFTP server enabled !!!
```

Telnet Command: sys cc

This command can display current country code and wireless region of this device.

Example

```
> sys cc
Country Code      : 0x 0 [International]
Wireless Region Code: 0x30
>
```

Telnet Command: sys version

This command can display current version for the system.

Example

```
> sys version
Router Model: Vigor2862Vn+   Version: 3.7.4.1 English
Profile version: 3.0.0      Status: 1 (0x49165e6c)
Router IP: 192.168.1.1     Netmask: 255.255.255.0
Firmware Build Date/Time: Mar 20 2014 14:09:50
Router Name: drayrouter
Revision: 40055 2860_374
VDSL2 Firmware Version: 05-04-08-00-00-06
```

Telnet Command: sys qrybuf

This command can display the system memory status and leakage list.

Example

```
> sys qrybuf
System Memory Status and Leakage List

Buf sk_buff ( 200B), used#: 1647, cached#: 30
Buf KMC4088 (4088B), used#: 0, cached#: 8
Buf KMC2552 (2552B), used#: 1641, cached#: 42
Buf KMC1016 (1016B), used#: 7, cached#: 1
Buf KMC504 ( 504B), used#: 8, cached#: 8
Buf KMC248 ( 248B), used#: 26, cached#: 22
Buf KMC120 ( 120B), used#: 67, cached#: 61
Buf KMC56 ( 56B), used#: 20, cached#: 44
Buf KMC24 ( 24B), used#: 58, cached#: 70
```

```
Dynamic memory: 13107200B; 4573168B used; 190480B/0B in level 1/2 cache.
```

```
FLOWTRACK Memory Status  
# of free = 12000  
# of maximum = 0  
# of flowstate = 12000  
# of lost by signature = 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]
```

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on pulling buffer.
<i>off</i>	It means to turn off pulling buffer.

Example

```
> sys pollbuf on  
% Buffer polling is on!  
  
> sys pollbuf off  
% Buffer polling is off!
```

Telnet Command: sys britask

This command can improve triple play quality.

Syntax

```
sys britask [on]
```

```
sys britask [off]
```

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on the bridge task for improving the triple play quality.
<i>off</i>	It means to turn off the bridge task.

Example

```
> sys britask on  
% bridge task is ON, now
```

Telnet Command: sys tr069

This command can set CPE settings for applying in VigorACS.

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]
```

Syntax Description

Parameter	Description
<i>get [parm] [option]</i>	It means to get parameters for tr-069. option=<nextlevel>: only gets nextlevel for GetParameterNames.
<i>set [parm] [value]</i>	It means to set parameters for tr-069.
<i>getnoti [parm]</i>	It means to get parameter notification value.
<i>setnoti [parm] [value]</i>	It means to set parameter notification value.
<i>log</i>	It means to display the TR-069 log.
<i>debug [on/off]</i>	on: turn on the function of sending debug message to syslog. off: turn off the function of sending debug message to syslog.
<i>save</i>	It means to save the parameters to the flash memory of the router.
<i>Inform [event code]</i>	It means to inform parameters for tr069 with different event codes. [event code] includes: 0-"0 BOOTSTRAP", 1-"1 BOOT", 2-"2 PERIODIC", 3-"3 SCHEDULED", 4-"4 VALUE CHANGE", 5-"5 KICKED", 6-"6 CONNECTION REQUEST", 7-"7 TRANSFER COMPLETE", 8-"8 DIAGNOSTICS COMPLETE", 9-"M Reboot"
<i>port [port num]</i>	It means to change tr069 listen port number.
<i>cert_auth [on/off]</i>	on: turn on certificate-based authentication. off: turn off certificate-based authentication.

Example

```
> sys tr069 get Int. nextlevel
Total number of parameter is 24
```

```

Total content length of parameter is 915
InternetGatewayDevice.LANDeviceNumberOfEntries
InternetGatewayDevice.WANDeviceNumberOfEntries
InternetGatewayDevice.DeviceInfo.
InternetGatewayDevice.ManagementServer.
InternetGatewayDevice.Time.
InternetGatewayDevice.Layer3Forwarding.
InternetGatewayDevice.LANDevice.
InternetGatewayDevice.WANDevice.
InternetGatewayDevice.Services.
InternetGatewayDevice.X_00507F_InternetAcc.
InternetGatewayDevice.X_00507F_LAN.
InternetGatewayDevice.X_00507F_NAT.
InternetGatewayDevice.X_00507F_Firewall.
InternetGatewayDevice.X_00507F_Bandwidth.
InternetGatewayDevice.X_00507F_Applications.
InternetGatewayDevice.X_00507F_VPN.
InternetGatewayDevice.X_00507F_VoIP.
InternetGatewayDevice.X_00507F_WirelessLAN.
InternetGatewayDevice.X_00507F_System.
InternetGatewayDevice.X_00507F_Status.

InternetGatewayDevice.X_00507F_Diagnostics.
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
```

Telnet Command: sys sip_alg

This command can turn on/off SIP ALG (Application Layer Gateway) for traversal.

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*

Syntax Description

Parameter	Description
<i>licmsg</i>	It means to display license message.
<i>licauth</i>	It means the license authentication time setting.
<i>regser</i>	It means the license register server setting.
<i>licera</i>	It means to erase license setting.
<i>licifno</i>	It means license and signature download interface setting.
<i>lic_wiz</i> [<i>set/reg/qry</i>]	It means the license wizard setting. qry: query service support status set [idx] [trial] [service type] [sp_id] [start_date] [License Key] reg: register service in portal
<i>dev_chg</i>	It means to change the device key.
<i>dev_key</i>	It means to show device key.

Example

```
> sys license licifno

License and Signature download interface setting:
licifno [AUTO/WAN#]

Ex: licifno wan1

Download interface is "auto-selected" now.
```


Telnet Command: sys diag_log

This command is used for RD debug.

Syntax

`sys diag_log [status| enable| disable| flush| lineno [w] | level [x] | feature [on/off] [y]/ log]`

Syntax Description

Parameter	Description
<i>status</i>	It means to show the status of diagnostic log.
<i>enable</i>	It means to enable the function of diag_log.
<i>disable</i>	It means to disenable the function of diag_log.
<i>flush</i>	It means the flush log buffer.
<i>lineno [w]</i>	It means the total lines for displaying message. w - Available value ranges from 100 to 50000.
<i>level[x]</i>	It determines the level of data displayed. x - Available value ranges from 0 to 12. The larger the number is, the detailed the data is displayed.
<i>feature [on/off][y]</i>	It is used to specify the function of the log. Supported features include SYS and DSL (Case-Insensitive). Default setting is "on" for "DSL".
<i>voip_feature [on/off][vf_name]</i>	It means VoIP feature. Type on to enable the feature or type off to disable the feature. vf_name: available settings include DRVTAPI, DRVMMC, DRVMPS, DRVFXO, DRVHAL, PSMPHONE, PSMSUPP, PSM, FXO, PSMISDN, DTMFPSE, CALLERID (Case-Insensitive).
<i>log</i>	It means the dump log buffer.

Example

```
> sys diag_log status
Status:
diag_log is Enabled.
lineno : 10000.
level : 3.
Enabled feature: SYS DSL
> sys diag_log log
0:00:02 [DSL] Current modem firmware: AnnexA_548006_544401
0:00:02 [DSL] Modem firmware feature: 5, ADSL_A, VDSL2
0:00:02 [DSL] xtseCfg=04 00 04 00 0c 01 00 07
0:00:02 [DSL] don't have last showtime mode!! set next mode to VDSL!!
0:00:02 [DSL] Status has changed: Stopped(0) -> FwWait(3)
0:00:02 [DSL] Status has changed: FwWait(3) -> Starting(1)
0:00:02 [DSL] Status has changed: Starting(1) -> Running(2)
0:00:02 [DSL] Status was switched: firmwareReady(3) to Init(5)
0:00:02 [DSL] Status was switched: Init(5) to Restart(10)
0:00:02 [DSL] Status was switched: Restart(10) to
FirmwareRequest(1)
0:00:02 [DSL] Line state has changed: 00000000 -> 000000FF
0:00:02 [DSL] Entering VDSL2 mode
```

```

0:00:03 [DSL] modem code: [05-04-08-00-00-06]
0:00:05 [DSL] Status was switched: FirmwareRequest(1) to
firmwareReady(3)
0:00:05 [DSL] Status was switched: firmwareReady(3) to Init(5)
0:00:05 [DSL] >> nXtseA=0d, nXtseB=00, nXtseV=07, nFwFeatures=5
0:00:05 [DSL] >> nHsToneGroupMode=0, nHsToneGroup=106,
nToneSet=43, nCamState
=2
0:00:05 [DSL] Line state has changed: 000000FF -> 00000100
0:00:05 [DSL] Line state has changed: 00000100 -> 00000200
0:00:05 [DSL] Status was switched: Init(5) to Train(6)

```

Telnet Command: testmail

This command is used to display current settings for sending test mail.

Example

```

> testmail
Send out test mail
Mail Alert:[Disable]
SMTP_Server:[0.0.0.0]
Mail to:[]
Return-Path:[]

```

Telnet Command: upnp off

This command can close UPnP function.

Example

```

>upnp off
UPNP say bye-bye

```

Telnet Command: upnp on

This command can enable UPnP function.

Example

```

>upnp on
UPNP start.

```

Telnet Command: upnp nat

This command can display IGD NAT status.

Example

```

> upnp nat ?
***** IGD NAT Status *****

((0))
InternalClient >>192.168.1.10<<, RemoteHost >>0.0.0.0<<
InternalPort >>21<<, ExternalPort >>21<<
PortMapProtocol >>TCP<<

```

```

The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
Ftp Example [MICROSOFT]
((1))
InternalClient >>0.0.0.0<<, RemoteHost >>0.0.0.0<<
InternalPort >>0<<, ExternalPort >>0<<
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
0<<

--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---

```

Telnet Command: upnp service

This command can display the information of the UPnP service. UPnP service must be enabled first.

Example

```

> upnp on
UPNP start.

> upnp service
>>>> SERVICE TABLE1 <<<<<
  serviceType urn:schemas-microsoft-com:service:OSInfo:1
  serviceId   urn:microsoft-com:serviceId:OSInfo1
  SCPDURL     /upnp/OSInfo.xml
  controlURL  /OSInfo1
  eventURL    /OSInfoEvent1
  UDN         uuid:774e9bbe-7386-4128-b627-001daa843464

>>>> SERVICE TABLE2 <<<<<
  serviceType
urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1
  serviceId   urn:upnp-org:serviceId:WANCommonIFC1
  SCPDURL     /upnp/WComIFCX.xml
  controlURL  /upnp?control=WANCommonIFC1
  eventURL    /upnp?event=WANCommonIFC1
  UDN         uuid:2608d902-03e2-46a5-9968-4a54ca499148
.
.
.

```

Telnet Command: upnp subscribe

This command can show all UPnP services subscribed.

Example

```

> upnp on
UPNP start.
> upnp subscribe

```

```

Vigor> upnp subscribe
>>>> (1) serviceType urn:schemas-microsoft-com:service:OSInfo:1

----- Subscribtion1 -----

sid = 7a2bbdd0-0047-4fc8-b870-4597b34da7fb

eventKey =1, ToSendEventKey = 1

expireTime =6926

active =1

DeliveryURLs
=<http://192.168.1.113:2869/upnp/eventing/twtnpnsiun>

>>>> (2) serviceType
urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1

----- Subscribtion1 -----

sid = d9cd47a5-d9c9-4d3d-8043-d03a82f27983

eventKey =1, ToSendEventKey = 1

.
.
.

```

Telnet Command: upnp tmpvs

This command can display current status of temp Virtual Server of your router.

Example

```

Vigor> upnp tmpvs
***** Temp virtual server status *****

((0))
real_addr >>192.168.1.10<<, pseudo_addr >>172.16.3.229<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>TCP<<
time >>0<<

((1))
real_addr >>0.0.0.0<<, pseudo_addr >>0.0.0.0<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>0<<
time >>0<<
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---

```

Telnet Command: upnp wan

This command is used to specify WAN interface to apply UPnP.

Syntax

upnp wan [*n*]

Syntax Description

Parameter	Description
<i>n</i>	It means to specify WAN interface to apply UPnP. n=0, it means to auto-select WAN interface. n=1, WAN1 n=2, WAN2

Example

```
> upnp wan 1
use wan1 now.
```

Telnet Command: usb list

This command is use to display the information about the brand name and model name of the USB modems which are supported by Vigor router.

Example

```
> usb list ?
Brand      Module                Standard
-----
Aiko       Aiko 83D              3.5G      Y
BandRich   Bandlux C170          3.5G      Y
BandRich   Bandlux C270          3.5G      Y
BandRich   Bandlux C321          3.5G      Y
BandRich   Bandlux C330          3.5G      Y
BandRich   Bandlux C331          3.5G      Y
BandRich   Bandlux C502          3.5G      Y
Huawei     Huawei E169u          3.5G      Y
Huawei     Huawei E220           3.5G      Y
Huawei     Huawei E303D          3.5G      Y
Huawei     Huawei E392           3.5G      Y
Huawei     Huawei E398           3.5G      Y
Sony Ericsson Sony Ericsson MD30  3.5G      Y
TP-LINK    TP-LINK MA180         3.5G      Y
TP-LINK    TP-LINK MA260         3.5G      Y
Vodafone   Vodafone K3765-Z      3.5G      Y
Vodafone   Vodafone K4605        3.5G      Y
ZTE        ZTE MF626             3.5G      Y
ZTE        ZTE MF627 plus       3.5G      Y
ZTE        ZTE MF633             3.5G      Y
ZTE        ZTE MF636             3.5G      Y
SpinCom    SpinCom GPRS Modem    3.5G      Y
```

```
- MORE - ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] -
```

Telnet Command: `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.

Example

```
> vigbrg status
%Vigor Bridge Function is enable!

%Wan1 management is disable!
```

Telnet Command: vigbrg cfgip

This command allows users to transfer a bridge modem into ADSL router by accessing into and adjusting specified IP address. Users can access into Web UI of the router to manage the router through the IP address configured here.

Syntax

vigbrg cfgip *[IP Address]*

Syntax Description

Parameter	Description
<i>IP Address</i>	It means to type an IP address for users to manage the router.

Example

```
> vigbrg cfgip 192.168.1.15
> vigbrg cfgip ?
% Vigor Bridge Config IP,
% Now: 192.168.1.15
```

Telnet Command: vigbrg wan1on

This command is used to enable the bridge WAN1 management.

Example

```
> vigbrg wan1on
%Enable Vigor Bridge Wan1 management!
```

Telnet Command: vigbrg wan1off

This command is used to disable the bridge WAN1 management.

Example

```
> vigbrg wan1off
%Disable Vigor Bridge Wan1 management!
```

Telnet Command: fullbrg

The command is used to enable Full Bridge Mode so that the router will work as a bridge modem which is able to forward incoming packets with VLAN tags.

Syntax

fullbrg status

fullbrg set -i *[WAN index]* -n *[Subnet index]* -b *[Bridge mode]*

Syntax Description

Parameter	Description
<i>-I [WAN index]</i>	WAN index: Ranges from 1 to 10. 1: WAN1, 2: WAN2, ...etc., In which, WAN3 and WAN 4 are USB WAN.
<i>-n[Subnet index]</i>	Subnet index: Ranges from 1 to 8.

	1: Subnet 1, 2: Subnet 2, ...etc.
-b[Bridge mode]	It means to enable / disable Bridge mode. 0: OFF 1: ON

Example

```

> fullbrg status ?
Show gConfig setting of full bridge
WAN 1 full bridge to LAN 1, mode=OFF.
WAN 2 full bridge to LAN 1, mode=OFF.
WAN 5 full bridge to LAN 1, mode=OFF.
WAN 6 full bridge to LAN 1, mode=OFF.
WAN 7 full bridge to LAN 1, mode=OFF.
WAN 8 full bridge to LAN 1, mode=OFF.
WAN 9 full bridge to LAN 1, mode=OFF.
WAN10 full bridge to LAN 1, mode=OFF.
> fullbrg set -i 2 -n 5 -b 1
Configure OK! Please reboot device to make it effective.
> sys reboot
> fullbrg status
Show gConfig setting of full bridge
WAN 1 full bridge to LAN 1, mode=OFF.
WAN 2 full bridge to LAN 5, mode=ON.
WAN 5 full bridge to LAN 1, mode=OFF.
WAN 6 full bridge to LAN 1, mode=OFF.
WAN 7 full bridge to LAN 1, mode=OFF.
WAN 8 full bridge to LAN 1, mode=OFF.
WAN 9 full bridge to LAN 1, mode=OFF.
WAN10 full bridge to LAN 1, mode=OFF.

```

Telnet Command: voip debug

This command can display debug message on the screen.

Syntax

voip debug [*flush*]

voip debug [*showmsg*]

Syntax Description

Parameter	Description
<i>flush</i>	It means to clear current log.
<i>showmsg</i>	It means to show current log.

Example

```

> voip debug showmsg
-->Send Message to 192.168.1.2:5060 <02:35:16>
INVITE sip:192.168.1.2 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.1:5060;branch=z9hG4bK-YMa-3630;rport
From: <sip:change_me@192.168.1.1>;tag=WLJ-11782
To: <sip:192.168.1.2>

```



```

Call-ID: PbU-25312@192.168.1.1
CSeq: 1 INVITE
Contact: <sip:change_me@192.168.1.1>
Max-Forwards: 70
supported: 100rel, replaces
User-Agent: DrayTek UA-1.2.3 DrayTek Vigor2910
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, INFO, REFER, NOTIFY, PRACK
Content-Type: application/sdp
Content-Length: 264

v=0
o=change_me 5972727 56415 IN IP4 192.168.1.1

```

Telnet Command: voip dialplan

This command allows users to set phone book settings.

Syntax

voip dialplan block *n* [-<command><parameter>]

voip dialplan phonebook *n* [-<command><parameter>]

voip dialplan region [-<command><parameter>]

voip dialplan local [1/0]

Syntax Description

Parameter	Description
voip dialplan block	
<i>n</i>	It means the index number of the VoIP settings. n=1 ~ 20
-<command><parameter>	The available commands with parameters are listed below.
-m 0/1	It means to enable or disable the block mode. 0 - Disable 1 - Enable
-p <path>	Determines the block path. 1:in_url, 2:in_number 3:out_url, 4:out_number 5:(in & out)_url, 6:(in & out)_number)
-n <number>	Determines the block number (maximum 29 characters).
-d <domain>	Block the specified domain.
-i <inf>	Block the specified interface(s) or All interfaces.
-s <Schedule>	Specify schedule profiles by indicating the index number of the schedule profile. Four schedule profiles can be used at one time.
-w	Delete the selected entry. N=null (clear all)
-v	List current settings.
voip dialplan phonebook	
<i>n</i>	It means the index number of the VoIP settings. n=1 ~ 60

-<command><parameter>	The available commands with parameters are listed below.
-d <number>	Specify the speed dial number.
-c <url>	Contact SIP URL I(max. 59 characters)
-n <name>	Contact name (max. 23 characters)
-a <enable>	Enable/disable the specify entry.
-m <mode>	Specify backup number mode. 0 - none 2 - PSTN
-b <number>	Specify the backup number.
-o <acc num>	Specify the dial out account. 0 - default 1 - acc1, 2 - acc2... ~ 12:=acc12
-z <enable>	Enable/disable ZRTP/SRTP VoIP security. 1 - enable 0 - disable
-l	Delete the specify entry.
-V	List current VoIP settings.
voip dialplan region	
-e	Enable or disable the regional function. 1 - enable 0 - disable
-m <number>	Return the last miss call.
-I <number>	Return the last incoming call.
-o <number>	Return the last outgoing call.
-F <number>	Hotkey to enable call forwarding (all) function.
-f <number>	Hotkey to enable call forwarding (busy) function.
-C <number>	Hotkey to enable call forwarding (no answer) function.
-c <number>	Hotkey to disable call forwarding function.
-W <number>	Hotkey to enable call waiting function.
-w <number>	Hotkey to disable call waiting function.
-H <number>	Hotkey to enable hide caller ID function.
-h <number>	Hotkey to disable hide caller ID function.
-D <number>	Hotkey to enable DND function.
-d <number>	Hotkey to disable DND function.
-A <number>	Hotkey to enable block anonymous calls function.
-a <number>	Hotkey to disable block anonymous calls function.
-U <number>	Hotkey to enable block unknow domain calls function.
-u <number>	Hotkey to disable block unknow domain calls function.
-P <number>	Hotkey to enable block IP calls function.
-p <number>	Hotkey to disable block IP calls function.
-l <number>	Hotkey to block last incoming call.
-v	List current status for Regional settings.
voip dialplan local	

<i>enable/disable</i>	Enable or disable the local calls. 1 - enable 0 - disable
-----------------------	---

Example

```

> voip dialplan phonebook 1 -d 1125
> voip dialplan region -l 8
> voip dialplan region -v
Your Setting for Regional
Regional Function is: Enable
Return the Last Miss Call: 20
Return the Last Incoming Call: *12
Return the Last Outgoing Call: 1
Hotkey to enable call forwarding (all) function: 0
Hotkey to enable call forwarding (busy) function: *90
Hotkey to enable call forwarding (no answer) function: *92
Hotkey to disable call forwarding function: 12
Hotkey to Enable Call Waiting Function: *56
Hotkey to Disable Call Waiting Function: *57
Hotkey to Enable Hide Caller ID Function: *67
Hotkey to Disable Hide Caller ID Function: *68
Hotkey to Enable DND Function: *78
Hotkey to Disable DND Function: *79
Hotkey to Enable Block Anonymous Calls Function: *77
Hotkey to Disable Block Anonymous Calls Function: *87
Hotkey to Enable Block Unknow Domain Calls Function: *40
Hotkey to Disable Block Unknow Domain Calls Function: *04
Hotkey to Enable Block IP Calls Function: *50
Hotkey to Disable Block IP Calls Function: *05
Hotkey to Disable Block The Last Incoming Call Function: 8

```

Telnet Command: voip dsp

Syntax

```

voip dsp countrytone [channel] [value]
voip dsp dialtonepwr [channel] [AbsoluteValue]
voip dsp EchoCanceller [type] [w_size] [nlp]
voip dsp cidtype [channel] [value]
voip dsp micgain [channel] [value/(1-10)]
voip dsp spkgain [channel] [value/(1-10)]
voip dsp jitterBuffer [port] [mode] [value]
voip dsp dtmfDetset [nLevel] [nTwist]
voip dsp dtmftonepwr [Level]
voip dsp cwtonepwr [ch] [value]
voip dsp pstnringfxs [1/2] [on/off]
voip dsp relaydbounce [on/off]
voip dsp setRingPat [ring_pattern_index] [patten_num]
voip dsp setDtmfCidlevel -I [value]

```

voip dsp setDtmfCidlevel -h [value]
voip dsp setDtmfCidlevel -r 0
voip dsp cidplusdigit [1/0] [channel] [value]

Syntax Description

Parameter	Description
<i>voip dsp countrytone</i>	
<i>[channel] [value]</i>	This command allows users to set the region for the tone settings. Different regions usually need different tone settings. Channel - 1 or 2. Value - displayed as follows: [2] UK, [3] USA, [4] Denmark, [5] Italy, [6] Germany, [7] Netherlands, [8] Portugal, [9] Sweden, [10] Australia, [11] Slovenia, [12] Czech, [13] Slovakia, [14] Hungary, [15] Switzerland , [16] France , [17] Malta
<i>voip dsp dialtonepwr</i>	
<i>channel</i>	This setting is used to adjust the loudness of the dial tone. The smaller the number is, the louder the dial tone is. It is recommended for you to use the default setting. Channel - Available channel number: 1 - 2
<i>AbsoluteValue</i>	AbsoluteValue - In -1 dB increments, with 1 corresponding to 6 dBm. Range - 1 to 30
<i>voip dsp EchoCanceler</i>	
<i>type</i>	This command is used to set the type of echo reduction. 0 - Disable the LEC processing. 1 - Cancel using the fixed window. 2 - Cancel using the fixed and moving window. 3 - Cancel using fixed window + Echo Suppressor.
<i>w_size</i>	The Line Echo Canceller (LEC) window size is 4, 6, 8 or 16 (ms).
<i>nlp</i>	Nlp - Non-linear processing (NLP) for more smooth transitions. 1 - disable 0 - enable
<i>voip dsp cidtype</i>	
<i>channel</i>	Set the caller ID type for FXS 1 (Channel 1) or FXS 2 (Channel 2). 1 - FXS 1 2 - FXS 2
<i>value</i>	Each number (1 to 6) represents different type. 1 - FSK_ETSI 2 - FSK_ETSI(UK) 3 - FSK_BELLCORE(US/AU) 4 - DTMF 5 - DTMF(Dk) 6 - DTMF(SE,NL,FIN) For example : Vigor> voip dsp cidtype 2 6 channel=2, current cidType: 6 That means the caller ID type for FXS2 (Channel2) is DTMF (SE, NL, FIN).
<i>voip dsp micgain</i>	

<i>channel</i>	Adjust the volume of microphone by entering number from 1- 10 for FXS 1 or FXS 2. 1 - FXS 1 2 - FXS 2
<i>value/(1-10)</i>	The larger the number is, the louder the volume will be.
<i>voip dsp spkgain</i>	
<i>channel</i>	Adjust the volume of speaker by entering number from 1- 10 for FXS 1 or FXS 2. 1 - FXS 1 2 - FXS 2
<i>value/(1-10)</i>	The larger the number is, the louder the volume will be.
<i>voip dsp jb</i>	
<i>port</i>	Set the size of jitter buffer. Available settings are 0 (FXS1) and 1 (FXS2).
<i>mode</i>	Available settings are Fixed and Adaptive (default setting).
<i>value</i>	Available settings are 1 ~ 180 (unit: msec). e.g., Vigor> voip dsp jb 1 FIXED 100
<i>voip dsp timer</i>	
<i>[Timer]</i>	Set the waiting time for dialing out. It means to set the timer settings. The unit is mini-second. The range is from 1 to 255. Value "1" is corresponding to 500ms. That is to say, Value "6" is corresponding 3000ms (i.e., 3 seconds) Timer: 1 ~ 20. Vigor> voip dsp timer 20 Set the timer:20
<i>Voip dsp debugMsg</i>	
<i>?</i>	Availbe settings include: clrev - clear phone hook status. getev - get phone hook status. clrfskcid - clear fsk data for caller-ID from PSTN line. getfskcid - get fsk data for caller-ID from PSTN line. clrdtmfcid - clear dtmf data for caller-ID from PSTN line. getdtmfcid - get dtmf data for caller-ID from PSTN line. voicebuf - get message for available voice buffer pool. clrint - clear status for interrupt. getint - get status for interrupt. Vigor> voip dsp debugMsg getint the interrupt status for ad0 = 21 the interrupt status for ad1 = 0 the interrupt status for vc = 0
<i>voip dsp dtmfDetset</i>	
<i>nLevel</i>	Set minimal signal level in dB, for DTMF detection. Range - (-96 ~ -1)
<i>nTwist</i>	Maximum allowed signal twist in dB, for DTMF detection. Range - (0 ~ 12)
<i>voip dsp dtmftonepwr</i>	
<i>Level</i>	Set power level for DTMF frequency. Level - 0 ~ 100. Power level for dtmf frequency in 0.3 dB steps.

	0 map to 0dB 1 map to -0.3dB 100 map to -30dB
<i>voip dsp cwtonepwr</i>	
<i>ch</i>	Set the call waiting tone power level. 1 - FXS 1 2 - FXS 2.
<i>value</i>	1 ~ 30, in -1 dB increments, with 1 corresponding to 8 dBm.
<i>voip dsp pstnringfxs</i>	
<i>1/2</i>	Enable or disable PSTN ring on FXS 1/FXS 2. 1 means FXS1; 2 means FXS2.
<i>on/off</i>	On means enable; off means disable.
<i>voip dsp relaydbounce</i>	
<i>on/off</i>	on: Enable relay filter noise. But it maybe ignore the caller-id!!! off: Disable relay filter noise. But the noise will cause the relay to switch to PSTN!!!
<i>voip dsp setRingPat</i>	
<i>ring_pattern_index</i>	This command can change the ring pattern at Index(2)-Index(6). ring_pattern_index - Index (1) was locked for your country.
<i>patten_num</i>	It's the ring pattern number (1~12) for a country. ----- <i>patten_num=1 Australia Ring Pattern:</i> <i>cadenceOneOn=400, cadenceOneOff=200</i> <i>cadenceTwoOn=400, cadenceTwoOff=2000</i> <i>patten_num=2 Denmark Ring Pattern:</i> <i>cadenceOneOn=1000, cadenceOneOff=4000</i>
<i>voip dsp setFaxECmode -s</i>	
<i>ch</i>	Set the FAX error correction mode. ch : range (0 ~ 1)
<i>mode</i>	mode : EC(error correction) ch(x) mode(0) : REDUNDANCY EC(error correction) ch(x) mode(1) : FEC
<i>voip dsp setDtmfCidlevel -l / voip dsp setDtmfCidlevel -h [value]</i> <i>voip dsp setDtmfCidlevel -r 0</i>	
<i>value</i>	"setDtmfCidLevel" is used to configure the signal strength for transferring to FXS DTMF caller ID. value - 0 ~ 64 voip dsp setDtmfCidLevel -l [value] voip dsp setDtmfCidLevel -h [value] voip dsp setDtmfCidLevel -r 0/1 r - reset low/high DTNF level to default setting. 0 means Disable; 1 means Enable. Note: This function is supported only by special mode.
<i>voip dsp setfxoCY</i>	
<i>value</i>	It is used to apply FXO country settings. 0: "use system country" 1: "Taiwan" 2: "Germany" 3: "Sweden" 4: "France" 5: "Switzerland"

	6: "Holland" 7: "Finland" 8: "Denmark" 9: "UK" 10: "Australia" 12: "Italy" 14: "Red_China" 15: "Singapore" 17: "Spain" 18: "Portugal" 20: "Poland" 21: "Czech" 22: "Hungary" 23: "Slovenia" 25: "Slovakia" 37: "Brasil" 61: "US"
<i>voip dsp setfxoringl</i>	
<i>value</i>	It is used to configure detection ring voltage threshold to apply to FXO. Available setting include: 0 : use driver default value 1 : Minimum voltage threshold: 25V 2 : Minimum voltage threshold: 35V 3 : Minimum voltage threshold: 45V Note: This function is supported only by special mode.
<i>voip dsp setfxoCid</i>	
<i>value</i>	Set FXO detect caller ID type. It is available only for the model with FXO port.
<i>voip dsp cidplusdigit</i>	
<i>[1/0] [channel] [value]</i>	Set the substitution (0-9) for '+' digit in caller ID. 1 - enable the substitution. 0 - disable the substitution. channel - 0 (FXS 1) -1 (FXS 2) value - 0 - 9
<i>voip dsp setRingThres</i>	
<i>port</i>	Set the threshold for ring signal. Port setting is "0" only.
<i>value</i>	Available settings 0-250. Unit is ms. The time is an approximate value.
<i>voip dsp setCidDetGain</i>	
<i>tx/rx gain</i>	Set the gain value of caller ID detected. Tx gain - Available settings -24 ~ 12. Default is 0. Rx gain - Available settings -24 ~ 12. Default is -6.

Example

```
> voip dsp countrytone ?
VoIP has been disable. Please enable VoIP first.
> voip sip misc -D 0
System reboot now!
> voip dsp countrytone ?
> Vigor> voip dsp countrytone?
usage:
```

```

voip dsp countrytone [channel][value]
[channel]: 1-2
[value]: ( [2] UK, [3] USA, [4] Denmark, [5] Italy, [6] Germany, [7] Netherland
s, [8] Portugal, [9] Sweden, [10] Australia, [11] Slovenia, [12] Czech, [13]
Slovakia, [14] Hungary, [15] Switzerland , [16] France , [17] Malta)
===== Channel=1 =====
current country tone: user defined

----- ( Dial tone ) -----
Feq1=425, Feq2=0, OneOn=0, Off=0, TwoOn=0, TwoOff=0
----- ( Ringing tone ) -----
Feq1=425, Feq2=0, OneOn=1500, OneOff=3000, TwoOn=0, TwoOff=0
----- ( Busy tone ) -----
Feq1=425, Feq2=0, OneOn=200, OneOff=200, TwoOn=0, TwoOff=0

===== Channel=2 =====
current country tone: user defined
> voip dsp dialtonepwr 1 20
Current power level of dialtone:20 (-13 db), channel=1
> voip dsp setCidDetGain tx 1
Current CID Detect Tx Gain [1], Rx Gain [-6]
> voip dsp setCidDetGain rx 3
Current CID Detect Tx Gain [1], Rx Gain [3]

```

Telnet Command: voip rtp

Syntax

voip rtp codec [*sip acc index*][*type/size/vad/one*][*value*]

voip rtp dtmf [*index*] [*mode/payloadtype*][*value*]

voip rtp port [*start/end*] [*value*]

voip rtp symmetric [*value*]

voip rtp tos ?

Syntax Description

Parameter	Description
<i>voip rtp codec</i>	
<i>[sip acc index][type/size/vad/one][value]</i>	Set the voice coding. sip acc index -SIP account index number. Available number, 1 ~ 12. type - Available settings include 0. G.711MU 1. G.711A 2. G.729A/B 3. G.723 4. G.726_32 size - Five options, 0 means 10ms 1 means 20ms 2 means 30ms 3 means 40ms 5 means 60ms Vad - 0 means to Disable the function of Voice Active Detector

	(vad); 1 means to Enable the function of Voice Active Detector (vad). One - 0 means to Disable the function of single codec; 1 means to Enable the function of single codec.
voip rtp dtmf	
<i>[index] [mode / payloadtype][value]</i>	Set the DTMF mode and Payload type for DTMF. Index - SIP account index number. Available number, 1 ~ 12. Mode - Four options to be selected. 0. Inband 1. Outband 2. SIP INFO (cisco) 3. SIP INFO (nortel) Payloadtype - Available settings 96~127. Value - Type 0~3 or 96~127 based on the mode specified. For example, > voip rtp dtmf 1 mode 1
voip rtp port	
<i>start/end</i>	Specifies the start/end port for RTP stream.
<i>value</i>	The default value is 10050/15000.
voip rtp symmetric	
<i>value</i>	Make the data transmission going through on both ends of local router and remote router not misleading due to IP lost. 1 - Enable 0 - Disable
voip rtp tos	
<i>value</i>	Set the type of service (TOS) setting for RTP packets. For example, > voip rtp tos 0x899 Set TOS: 0x899

Example

```

> voip rtp codec 1 type 3
> voip rtp dtmf 2 mode 3
> voip rtp port start 10070 end 14400
Set start port: 10070
> voip rtp port end 14400
Set end port: 14400
> voip rtp symmetric 1
Set symmetric rtp to Enable

```

Telnet Command: voip sip

This command allows users to set SIP account.

Syntax

```
voip sip acc n [-<command> <parameter> | ... ]
```

```
voip sip calllog
```

```
voip sip ep n [-<command> <parameter> | ... ]
```

voip sip misc[-<command> <parameter> | ...]

voip sip nat [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
<i>voip sip acc</i> - Allows users to set SIP account.	
<i>n</i>	n = 1 to 12 It means the index number of the VoIP settings.
<i>-P [profile]</i>	It means the name of the account profile (maximum 11 characters).
<i>-r [reg mode]</i>	Set registration mode for SIP account. 0 - none 1 - auto 2 - wan1 only 3 - wan2 only 4 - lan/vpn 5 - PVC 6 - wan3 only 7 - wan4 only 8 - wan1 first 9 - wan2 first 10 - wan3 first 11 - wan4 first
<i>-o [port]</i>	Set the port number for sending/receiving SIP message for building a session. The default value is 5060.
<i>-d [domain]</i>	Set the domain name or IP address of the SIP Registrar server. The maximum is 63 characters.
<i>-y [proxy]</i>	Set domain name or IP address of SIP proxy server. The maximum is 63 characters.
<i>-b [enable]</i>	Enable / disable outbound proxy by SIP account. 0 - disable 1 - enable
<i>-s [enable]</i>	Enable / disable to locate SIP server (rfc 3263). 0 - disable 1 - enable
<i>-N [name]</i>	Set SIP account display name. Name - max. 23 characters.
<i>-n [number]</i>	Set SIP account number. Number - max. 63 characters.
<i>-a [id]</i>	Set SIP authentication ID. Id - max. 63 characters.
<i>-A [enable]</i>	Enable /disable to use SIP authentication ID. 0 - disable 1 - enable
<i>-p [passwd]</i>	Set SIP account password (max. 63 characters).
<i>-e [sec]</i>	Set expiry time (default 3600) for SIP account.
<i>-w [enable]</i>	Enable to make phone call without registering.
<i>-m [mode]</i>	Set NAT traversal mode. 0 - disable 1 - stun 2 - manual

	3 - nortel
<i>-F [mode]</i>	Set call forwarding mode. 0 - disable 1 - always 2 - busy 3 - no answer 4 - busy or no answer
<i>-u [url]</i>	Set SIP URL for call forwarding (max. 63 characters).
<i>-t [sec]</i>	Set call forwarding timer. For example, voip sip acc 1 -t 30
<i>-g [port]</i>	Set the ring port for incoming call. For example, Port - r1 means FXS1; r2 means FXS2.
<i>-z [pattern]</i>	Set account ring pattern (1 ~ 6).
<i>-i [enable]</i>	Remove all bindings while they are un-registered. 0 means Disable; and 1 means Enable.
<i>-B <enable></i>	Enable / disable the function of Broadsoft Call Control. 0 - disable 1 - enable
<i>-S [idx]</i>	Enable and use alias IP to register. idx - 1 to 31. If 0 is used, such function will be disabled.
<i>-k [num1 num2...]</i>	Set backup wan list (first wan, second wan...). range: 1 to 4.
<i>-v</i>	View current status for account settings.
Voip sip calllog	Display current status for SIP call log.
voip sip ep	
<i>n</i>	The index number of the VoIP settings. n - 1, 2.
<i>-o [acc]</i>	Available dial out account (1 ~ 12).
<i>-L [url]</i>	Set SIP URL (max. 63 characters) for hot line.
<i>-I [enable]</i>	Enable / disable the function of hot line. 0 - disable 1 - enable
<i>-W [enable]</i>	Enable / disable the function of warm line. 0 - disable 1 - enable
<i>-w [enable]</i>	Enable / disable the function of call waiting enable. 0 - disable 1 - enable
<i>-E [enable]</i>	Enable / disable the function of call waiting enable but only remind one time. 0 - disable 1 - enable
<i>-x <enable></i>	Enable / disable the function of call transfer. 0 - disable 1 - enable
<i>-d [enable]</i>	Enable / disable the function of DND (Do Not Disturb) 0 - disable

	1 - enable
-s [<i>id</i>]	Indicate DND schedule. Id - s1, s2, s3, s4 (max. 4 schedule)
-h [<i>enable</i>]	Enable / disable the function of calling line identification restriction (CLIR). 0 - disable 1 - enable
-u [<i>mode</i>]	Set CLIR mode. 0 - means "draft-ietf-sip-privacy" 1 - means "rfc 3323/3325"
-z [<i>enable</i>]	Enable / disable playing dial tone when registered on sip server. 0 - disable 1 - enable
-n [<i>enable</i>]	Enable / disable session timer. 0 - disable 1 - enable
-m [<i>sec</i>]	Set the value for session timer (unit: sec).
-R [<i>min,max</i>]	Set the flash hook time range 100-2000 (unit: ms).
-8 [<i>enable</i>]	Enable or disable T.38 fax relay feature. 0 - disable 1 - enable
-v	View current settings.
voip sip misc - Allows users to set miscellaneous settings for the device.	
-c [<i>enable</i>]	Enable compact header to shorten the packet (0: disable, 1: enable).
-s [<i>enable</i>]	Change "#" into digit number. 0 - disable 1 - enable
-e [<i>enable</i>]	Enable Europe style flash hook operation mode. 0 - disable 1 - enable
-h [<i>enable</i>]	Enable/disable call hold mode based on protocol RFC2543 (0: disable, 1:enable).
-i [<i>enable</i>]	Enable CODEC change without Re-INVITE. 0 - disable 1 - enable
-p [<i>enable</i>]	Enable PRACK message. 0 - Not support PRACK. 1 - Support PRACK.
-P [<i>enable</i>]	Enable IP Call. 0 - Disable IP call. 1 - Enable IP call.
-H [<i>enable</i>]	SIP INFO packet will be sent out when encountering hook flash event. 0 - disable 1 - enable
-t [<i>val</i>]	Set the mode of User-Agent (e.g., phone, software, and device) for SIP packet. 0 - Hide SIP header "User-Agent".

	1 - Show SIP header "User-Agent". 2 - Use default "User-Agent" value. 3 - Use user-defined "User-Agent" value.
<i>-u UValue</i>	For every SIP user agent identifies itself with a string, this command allows you to set the value (e.g, IP address, phone number, e-mail address) of User-Agent. The length of the string must be less than 64 characters.
<i>-D [disable]</i>	Disable VoIP Service. 1 - disable VoIP service. 0 - enable VoIP service. System will automatic reboot to activate voip service
<i>-v</i>	View current status for miscellaneous settings.
<i>voip sip nat</i> - Allows users to set NAT Traversal Setting.	
<i>-s [server]</i>	Set the IP address for STUN server.
<i>-t [sec]</i>	Set ping interval for SIP account. Sec - 6 - 600
<i>-i [ip]</i>	Indicate external IP address.
<i>-v</i>	View current settings for SIP NAT.

Example

```

> voip sip misc -t 1
includes User-Agent header

> voip sip misc -u 91704688carrie
user-defined User-Agent:91704688carrie
> voip sip acc 1 -P carrie_1 -r 1 -d 172.16.3.133
> voip sip acc 1 -t 30
> voip sip misc -h 1
> voip sip acc 1 -v
index      : 1
profile    : carrie_1
reg mode   : 1 | reg. [No]
alias_ip_idx : 0
backup list :
domain     : 172.16.3.133
proxy      : | outbound [No] | DNS-SRV [No]
noreg call : No
disp. Name :
acc number : ---
auth. ID   : | [disable]
expiry     : 3600
NAT mode   : 0
ring ports : 0
ring pat.  : 1
call fwd mode : 0
call fwd url :
call fwd timer : 30
Broadsoft  : disable
Italian ITSP modification: disable

```

Telnet Command: voip secure

This command allows users to enable or disable secure phone feature, and SAS voice prompt.

Syntax

`voip secure general [-<command> <parameter> | ...]`

Syntax Description

Parameter	Description
<code>voip secure general -e</code>	Enable / disable secure phone feature. 0 - disable 1 - enable
<code>voip secure general -p</code>	Enable /disable SAS voice prompt. 0 - disable 1 - enable
<code>voip secure general -v</code>	view only secure phone general settings

Example

```
> voip secure general -v
secure phone feature is disabled
SAS voice prompt is enabled
> voip secure general -p 0
SAS voice prompt is disabled
```

Telnet Command: vpn l2lset

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]
```

Syntax Description

Parameter	Description
<code>list index</code>	It means the index number of L2L (LAN to LAN) profile.
<code>peerid</code>	It means the peer identity for aggressive mode.
<code>localid</code>	It means the local identity for aggressive mode.
<code>main</code>	It means to choose proposal for main mode.
<code>auto index</code>	It means to choose default proposals.
<code>proposal index</code>	It means to choose specified proposal.

<i>aggressive</i>	It means the chosen DH group for aggressive mode
<i>pfs</i>	It means "perfect forward secrete" .
<i>on/off</i>	It means to turn on or off the PFS function.
<i>phase1</i>	It means phase 1 of IKE.
<i>lifetime</i>	It means the lifetime value (in second) for phase 1 and phase 2.
<i>phase2</i>	It means phase 2 of IKE.

Example

```
> VPN l2lset 1 peerid 10226
```

Telnet Command: vpn l2lDrop

This command allows users to terminate current LAN to LAN VPN connection.

Example

```
> vpn l2lDrop
>
```

Telnet Command: vpn dinset

This command allows users to configure setting for remote dial-in VPN profile.

Syntax

`vpn dinset <list index>`

`vpn dinset <list index> <on/off>`

`vpn dinset <list index> motp <on/off>`

`vpn dinset <list index> pin_secret <pin> <secret>`

Syntax Description

Parameter	Description
<i><list index></i>	It means the index number of the profile.
<i><on/off></i>	It means to enable or disable the profile. on - Enable. off - Disable.
<i>motp <on/off></i>	It means to enable or disable the authentication with mOTP function. on - Enable. off - Disable.
<i>pin_secret<pin> <secret></i>	It means to set PIN code with secret. <i><pin></i> - Type the code for authentication (e.g, 1234). <i><secret></i> - Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6)

Example

```
> vpn dinset 1

Dial-in profile index 1
```

```

Profile Name: ???
Status: Deactive

Mobile OTP: Disabled

Password:

Idle Timeout: 300 sec

> vpn dinset 1 on
% set profile active

> vpn dinset 1 motp on
% Enable Mobile OTP mode!>
> vpn dinset 1 pin_secret 1234 e759bb6f0e94c7ab4fe6
> vpn dinset 1

Dial-in profile index 1

Profile Name: ???
Status: Active

Mobile OTP: Enabled

PIN: 1234

Secret: e759bb6f0e94c7ab4fe6

Idle Timeout: 300 sec

```

Telnet Command: vpn subnet

This command allows users to specify a subnet selection for the specified remote dial-in VPN profile.

Syntax

vpn subnet [*index*] [1/2/3/4/5/6]

Syntax Description

Parameter	Description
< <i>index</i> >	It means the index number of the VPN profile.
<1/2/3/4/5/6>	1 - it means LAN1 2 - it means LAN2. 3 - it means LAN3 4 - it means LAN4. 5 - it means LAN51 6 - it means LAN6.

Example


```
> vpn subnet 1 2
>
```

Telnet Command: vpn setup

This command allows users to setup VPN for different types.

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>
```

Syntax Description

Parameter	Description
For PPTP Dial-Out	
<index>	It means the index number of the profile.
<name>	It means the name of the profile.
<ip>	It means the IP address to dial to.
<usr> <pwd>	It means the user and the password required for the PPTP connection.
<nip> <nmask>	It means the remote network IP and the mask. e.g., vpn setup 1 name1 pptp_out 1.2.3.4 vigor 1234 192.168.1.0 255.255.255.0
For IPsec Dial-Out	
<index>	It means the index number of the profile.
<name>	It means the name of the profile.
<ip>	It means the IP address to dial to.
<key>	It means the value of IPsec Pre-Shared Key.
<nip> <nmask>	It means the remote network IP and the mask. e.g., vpn setup 1 name1 ipsec_out 1.2.3.4 1234 192.168.1.0 255.255.255.0
For L2TP Dial-Out	
<index>	It means the index number of the profile.
<name>	It means the name of the profile.
<ip>	It means the IP address to dial to.
<usr> <pwd>	It means the user and the password required for the L2TP connection.
<nip> <nmask>	It means the remote network IP and the mask. e.g., vpn setup 1 name1 l2tp_out 1.2.3.4 vigor 1234 192.168.1.0

	255.255.255.0
For Dial-In	
<index>	It means the index number of the profile.
<name>	It means the name of the profile.
<ip>	It means the IP address allowed to dial in.
<usr> <pwd>	It means the user and the password required for the PPTP/L2TP connection.
<key>	It means the value of IPsec Pre-Shared Key.
<nip> <nmask>	It means the remote network IP and the mask. e.g., vpn setup 1 name1 dialin 1.2.3.4 vigor 1234 abc 192.168.1.0 255.255.255.0

Example

```
> vpn setup 1 name1 dialin 1.2.3.4 vigor 1234 abc 192.168.1.0
255.255.255.0
% Profile Change Log ...

% Profile Index : 1
% Profile Name : name1
% Username : vigor
% Password : 1234
% Pre-share Key : abc
% Call Direction : Dial-In
% Type of Server : ISDN PPTP IPsec L2TP
% Dial from : 1.2.3.4
% Remote Network IP : 192.168.1.0
% Remote Network Mask : 255.255.255.0
>
```

Telnet Command: vpn option

This command allows users to configure settings for LAN to LAN profile.

Syntax

vpn option <index> <cmd1>=<param1> [<cmd2>=<para2> | ...]

Syntax Description

Parameter	Description
<index>	It means the index number of the profile. Available index numbers: 1 ~ 32
For Common Settings	
<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

<i>thr</i>	It means the way that VPN connection passes through. Available settings are w1f, w1o, w2f, and w2o. w1f - WAN1 First. w1o - WAN1 Only. w2f - WAN2 First. w2o - WAN2 Only.
<i>nnpkt</i>	It means the NetBios Naming Packet. on - Enable the function to pass the packet. off - Disable the function to block the packet.
<i>dir</i>	It means the call direction. Available settings are b, o and i. b - Both o - Dial-Out i - Dial-In.
<i>idle=[value]</i>	It means Always on and Idle Time out. Available values include: -1 - it means always on for dial-out. 0 - it means always on for dial-in. Other numbers (e.g., idle=200, idle=300, idle=500) mean the router will be idle after the interval (seconds) configured here.
<i>palive</i>	It means to enable PING to keep alive. -1 - disable the function. 1,2,3,4 - Enable the function and PING IP 1.2.3.4 to keep alive.
For Dial-Out Settings	
<i>ctype</i>	It means "Type of Server I am calling". "ctype=t" means PPTP. "ctype=s" means IPsec. "ctype= l" means L2TP(IPsec Policy None). "ctype= l1" means L2TP(IPsec Policy Nice to Have). "ctype= l2" means L2TP(IPsec Policy Must).
<i>dialto</i>	It means Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89).
<i>ltype</i>	It means Link Type. "ltype=0" means "Disable". "ltype=1" means "64kbps". "ltype=2" means "128kbps". "ltype=3" means "BOD".
<i>oname</i>	It means Dial-Out Username. "oname=admin" means to set Username = admin.
<i>opwd</i>	It means Dial-Out Password "opwd=1234" means to set Password = 1234.
<i>pauth</i>	It means PPP Authentication. "pauth=pc" means to set PPP Authentication = PAP&CHAP. "pauth=p" means to set PPP Authentication = PAP Only
<i>ovj</i>	It means VJ Compression. "ovj=on/off" means to enable/disable VJ Compression.
<i>okey</i>	It means IKE Pre-Shared Key. "okey=abcd" means to set IKE Pre-Shared Key = abcd.
<i>ometh</i>	It means IPsec Security Method. "ometh=ah/" means AH.

	<p>"ometh=espd/espda/" means ESP DES without/with Authentication.</p> <p>"ometh=esp3/esp3a/" means ESP 3DES without/with Authentication.</p> <p>"ometh=espa/espaa" means ESP AES without/with Authentication.</p>
<i>sch</i>	<p>It means Index(1-15) in Schedule Setup.</p> <p>sch=1,3,5,7 Set schedule 1->3->5->7</p>
<i>rca1lb</i>	<p>It means Require Remote to Callback.</p> <p>"rca1lb=on/off" means to enable/disable Set Require Remote to Callback.</p>
<i>ikeid</i>	<p>It means IKE Local ID.</p> <p>"ikeid=vigor" means Set Local ID = vigor.</p>
For Dial-In Settings	
<i>itype</i>	<p>It means Allowed Dial-In Type. Available settings include:</p> <p>"itype=t" means PPTP.</p> <p>"itype=s" means IPSec.</p> <p>"itype=L1" means L2TP (None).</p> <p>"itype=L1" means L2TP(Nice to Have).</p> <p>"itype=I2" means L2TP(Must).</p>
<i>peer</i>	<p>It means specify Peer VPN Server IP for Remote VPN Gateway.</p> <p>Type "203.12.23.48" means to allow VPN dial-in with IP address of 203.12.23.48.</p> <p>Type "off" means any remote IP is allowed to dial in.</p>
<i>peerid</i>	<p>It means the peer ID for Remote VPN Gateway.</p> <p>Type "draytek" means the word is used as local ID.</p>
<i>iname</i>	<p>It means Dial-in Username.</p> <p>"iname=admin" means to set username as "admin".</p>
<i>ipwd</i>	<p>It means Dial-in Password.</p> <p>"ipwd=1234" means to set password as "1234".</p>
<i>ivj</i>	<p>It means VJ Compression.</p> <p>"ivj=on/off" means to enable /disable VJ Compression.</p>
<i>ikey</i>	<p>It means IKE Pre-Shared Key.</p> <p>"ikey=abcd" means to set IKE Pre-Shared Key = abcd.</p>
<i>imeth</i>	<p>It means IPSec Security Method</p> <p>"imeth=h" means "Allow AH".</p> <p>"imeth=d" means "Allow DES".</p> <p>"imeth=3" means "Allow 3DES".</p> <p>"imeth=a" means "Allow AES".</p>
For TCP/IP Settings	
<i>mywip</i>	<p>It means My WAN IP.</p> <p>"mywip=1.2.3.4" means to set My WAN IP as "1.2.3.4".</p>
<i>rgip</i>	<p>It means Remote Gateway IP.</p> <p>"rgip=1.2.3.4" means to set Remote Gateway IP as "1.2.3.4".</p>
<i>rnip</i>	<p>It means Remote Network IP.</p> <p>"rnip=1.2.3.0" means to set Remote Network IP as "1.2.3.0".</p>
<i>rnmask</i>	<p>It means Remote Network Mask.</p> <p>"rnmask=255.255.255.0" means to set Remote Network Mask as "255.255.255.0".</p>

<i>rip</i>	It means RIP Direction. "rip=d" means to set RIP Direction as "Disable". "rip=t" means to set RIP Direction as "TX". "rip=r" means to set RIP Direction as "RX". "rip=b" means to set RIP Direction as "Both".
<i>mode</i>	It means the option of "From first subnet to remote network, you have to do". "mode=r" means to set Route mode. "mode=n" means to set NAT mode.
<i>droute</i>	It means to Change default route to this VPN tunnel (Only single WAN supports this). droute=on/off means to enable/disable the function.

Example

```
> vpn option 1 idle=250
% Change Log..

% Idle Timeout = 250
```

Telnet Command: vpn mroute

This command allows users to list, add or delete static routes for a certain LAN to LAN VPN profile.

Syntax

```
vpn mroute <index> list
vpn mroute <index> add <network ip>/<mask>
vpn mroute <index> del <network ip>/<mask>
```

Syntax Description

Parameter	Description
<i>list</i>	It means to display all of the route settings.
<i>add</i>	It means to add a new route.
<i>del</i>	It means to delete specified route.
<index>	It means the index number of the profile. Available index numbers: 1 ~ 32
<network ip>/<mask>	Type the IP address with the network mask address.

Example

```
> vpn mroute 1 add 192.168.5.0/24
% 192.168.5.0/24
% Add new route 192.168.5.0/24 to profile 1
```

Telnet Command: vpn list

This command allows users to view LAN to LAN VPN profiles.

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
<i>all</i>	It means to list configuration of the specified profile.
<i>com</i>	It means to list common settings of the specified profile.
<i>out</i>	It means to list dial-out settings of the specified profile.
<i>in</i>	It means to list dial-in settings of the specified profile.
<i>net</i>	It means to list Network Settings of the specified profile.
<i><index></i>	It means the index number of the profile. Available index numbers: 1 ~ 32

Example

```

> vpn list 32 all
% Common Settings

% Profile Name           : ???
% Profile Status        : Disable
% Netbios Naming Packet : Pass
% Call Direction        : Both
% Idle Timeout          : 300
% PING to keep alive    : off

% Dial-out Settings

% Type of Server         : PPTP
% Link Type:             : 64k bps
% Username              : ???
% Password               :
% PPP Authentication     : PAP/CHAP
% VJ Compression        : on
% Pre-Shared Key        :
% IPSec Security Method : AH
% Schedule               : 0,0,0,0
% Remote Callback       : off
% Provide ISDN Number   : off
% IKE phase 1 mode      : Main mode
% IKE Local ID          :

% Dial-In Settings

--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
> vpn list 1 com
% Common Settings

```

```

% Profile Name          : ???
% Profile Status       : Disable
% Netbios Naming Packet : Pass
% Call Direction       : Both
% Idle Timeout         : 300
% PING to keep alive   : off
>

```

Telnet Command: vpn remote

This command allows users to enable or disable *PPTP/IPSec/L2TP* VPN service.

Syntax

vpn remote [*PPTP/IPSec/L2TP*] [*on/off*]

Syntax Description

Parameter	Description
<i>PPTP/IPSec/L2TP</i>	There are four types to be selected.
<i>on/off</i>	on - enable VPN remote setting. off - disable VPN remote setting.

Example

```

> vpn remote PPTP on
Set PPTP VPN Service : On

Please restart the router!!

```

Telnet Command: vpn 2ndsubnet

This command allows users to enable second subnet IP as VPN server IP.

Syntax

vpn 2ndsubnet *on*

vpn 2ndsubnet *off*

Syntax Description

Parameter	Description
<i>on/off</i>	It means to enable or disable second subnet.

Example

```

> vpn 2ndsubnet on
%Enable second subnet IP as VPN server IP!

```

Telnet Command: vpn 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 means Remote Access User Accounts. L2I means LAN-to-LAN Profile. Specify which one will be applied by NetBios.
<index>	The index number of the profile.
<Block/Pass>	Pass - Have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. Block - When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, set it block data transmission of Netbios Naming Packet inside the tunnel.

Example

```
> vpn NetBios set 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>

Syntax Description

Parameter	Description
<i>show</i>	It means to display current setting status.
<i>default</i>	TCP maximum segment size for all the VPN connection will be set as 1360 bytes.
<i>set</i>	Use it to specify the connection type and value of MSS.
<connection type>	1-4 represent various type. 1 - PPTP 2 - L2TP 3 - IPSec 4 - L2TP over IPSec
<TCP maximum segment size range>	Each type has different segment size range. PPTP - 1 ~ 1412 L2TP - 1 ~ 1408 IPSec - 1 ~ 1381

Example

```

>vpn mss set 1 1400
% VPN TCP maximum segment size (MSS) :
  PPTP = 1400
  L2TP = 1360
  IPSec = 1360
  L2TP over IPSec = 1360
>vpn mss show
VPN TCP maximum segment size (MSS) :
  PPTP = 1400
  L2TP = 1360
  IPSec = 1360
  L2TP over IPSec = 1360

```

Telnet Command: vpn ike

This command is used to display IKE memory status and leakage list.

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>

Syntax Description

Parameter	Description
<H2I/L2I>	H2I means Host to LAN (Remote Access User Accounts). L2I means LAN-to-LAN Profile.
<index>	The index number of the profile.
<Block/Pass>	Set Block/Pass the Multicast Packets. The default is Block.

Example

```
> vpn Multicast set 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
<i>on/off</i>	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
<i>on/off</i>	on - the packets can pass through NAT. off - the packets cannot pass through NAT.

Example

```
> vpn pass2nat on
% Packets would go through by NAT when VPN disconnect!!
```

Telnet Command: 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
<i><WAN interface number></i>	Type a number to represent the physical interface. For Vigor130, the number is 1 (which means WAN1).
<i><MRU size ></i>	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
<i>value</i>	It means the number of MTU for PPP. The available range is from 1000 to 1500. For Static IP/DHCP, the maximum number will be 1500. For PPPoE, the maximum number will be 1492. For PPTP/L2TP, the maximum number will be 1460.

Example

```
> wan mtu 1100
> wan mtu ?
Static IP/DHCP (Max MSS: 1500)
PPPoE(Max MSS: 1492)
PPTP/L2TP(Max MSS: 1460)
% wan ppp_mss <MSS size: 1000 ~ 1500>
% Now: 1100
```

Telnet Command: wan DF_check

This command allows you to enable or disable the function of DF (Don't fragment)

Syntax

wan DF_check *[on]*

wan DF_check *[off]*

Syntax Description

Parameter	Description
<i>on/off</i>	It means to enable or disable DF.

Example

```
> wan DF_check on
%DF bit check enable!
> 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 enable wan connection.

Example

```
> wan enable WAN
%WAN1 enabled.
```

Telnet Command: wan forward

This command allows you to enable or disable the function of WAN forwarding. The packets are allowed to be transmitted between different WANs.

Syntax

`wan forward [on]`

`wan forward [off]`

Syntax Description

Parameter	Description
<i>on/off</i>	It means to enable or disable WAN forward.

Example

```
> wan forward ?
%WAN forwarding is Disable!

> wan forward on
%WAN forwarding is enable!
```

Telnet Command: wan status

This command allows you to display the status of WAN connection, including connection mode, TX/RX packets, DNS settings and IP address.

Example

```
> wan status
WAN1: Offline, stall=N
Mode: ---, Up Time=00:00:00
IP=---, GW IP=---
TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0
Primary DNS=0.0.0.0, Secondary DNS=0.0.0.0

PVC_WAN3: Offline, stall=N
Mode: ---, Up Time=00:00:00
IP=---, GW IP=---
TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0

PVC_WAN4: Offline, stall=N
Mode: ---, Up Time=00:00:00
IP=---, GW IP=---
TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0

PVC_WAN5: Offline, stall=N
Mode: ---, Up Time=00:00:00
IP=---, GW IP=---
TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0
```

Telnet Command: wan 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
```

Syntax Description

Parameter	Description
<i>init</i>	Set initial modem AT command (default value is "AT&FE0V1X1&D2&C1S0=0").
<i>init2</i>	Set the second initial modem AT command.
<i>dial</i>	Set dial modem AT command (default value is "ATDT*99#").
<i>pin</i>	Set PIN code for SIM card. "0":disable
<i>paponly</i>	It means PAP Only. Set the PPP authentication of the USB WAN.

	on: None. off: PAP or CHAP.
<i>backup_wait</i>	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.
<i>pipe</i>	It is for RD debug only. Please don't use it without our advice.
<i>wakeup [on/off]</i>	It is for RD debug only. Please don't use it without our advice.
<i>vid</i>	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.
<i>pid</i>	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.
<i>status</i>	Display current status of USB modem.

Example

```
> 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]`

Syntax Description

Parameter	Description
<i>show basic</i>	It means to display current VDSL status.
<i>fbk_mode</i>	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      Downstream      Unit
```

```

Actual Data Rate:      0      0      Kb/s
SNR:      0      0      0.1dB
> wan vdsl fbk_mode vdsl_only
Set VDSL fallback mode to VDSL ONLY
Reboot system to take effect
>

```

Telnet Command: wan lte

This command allows you to configure LTE WAN (for L model only).

Syntax

`wan lte auth [0/1]`

`wan lte band`

`wan lte del [index #/all]`

`wan lte pass [string]`

`wan lte quota [-<command><parameter>I...]`

`wan lte read [index #/all]`

`wan lte reboot [-<command><parameter>I...]`

`wan lte reply [-<command><parameter>I...]`

`wan lte send [number][message]`

`wan lte stus`

`wan lte tag [index #/all]`

`wan lte user [string]`

`wan lte wms [send[cdma/gwpp]/recv[cdma/gwgw]/setting]`

Syntax Description

Parameter	Description
<code>auth [0/1]</code>	Set PPP authentication of LTE WAN. 0: None. 1: PAP or CHAP.
<code>band</code>	Display working band information for LTE network connection.
<code>del [index #/all]</code>	Delete an SMS from the LTE SIM card by specifying the index number. Use "all" to delete all.
<code>pass</code>	Set the password of LTE WAN.
<code>quota [-<command><parameter>I...]</code>	Set settings of SMS Quota Limit function. Available commands with parameter are listed below: [...] 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. -d <day>: Set the refresh day. -e <0/1>: Enable or disable SMS Quota Limit function. (0: disable 1: enable) -h <hour>: Set the refresh hour. -m <0/1/2>: Set SMS quota refresh mode. (0: None 1: monthly 2: periodically)

	<p>-n <number>: Set SMS quota. The available number is between 1 and 1000000.</p> <p>-s <0/1>: Set whether to stop sending SMS after SMS quota exceeded. (0: no 1: yes)</p>
<i>read</i>	Display information of an SMS in the LTE SIM card by specifying the index number. Use "all" to display all.
<i>reboot</i>	<p>Set settings of Reboot on SMS Message function.</p> <p><command> <parameter> ...</p> <p>The available commands with parameters are listed below.</p> <p>[...] means that you can type in several commands in one line.</p> <p>-a <0/1>: Enable or disable Access Control List. (0: disable 1: enable)</p> <p>-e <0/1>: Enable or disable Reboot on SMS Message function. (0: disable 1: enable)</p> <p>-p <password>: Set the Password / PIN. This setting is necessary if this function is enabled.</p> <p>-x <number>: Set the first phone number in Access Control List.</p> <p>-y <number>: Set the second phone number in Access Control List.</p> <p>-z <number>: Set the third phone number in Access Control List.</p>
<i>reply</i>	<p>Set settings of Reply with Router Status Message function.</p> <p><command> <parameter> ...</p> <p>The available commands with parameters are listed below.</p> <p>[...] means that you can type in several commands in one line.</p> <p>-a <0/1>: Enable or disable Access Control List. (0: disable 1: enable)</p> <p>-c <0/1>: Set whether to reply with MAC address. (0: no 1: yes)</p> <p>-e <0/1>: Enable or disable Reboot on SMS Message function. (0: disable 1: enable)</p> <p>-f <0/1>: Set whether to reply with WAN1 IP address. (0: no 1: yes)</p> <p>-g <0/1>: Set whether to reply with WAN2 IP address. (0: no 1: yes)</p> <p>-h <0/1>: Set whether to reply with LTE WAN IP address. (0: no 1: yes)</p> <p>-i <0/1>: Set whether to reply with WAN4 IP address. (0: no 1: yes)</p> <p>-j <0/1>: Set whether to reply with WAN1 data usage. (0: no 1: yes)</p> <p>-k <0/1>: Set whether to reply with WAN2 data usage. (0: no 1: yes)</p> <p>-l <0/1>: Set whether to reply with LTE WAN data usage. (0: no 1: yes)</p> <p>-m <0/1>: Set whether to reply with WAN4 data usage. (0: no 1: yes)</p> <p>-n <0/1>: Set whether to reply with Router name. (0: no 1: yes)</p> <p>-p <password>: Set the Password / PIN. This setting is necessary if this function is enabled.</p> <p>-u <0/1>: Set whether to reply with Router system uptime. (0: no 1: yes)</p> <p>-v <0/1>: Set whether to reply with Router firmware version. (0: no 1: yes)</p> <p>-x <number>: Set the first phone number in Access Control List.</p> <p>-y <number>: Set the second phone number in Access Control List.</p> <p>-z <number>: Set the third phone number in Access Control List.</p>
<i>send</i>	Send an SMS message to the specified phone number through the LTE SIM card.
<i>stus</i>	Display status of LTE connection.
<i>tag</i>	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.
<i>user</i>	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.

Example

```
> 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
<i>on</i>	Enable ping detection. The IP address of the target shall be set.
<i>off</i>	Enable ARP detection (default).
<i>always_on</i>	Disable link detect, always connected(only support static IP)
<i>target</i>	Set the ping target.
<i>Target2</i>	Set the secondary ping target.

<i>Target_gw</i>	Set whether to use gateway as ping target. (1: yes 0: no) Note that USB WAN (PPP mode) cannot support PING gateway
<i>ip addr</i>	It means the IP address used for detection. Type an IP address in this field.
<i>ttl</i>	It means to set the ping TTL value (work as trace route) If you do not set any value for ttl here or just type 0 here, the system will use default setting (255) as the ttl value.
<i>interval [interval]</i>	Set the interval between each ping operation. Available setting is between 1 and 3600. The unit is second. <i>[interval]</i> : Type a value.
<i>retry [retry]</i>	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. <i>[retry]</i> : Type a number.
<i>status</i>	It means to show the current status.

Example

```

> wan detect status
WAN1: always on
WAN2: off
WAN3: off
WAN4: off
WAN5: off
> wan detect wan1 target 192.168.1.78
Set OK

> wan detect wan1 on
Set OK

> wan detect status
WAN1: on, Target=192.168.1.78, TTL=255
WAN2: off
WAN3: off
WAN4: off
WAN5: off
>

```

Telnet Command: wan lb

This command allows you to Enable/Disable for each WAN to join auto load balance member.

Syntax

```
wan lb [wan1/wan2/...] on
wan lb [wan1/wan2/...] off
wan lb status
```

Syntax Description

Parameter	Description
<i>wan1/wan2</i>	Specify which WAN will be applied with load balance.
<i>on</i>	Make WAN interface as the member of load balance.
<i>off</i>	Cancel WAN interface as the member of load balance.
<i>status</i>	Show the current status.

Example

```
> wan lb status
WAN1: on
WAN2: on
WAN3: on
WAN4: on
WAN5: on
WAN6: on
WAN7: on
```

Telnet Command: wan mvlan

This command allows you to configure multi-VLAN for WAN and LAN. It supports pure bridge mode (modem mode) between Ethernet WAN and LAN port 2~4.

Syntax

```
wan mvlan [pvc_no/status/save/enable/disable] [on/off/clear/tag tag_no] [service
type/vlan priority] [px ... ]
wan mvlan keep-tag[pvc_no][on/off]
```

Syntax Description

Parameter	Description
<i>pvc_no</i>	It means index number of PVC. There are 10 PVC, 0(Channel-1) to 9(Channel-9) allowed to be configured. However, bridge mode can be set on PVC number 2 to 9.
<i>status</i>	It means to display the whole Bridge status.
<i>save</i>	It means to save the configuration into flash of Vigor router.
<i>enable/disable</i>	It means to enable/disable the Multi-VLAN function.
<i>on/off</i>	It means to turn on/off bridge mode for the specific channel.
<i>clear</i>	It means to turn off/clear the port.
<i>tag tag_no</i>	It means to tag a number for the VLAN.

	-1: No need to add tag number. 1-4095: Available setting numbers used as tagged number.
<i>service type</i>	It means to specify the service type for VLAN. 0: Normal. 1: IGMP.
<i>vlan priority</i>	It means to specify the priority for the VALN setting. Range is from 0 to 7.
<i>px</i>	It means LAN port. Available setting number is from 2 to 4. Port number 1 is locked for NAT usage.
<i>keep tag</i>	It means Multi-VLAN packets will keep their VLAN headers to LAN.

Example

PVC 7 will map to LAN port 2/3/4 in bridge mode; service type is Normal. No tag added.

```
> > wan mvlan 7 on p2 p3 p4
PVC Bridge p1 p2 p3 p4 p5 p6 Service Type Tag Priority Keep Tag
-----
7 ON 0 0 1 1 0 0 Normal 0(OFF) 0 OFF
>
```

Telnet Command: wan multifno

This command allows you to specify a channel (in Multi-PVC/VLAN) to make bridge connection to a specified WAN interface.

Syntax

`wan multifno [channel #] [WAN interface #]`

`wan multifno status`

Syntax Description

Parameter	Description
<i>channel #</i>	There are 4 (?) channels including VLAN and PVC. Available settings are: 1=Channel 1 3=Channel 3 4=Channel 4 5=Channel 5
<i>WAN interface #</i>	Type a number to indicate the WAN interface. 1=WAN1 2=WAN2
<i>status</i>	It means to display current bridge status.

Example

```
> wan multifno 5 1
% Configured channel 5 uplink to WAN1
> wan multifno status
% Channel 3 uplink ifno: 3
% Channel 4 uplink ifno: 3
```

```

% Channel 5 uplink ifno: 3
% Channel 6 uplink ifno: 3
% Channel 7 uplink ifno: 3
>

```

Telnet Command: wan vlan

This command allows you to 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
<i>wan [#]</i>	Specify which WAN interface will be tagged.
<i>tag [value]</i>	Type a number for tagging on WAN interface.
<i>enable/disable</i>	Enable: Specified WAN interface will be tagged. Disable: Disable the function of tagging on WAN interface.
<i>stat</i>	Display current VLAN status.

Example

```

> wan vlan stat

% Interface      Pri      Tag      Enabled
% =====
% WAN1 (ADSL)    0        0
% WAN1 (VDSL)    0        0
% WAN2           0        0

```

Telnet Command: wan budget

This command allows you determine the data *traffic volume* for each WAN interface respectively to prevent from overcharges for data transmission by the ISP.

Syntax

```
wan budget wan [#] rdate [day] [hour]
```

```
wan budget wan [#] [enable/disable]
```

```
wan budget wan [#] thres [budget limit (MB)]
```

```
wan budget wan [#] gthres [budget limit (GB)]
```

```
wan budget wan [#] mode [monthly/periodic/none]
```

```
wan budget wan [#] psday [th day in periodic]
```

```
wan budget wan [#] action [action bitmap]
```

```
wan budget status
```

Syntax Description

Parameter	Description
<i>wan[#]</i>	Specify the WAN interface.

<i>rdate</i>	Specify the WAN budget refresh time. day - Available settings are from 1 to 30. hour - Available settings are from 1 to 23. E.g., wan budget wan 1 rdate 5 10 If monthly mode is selected: WAN budget will be refreshed on 5th day at 10:00 in each month If periodic mode is selected: WAN budget will be refreshed every 5 days and 10 hours
<i>enable/disable</i>	enable - Enable the function of wan budget. disable - Disable the function of wan budget.
<i>thres [budget limit (MB)]</i>	Specify the maximum value for WAN budget limit. (Unit: MB) budget limit - Type a number.
<i>gthres [budget limit (GB)]</i>	Specify the maximum value of wan budget limit. (Unit: GB) budget limit - Type a number.
<i>mode [monthly periodic none]</i>	Specify the calculation mode (monthly, periodically, or none) for WAN budget.
<i>psday [th day in periodic]</i>	It is used only when mode is set with "periodic". Specify the order of "today" in the cycle. E.g., wan budget wan 5 psday → It means "today" is the 5 th day in the billing cycle.
<i>action [action bitmap]</i>	Determine the action to be performed when it reaches the WAN budget limit. <i>action bitmap</i> - Type a total number of actions to be executed. Different numbers represent different actions. 1: shutdown wan 2: send mail alert 4: send sms alert For example, if you type "5" (5=1+4), the system will send SMS alert when WAN shutdown is detected.
<i>status</i>	Display current configuration status of WAN budget.

Example

```
> wan budget wan 1 action 5
% WAN 1 budget action set to 5
> wan budget wan 1 gthres 10
% WAN 1 budget limit set to 10 GB
```

Telnet Command: wan detect_mtu

This command allows you to run a WAN MTU Discovery. The user can specify an IPv4 target to ping and find the suitable MTU size of the WAN interface.

Syntax

```
wan detect_mtu -w [number] -i [Host/IP address] -s [base_size] -d [decrease_size] (-c [count])
```

Syntax Description

Parameter	Description
<i>-w [number]</i>	Specify the WAN interface. Value: Type the number of WAN interface. 1: WAN1; 2:WAN2....and etc.
<i>-i [Host/IP address]</i>	Specify the IPv4 target to detect. It can be an IPv4 address or domain name. Host/IP address: Type the IP address/domain name of the target.
<i>-s [base_size]</i>	Set the MTU size base for Discovery. base_size: Available setting is 1000 ~ 1500.
<i>-d [decrease size]</i>	Set the MTU size to decrease between detections. decrease size: Available setting is 1 ~ 100.
<i>-c [count]</i>	Set the maximum times of ping failure during a Discovery.

count: Available settings are 1 ~ 10. Default value is 3.

Example

```
> wan detect_mtu -w 2 -i 8.8.8.8 -s 1500 -d 30 -c 10
detecting mtu size:1500!!!

mtu size:1470!!!
```

Telnet Command: wan detect_mtu6

This command allows you to run a WAN MTU Discovery. The user can specify an IPv6 target to ping and find the suitable MTU size of the WAN interface.

Syntax

wan detect_mtu6 -w *[number]* -i *[IPv6 address]* -s *[base_size]*

Syntax Description

Parameter	Description
-w <i>[number]</i>	Specify the WAN interface number: Type the number of WAN interface. 1: WAN1; 2:WAN2....and etc.
-i <i>[IPv6 address]</i>	Specify the IPv6 target to detect. It must be an IPv6 IP address. IPv6 address: Type the IPv6 address of the target.
-s <i>[base_size]</i>	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: hspportal

This command is used to configure a profile (Hotspot Web Portal) with specified URL for accessing into or display a message when a wireless/LAN user connects to Internet through this router.

Syntax

hspportal setup -p *<profile>* [-i *<lan>*] [-s *<ssid>*] ...

hspportal setup -p *<profile>* -c

Syntax Description

Parameter	Description
-p	Indicate available profile to be configured. Number of profile: 1 /2 /3 / 4.
-i	Apply to LAN interfaces. E.g., apply LAN1 and LAN2: -i 1, 2.
-s	Apply to WLAN interfaces. E.g., apply SSID1 and SSID2: -s 1, 2.
-a	Apply to WLAN5G interfaces. E.g., apply SSID1 and SSID2: -s 1, 2.
-m	Select login mode.

	0:skip 1:click 2:social 3:pin 4:social or pin
<i>-f</i>	Configure facebook login. 0: disable. 1: enable.
<i>-g</i>	Configure google login. 0: disable. 1: enable.
<i>-h</i>	Enable HTTPS redirection. 0: disable. 1: enable.
<i>-v</i>	Enable portal detection. 0: disable. 1: enable.
<i>-i</i>	Configure APP id. For example, to configure facebook APP id, you can type: >hsportal -p 1 -f -i this_is_app_id Profile 1 set facebook login disabled ... [OK]
<i>-k</i>	Configure app key. For example, to configure google APP key, you can type: > hsportal -p 1 -g -i this_is_app_key Profile 1 set google login disabled ... [OK]
<i>-r</i>	Configure landing page mode. 0: fixed URL. 1: user request. 2: bulletin. E.g. > hsportal -p 1 -r 0 Profile 1 set landing page mode 0 ... [OK]
<i>-e</i>	Enable the specified profile.
<i>-d</i>	Disable the specified profile.
<i>-c</i>	Reset the specified profile. Number of profile: 1 /2 /3 / 4.
<i>-o</i>	Clear profiles for all clients.

Example

```

> hsportal setup -p 1 -c
Reset profile 1 ... [OK]
> hsportal setup -p 1 -r 0
Profile 1 set landing page mode 0 ... [OK]
> hsportal setup -p 2 -g 1 -k app_key_google
Profile 2 set google login enabled ... [OK]
Profile 2 set API KEY ... [OK]
>

```


Telnet Command: wl acl

This command allows the user to configure wireless access control settings.

Syntax

```
wl acl enable [ssid1 ssid2 ssid3 ssid4]
wl acl disable [ssid1 ssid2 ssid3 ssid4]
wl acl add [MAC] [ssid1 ssid2 ssid3 ssid4] [isolate]
wl acl del [MAC]
wl acl mode [ssid1 ssid2 ssid3 ssid4] [white/black]
wl acl show
wl acl showmode
wl acl clean
```

Syntax Description

Parameter	Description
<i>enable [ssid1 ssid2 ssid3 ssid4]</i>	It means to enable the settings for SSID1, SSID2, SSID3 and SSID4.
<i>disable [ssid1 ssid2 ssid3 ssid4]</i>	It means to disable the settings for SSID1, SSID2, SSID3 and SSID4.
<i>add [MAC] [ssid1 ssid2 ssid3 ssid4] [isolate]</i>	It means to associate a MAC address to certain SSID interfaces' access control settings. The isolate setting will limit the wireless client's network capabilities to accessing the wireless LAN only. [MAC] format: xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx or xx.xx.xx.xx.xx.xx
<i>del [MAC]</i>	It means to delete a MAC address entry defined in the access control list.
<i>mode [ssid1 ssid2 ssid3 ssid4] [white/black]</i>	It means to set white/black list for each SSID.
<i>wl acl show</i>	It means to show access control status.
<i>wl acl showmode</i>	It means to show the mode for each SSID.
<i>wl acl clean</i>	It means to clean all access control setting.

Example

```
> > wl acl showmode
ssid1: none
ssid2: none
ssid3: none
ssid4: none
> wl acl add 00-50-70-ff-12-70
Set Done !!
> wl acl add 00-50-70-ff-12-70 ssid1 ssid2 isolate
Set Done !!
> wl acl show
-----Enable Mac Address Filter-----
ssid1: dis  ssid2: dis  ssid3: dis  ssid4: dis
-----MAC Address Filter-----
```

Index	Attribute	MAC Address	Associated SSIDs
0		00:50:70:ff:12:70	ssid1 ssid2 ssid3 ssid4
1	s	00:50:70:ff:12:70	ssid1 ssid2

s: Isolate the station from LAN
>

Telnet Command: wl config

This command allows users to configure general settings and security settings for wireless connection.

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]*

Syntax Description

Parameter	Description
<i>mode[value]</i>	It means to select connection mode for wireless connection. Available settings are: "11bgn", "11gn", "11n", "11bg", "11g", or "11b".
<i>mode show</i>	It means to display what the current wireless mode is.
<i>channel [number]</i>	It means the channel of frequency of the wireless LAN. The available settings are 0,1,2,3,4,5,6,7,8,9,10,11,12 and 13. number=0, means Auto number=1, means Channel 1 number=13, means Channel 13.
<i>preamble [enable]</i>	It means to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. 0: disable to use long preamble. 1: enable to use long preamble.
<i>txburst [enable]</i>	It means to enhance the performance in data transmission about 40%* more (by enabling Tx Burst). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. 0: disable the function. 1: enable the funciton.
<i>ssid[ssid_num enable ssid_name [hidden_ssid]]</i>	It means to set the name of the SSID, hide the SSID if required. <i>ssid_num</i> : Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. <i>ssid_name</i> : Give a name for the specified SSID.

	<i>hidden_ssid</i> : Type 0 to hide the SSID or 1 to display the SSID
<i>Security [SSID_NUMBER][mode][key][index]</i>	<p>It means to configure security settings for the wireless connection.</p> <p><i>SSID_NUMBER</i>: Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4.</p> <p><i>mode</i>: Available settings are:</p> <p>disable: No security.</p> <p>wpa1x: WPA/802.1x Only</p> <p>wpa21x: WPA2/802.1x Only</p> <p>wpamix1x: Mixed (WPA+WPA2/802.1x only)</p> <p>wep1x: WEP/802.1x Only</p> <p>wpa2psk: WPA/PSK</p> <p>wpa2psk: WPA2/PSK</p> <p>wpamixpsk: Mixed (WPA+WPA2)/PSK</p> <p>wep: WEP</p> <p><i>key, index</i>: Moreover, you have to add keys for <i>wpa2psk</i>, <i>wpamixpsk</i> and <i>wep</i>, and specify index number of schedule profiles to be followed by the wireless connection.</p> <p>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.</p>
<i>ratectl [ssid_num enable upload download]</i>	<p>It means to set the rate control for the specified SSID.</p> <p><i>ssid_num</i>: Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4.</p> <p><i>enable</i>: It means to enable the function of the rate control for the specified SSID. 0: disable and 1:enable.</p> <p><i>upload</i>: It means to configure the rate control for data upload. The unit is kbps.</p> <p><i>download</i>: It means to configure the rate control for data download. The unit is kbps.</p>
<i>isolate [ssid_num lan member]</i>	<p>It means to isolate the wireless connection for LAN and/or Member.</p> <p><i>lan</i> - It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other.</p> <p><i>member</i> - It can make the wireless clients (stations) with the same SSID not accessing for each other.</p>

Example

```

> wl config mode 11bgn
Current mode is 11bgn
% <Note> Please restart wireless after you set the channel
> wl config channel 13
Current channel is 13
% <Note> Please restart wireless after you set the channel.
> wl config preamble 1
Long preamble is enabled
% <Note> Please restart wireless after you set the parameters.
> wl config ssid 1 enable dray
SSID Enable Hide_SSID Name
1 1 0 dray
% <Note> Please restart wireless after you set the parameters.
> wl config security 1 wpa1x
%% Configured Wlan Security Setting:
% SSID1
%% Mode: wpa1x
%% Wireless card must be reset for configurations to take effect

```

```
%% (Telnet Command: wl restart)
```

Telnet Command: wl set

This command allows users to configure basic wireless settings.

Syntax

```
wl set [SSID] [CHAN[En]]
```

```
wl set txburst [enable]
```

Syntax Description

Parameter	Description
<i>SSID</i>	It means to type the SSID for the router. The maximum character that you can use is 32.
<i>CHAN[En]</i>	It means to specify required channel for the router. <i>CHAN</i> : The range for the number is between 1 ~ 13. <i>En</i> : type <i>on</i> to enable the function; type <i>off</i> to disable the function.
<i>txburst [enable]</i>	It means to enhance the performance in data transmission about 40%* more (by enabling Tx Burst). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. 0: disable the function. 1: enable the function.

Example

```
> wl set MKT 2 on
% New Wlan Setting is:
% SSID=MKT
% Chan=2
% Wl is Enable
```

Telnet Command: wl act

This command allows users to activate wireless settings.

Syntax

```
wl act [En]
```

Syntax Description

Parameter	Description
<i>En</i>	It means to enable or disable the function of VPN isolation. 0: diable 1: enable

Example

```
> wl act on
% Set Wlan to Enable.
```

Telnet Command: wl 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]`

Syntax Description

Parameter	Description
<i>start</i>	It means to start AP scanning.
<i>set [wlist/blist/stime] [MAC]</i>	Set white list/block list/scan time. <i>wlist</i> - It means to set white list for passing. MAC address must be added in the end. e.g., <code>wl scan set wlist 001122aabbcc</code> <i>blist</i> - It means to set black list for blocking. MAC address must be added in the end. <i>stime</i> - It means to set scanning time. Time value (2-5 second) must be added in the end. e.g., <code>wl scan set time 5</code>
<i>del</i>	Remove white list/block list. e.g., <code>wl scan del wlist 001122aabbcc</code>
<i>filter</i>	Set which filter you want. <i>ssid</i> - scanning the AP based on SSID setting. <i>channel</i> - scanning the AP based on channel setting. <i>mac</i> - scanning the AP based on MAC address setting..
<i>show [0/1/2/3]</i>	It is used to show AP list. 0 - display white list 1 - display block list, 2 - display gray/unknown list, 3 - display all list

Example

```
> 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
<i>enable/disable</i>	It means to enable/disable the station management control.
<i>ssid_num</i>	It means channel selection. Available channel for 2.4G: 0/1/2/3 Available channel for 5G: 4/5/6/7.
<i>show</i>	It means to display status or configuration of the selected channel.
<i>c</i>	It means connection time. The unit is minute.
<i>r</i>	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*]

Syntax Description

Parameter	Description
<i>ssid</i>	It means the number of SSID. 1: SSID1 2: SSID2 3: SSID3 4: SSID4
<i>En</i>	It means to enable or disable the function of VPN isolation. 0: disable 1: enable

Example

```
> wl iso_vpn 1 on
% ssid: 1 isolate vpn on :1
```

Telnet Command: **wl wpa**

This command allows you to configure WPA wireless settings.

Syntax

wl wpa 1/2/3

Syntax Description

Parameter	Description
<i>wl wpa</i>	Type 1/2/3 to represent different WPA modes.

	1 - means WPA+WPA2 2 - means WPA2 Only 3 - means WPA Only
--	---

Example

```
> wl wpa 1
>
```

Telnet Command: wl wmm

This command allows users to set WMM for wireless connection. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs).

Syntax

`wl wmm ap QueIdx Aifsn Cwmin Cwmax Txop ACM`

`wl wmm bss QueIdx Aifsn Cwmin Cwmax Txop ACM`

`wl wmm ack Que0_Ack Que1_Ack Que2_Ack Que3_Ack`

`wl wmm enable SSID0 SSID1 SSID2 SSID3`

`wl wmm apsd value`

`wl wmm show`

Syntax Description

Parameter	Description
<i>ap</i>	It means to set WMM for access point.
<i>bss</i>	It means to set WMM for wireless clients.
<i>ack</i>	It means to map to the Ack policy settings of AP WMM.
<i>enable</i>	It means to enable the WMM for each SSID. 0: disable 1: enable
<i>Apsd [value]</i>	It means to enable / disable the ASPD(automatic power-save delivery) function. 0: disable 1: enable
<i>show</i>	It displays current status of WMM.
<i>QueIdx</i>	It means the number of the queue which the WMM settings will be applied to. There are four queues, best effort, background, voice, and video.
<i>Aifsn</i>	It controls how long the client waits for each data transmission.
<i>Cwmin/ Cwmax</i>	CWMin means contention Window-Min and CWMax means contention Window-Max. Specify the value ranging from 1 to 15.
<i>Txop</i>	It means transmission opportunity. Specify the value ranging from 0 to 65535.
<i>ACM</i>	It can restrict stations from using specific category class if it is enabled. 0: disable 1: enable

Example

```
> wl wmm ap 0 3 4 6 0 0
  QueIdx=0: APAifsn=3,APCwmin=4,APCwmax=6, APTxop=0,APACM=0
> wl wmm enable 1 0 1 0
  WMM_SSID0 =1, WMM_SSID1 =0,WMM_SSID2 =1,WMM_SSID3 =0
> wl wmm show
  Enable WMM: SSID0 =1, SSID1 =0,SSID2 =1,SSID3 =0
  APSD=0
  QueIdx=0: APAifsn=3,APCwmin=4,APCwmax=6, APTxop=0,APACM=0
  QueIdx=1: APAifsn=7,APCwmin=4,APCwmax=10, APTxop=0,APACM=0
  QueIdx=2: APAifsn=1,APCwmin=3,APCwmax=4, APTxop=94,APACM=0
  QueIdx=3: APAifsn=1,APCwmin=2,APCwmax=3, APTxop=47,APACM=0
  QueIdx=0: BSSAifsn=3,BSSCwmin=4,BSSCwmax=10, BSSTxop=0,BSSACM=0
  QueIdx=1: BSSAifsn=7,BSSCwmin=4,BSSCwmax=10, BSSTxop=0,BSSACM=0
  QueIdx=2: BSSAifsn=2,BSSCwmin=3,BSSCwmax=4, BSSTxop=94,BSSACM=0
  QueIdx=3: BSSAifsn=2,BSSCwmin=2,BSSCwmax=3, BSSTxop=47,BSSACM=0
  AckPolicy[0]=0: AckPolicy[1]=0,AckPolicy[2]=0,AckPolicy[3]=0
```


Telnet Command: wl ht

This command allows you to configure wireless settings.

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
<i>wl ht bw value</i>	The value you can type is 0 (for BW_20) and 1 (for BW_40).
<i>wl ht gi value</i>	The value you can type is 0 (for GI_800) and 1 (for GI_4001)
<i>wl ht badecline value</i>	The value you can type is 0 (for disabling) and 1 (for enabling).
<i>wl ht autoba value</i>	The value you can type is 0 (for disabling) and 1 (for enabling).
<i>wl ht rdg value</i>	The value you can type is 0 (for disabling) and 1 (for enabling).
<i>wl ht msdu value</i>	The value you can type is 0 (for disabling) and 1 (for enabling).
<i>wl ht txpower value</i>	The value you can type ranges from 1 - 6 (level).
<i>wl ht antenna value</i>	The value you can type ranges from 0-3. 0: 2T3R 1: 2T2R 2: 1T2R 3: 1T1R
<i>wl ht greenfield value</i>	The value you can type is 0 (for mixed mode) and 1 (for green field).

Example

```
> wl ht bw value 1
BW=0
<Note> Please restart wireless after you set new parameters.
> wl restart
Wireless restart.....
```

Telnet Command: wl restart

This command allows you to restart wireless setting.

Example

```
> wl restart
Wireless restart.....
```

Telnet Command: wl wds

This command allows you to configure WDS settings.

Syntax

`wl wds mode [value]`

`wl wds security [value]`

`wl wds ap [value]`

`wl wds hello [value]`

`wl wds status`

`wl wds show`

`wl wds mac [value]`

`wl wds flush`

Syntax Description

Parameter	Description
<code>mode [value]</code>	It means to specify connection mode for WDS. [value]: Available settings are : d: Disable b: Bridge r: Repeater
<code>security [value]</code>	It means to configure security mode with encrypted keys for WDS. <code>mode</code> : Available settings are: disable: No security. wep: WEP wpapsk [key]: WPA/PSK wpa2psk [key]: WPA2/PSK <code>key</code> : Moreover, you have to add keys for <code>wpapsk</code> , <code>wpa2psk</code> , and <code>wep</code> , and specify index number of schedule profiles to be followed by the wireless connection. WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8-63 ASCII text string or 64 Hexadecimal digit format. e.g., <code>wl dual wds security disable</code> <code>wl dual wds security wep 12345</code> <code>wl dual wds security wpa2psk 12345678</code>
<code>ap [value]</code>	It means to enable or disable the AP function. Value: 1 - enable the function. 0 - disable the function.
<code>hello [value]</code>	It means to send hello message to remote end (peer). Value: 1 - enable the function.

	0 - disable the function.
<i>status</i>	It means to display WDS link status for 2.4GHz connection.
<i>show</i>	It means to display current WDS settings.
<i>mac add [index addr]</i>	add <i>[index addr]</i> - Add the peer MAC entry in Repeater/Bridge WDS MAC table.
<i>mac clear/disable/enable [index/all]</i>	clear/disable/enable <i>[index/all]</i> - Clear, disable, enable the specified or all MAC entries in Repeater/Bridge WDS MAC table. e.g, wl dual wds mac enable 1
<i>flush</i>	It means to reset all WDS setting.

Example

```
> wl wds status
Please enable WDS hello function first.

> wl wds hello 1
% <Note> Please restart router after you set the parameters.

> wl wds status
```

Telnet Command: wl apcli

This command allows users to configure AP client mode for wireless connection (2.4GHz).

Syntax

```
wl apcli show
wl apcli enable [1/0]
wl apcli security [mode]
wl apcli ssid [ssid_name]
wl apcli bssid [mac address]
```

Syntax Description

Parameter	Description
<i>show</i>	Display current status of wireless AP client.
<i>enable [1/0]</i>	It means to enable wireless 2.4GHz AP client mode. 1 - enable 0 - disable
<i>security [mode]</i>	There are several modes to be selected: Disable - disable the security settings. wpa2psk [key] - WPA Pre-shared Key will be used. Keys must start with 0x to be identified as a Hexadecimal number key. WPA keys must be in 8-63 ASCII string or 64 Hexadecimal digit format. wpa2psk [key] - WPA2 Pre-shared Key will be used. Keys must start with 0x to be identified as a Hexadecimal number key. WPA keys must be in 8-63 ASCII string or 64 Hexadecimal digit format. wpa2mixpsk [key] - WPA Mixed Pre-shared Key will be used. Keys must start with 0x to be identified as a Hexadecimal number key. WPA keys must be in 8-63 ASCII string or 64 Hexadecimal digit format. wep [key] [index] - WEP key will be used. You need to type the key string and specify the index number of the profile to be applied.

	WEP keys must be in 5/13 ASCII string or 10/26 Hexadecimal digit format.
<i>ssid [ssid_name]</i>	Specify the SSID for wireless 2.4GHz AP client.
<i>bssid</i>	Type the MAC address for wireless 2.4GHz AP client.

Example

```
> wl apcli enable 1
Wireless AP-Clinet is enabled
> wl apcli show
% Wireless AP-Clinet is enabled
% Current SSID is test
%% Security Mode: disable
% Wireless client is disconnected
%% data rate=---, mode=---, signal=0%
```

Telnet Command: wl btncctl

This command allows you to enable or disable wireless button control.

Syntax

`wl btncctl [value]`

Syntax Description

Parameter	Description
<i>value</i>	0: disable 1: enable

Example

```
> wl btncctl 1
Enable wireless botton control
Current wireless botton control is on
>
```

Telnet Command: wl iwpriv

This command is reserved for RD debug. Do not use them.

Telnet Command: wl stalist

This command is used to display the wireless station which accessing Internet via Vigor router.

Syntax

`wl stalist`

Example

```
> wl stalist
wl stalist show      : show station list
wl stalist num       : show number of stations
wl stalist neighbor  : show neighbor station list
```

Telnet Command: wl set8021x

This command allows you to configure the external or internal server used by Vigor router for wireless authentication.

Syntax

```
wl set8021x -t [0/1]
```

```
wl set8021x -v
```

Syntax Description

Parameter	Description
-t	Specify the type (external or internal) of wireless authentication server. 0 - Indicate the external RADIUS server. 1 - Indicate the local 802.1x server.
-v	View the settings of 802.1x.

Example

```
> wl set8021x -t 1
% <Note> Please restart wireless after you set the parameters.
> wl set8021x -v
802.1X type is : Local 802.1X
>
```

Telnet Command: wl bndstrg

This command allows users to configure settings for Band Steering (2.4GHz).

Syntax

```
wl bndstrg show
```

```
wl bndstrg enable [1/0]
```

```
wl bndstrg chk_time [value]
```

Syntax Description

Parameter	Description
show	Display current status for Band Steering function.
enable [1/0]	It means to enable wireless 2.4GHz AP client mode. 1 - enable 0 - disable
chk_time [value]	If the wireless station does not have the capability of 5GHz network connection, the system shall wait and check for several seconds (15 seconds, in default) to make the 2.4GHz network connection. Specify the time limit for Vigor router to detect the wireless client. [value] - 1 to 60 seconds.

Example

```
> wl bndstrg show
band steering: disable
chk_time: 15 sec
```

```

> wl bndstrg chk_time 50 30
argv[0]:chk_time, argv[1]:50, argv[2]:30

%% Wireless card must be reset for configurations to take effect
%% (Telnet Command: wl restart)

```

Telnet Command: wl artfns

This command allows users to configure airtime fairness function for wireless (2.4GHz) connection.

Syntax

```

wl artfns enable [value]
wl artfns trg_num [value]
wl artfns show

```

Syntax Description

Parameter	Description
<i>enable [value]</i>	It means to enable wireless airtime fairness function. 1 - enable 0 - disable
<i>Trg_num [value]</i>	Set a threshold when the active station number achieves this number, the airtime fairness function will be applied. Available values will be 2 to 64.
<i>show</i>	Display current status (enable or disable) and triggering client number for airtime fairness function.

Example

```

> wl artfns enable 1
> wl artfns trg_num 3
> wl artfns show
airtime fairness: enable
trg_num: 3
>

```

Telnet Command: wl drays

This command allows the user to configure settings for Roaming for wireless clients.

Syntax

```

wl drays set [mode] [rs_low] [rs_low_security] [delta]
wl drays restart
wl drays show

```

Syntax Description

Parameter	Description
<i>set [mode] [rs_low] [rs_low_security] [delta]</i>	Select a mode for roaming. 0 - disable 1 - Strictly Minimum RSSI 2 - Minimum RSSI rs_low - Set a value of Strictly Minimum RSSI (62-86).

	rs_low_security - Set a value of Minimum RSSI (62-86). delta - Set a value of Adjacent AP RSSI (1-20).
<i>restart</i>	Restart to activate roaming function.
<i>show</i>	Display current configuration of roaming function.

Example

```
> wl drayrs show
% Mode : Disable
% rs_low      : -73
% rs_low_secure : -66
% delta      : 5
>
```

Telnet Command: wl_dual acl

This command allows the user to configure wireless (5GHz) access control settings.

Syntax

```
wl dual acl enable [ssid1 ssid2 ssid3 ssid4]
wl dual acl disable [ssid1 ssid2 ssid3 ssid4]
wl dual acl add [MAC][ssid1 ssid2 ssid3 ssid4][isolate]
wl dual acl del [MAC]
wl dual acl mode [ssid1 ssid2 ssid3 ssid4] [white/black]
wl dual acl show
wl dual acl showmode
wl dual acl clear
```

Syntax Description

Parameter	Description
<i>enable</i> [ssid1 ssid2 ssid3 ssid4]	It means to enable the settings for SSID1, SSID2, SSID3 and SSID4.
<i>disable</i> [ssid1 ssid2 ssid3 ssid4]	It means to disable the settings for SSID1, SSID2, SSID3 and SSID4.
<i>add</i> [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-xx or xx:xx:xx:xx:xx:xx or xx.xx.xx.xx.xx.xx
<i>isolate</i>	It means to isolate the wireless connection of the wireless client (identified with the MAC address) from LAN.
<i>del</i> [MAC]	It means to delete a MAC address entry defined in the access control list. [MAC] format: xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx or xx.xx.xx.xx.xx.xx
<i>mode</i> [ssid1 ssid2 ssid3 ssid4] [white/black]	It means to set white/black list for each SSID.
<i>show</i>	It means to display current status of access control.
<i>showmode</i>	It means to show the mode for each SSID.

clear

It means to clear all of the access control settings.

Example

```
> wl_dual acl showmode
SSID1: None
SSID2: None
SSID3: None
SSID4: None
> wl_dual acl add 00-50-70-ff-12-80
> wl_acl add 00-50-70-ff-12-80 ssid1 ssid2 isolate
Set Done !!
> wl_acl show
-----Enable Mac Address Filter-----
ssid1: dis  ssid2: dis  ssid3: dis  ssid4: dis
-----MAC Address Filter-----
Index  Attribute      MAC Address      Associated SSIDs
  0      s             00:50:70:ff:12:80  ssid1 ssid2

s: Isolate the station from LAN
```

Telnet Command: *wl_dual apscan*

This command is used to scan Access Point installed near the location of Vigor router.

Syntax

wl_dual apscan start

wl_dual apscan show

Syntax Description

Parameter	Description
<i>start</i>	It means to execute the AP scanning.
<i>show</i>	It means to display the content of the AP list.

Example

```
> wl_dual apscan start
> wl_dual apscan show
AP scan is ongoing.
> wl_dual apscan ?
% wl_dual apscan [start/show]
% start: do AP scan
% show: show AP list

> wl_dual apscan show
5G Access Point List :
BSSID           Channel  SSID
```


Telnet Command: wl_dual cardmac

Example

```
> wl_dual cardmac  
Card MAC: 54:2a:a2:37:00:ef
```

Telnet Command: wl_dual config

This command allows users to configure general settings and security settings for wireless connection (5GHz).

wl_dual config enable *[value]*

wl_dual config enable show

wl_dual config mode *[value]*

wl_dual config mode show

wl_dual config channel *[number]*

wl_dual config channel show

wl_dual config preamble *[enable]*

wl_dual config preamble show

wl_dual config ssid *[ssid_num enable ssid_name]*

wl_dual config ssid hide *[ssid_num enable]*

wl_dual config ssid show

wl_dual config ratectl *[ssid_num enable upload download]*

wl_dual config ratectl show

wl_dual config isolate lan *[ssid_num enable]*

wl_dual config isolate member *[ssid_num enable]*

wl_dual config isolate vpn *[ssid_num enable]*

wl_dual config isolate show

Syntax Description

Parameter	Description
<i>enable[value]</i>	It means to enable/disable the 5GHz wireless function. 1: enable 0: disable
<i>show</i>	It means to display if 5G wireless function is enabled or not.
<i>mode[value]</i>	It means to select connection mode for wireless connection. Available settings are: "11a", "11n_5g", "11n" and "11an".
<i>mode show</i>	It means to display what the current wireless mode is.
<i>channel [number]</i>	It means the channel of frequency of the wireless LAN. The available settings are: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136 and 140. number=0, means Auto number=36, means Channel 36 Number=52, means Channel 52.
<i>channel show</i>	It means to display what the current channel is.
<i>preamble [enable]</i>	It means to define the length of the sync field in an 802.11 packet.

	<p>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.</p> <p>0: disable to use long preamble. 1: enable to use long preamble.</p>
<i>preamble show</i>	It means to display if preamble is enabled or not.
<i>ssid[ssid_num enable ssid_name]</i>	<p>It means to set the name of the SSID, hide the SSID if required.</p> <p><i>ssid_num</i>: Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. <i>ssid_name</i>: Give a name for the specified SSID.</p>
<i>ssid hide [ssid_num enable]</i>	<p>It means to hide the name of the SSID if required.</p> <p><i>ssid_num</i>: Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. <i>enable</i>: Type 0 to hide the SSID or 1 to display the SSID.</p>
<i>ssid show</i>	It means to display a table of SSID configuration.
<i>ratectl [ssid_num enable upload download]</i>	<p>It means to set the rate control for the specified SSID.</p> <p><i>ssid_num</i>: Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. <i>enable</i>: It means to enable the function of the rate control for the specified SSID. 0: disable and 1:enable. <i>upload</i>: It means to configure the rate control for data upload. The unit is kbps. <i>download</i>: It means to configure the rate control for data download. The unit is kbps. (example: <i>wl dual config ratectl 1 1 25 25</i>)</p>
<i>ratectl show</i>	It means to display the data transmission rate (upload and download) for SSID1, SSID2, SSID3 and SSID4.
<i>isolate lan [ssid_num enable]</i>	<p>It means to isolate the wireless connection from LAN.</p> <p>It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other.</p> <p><i>ssid_num</i>: Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. <i>enable</i>: It means to enable such function. 0: disable and 1:enable</p>
<i>isolate member [ssid_num enable]</i>	<p>It means to isolate the wireless connection from Member.</p> <p>It can make the wireless clients (stations) with the same SSID not accessing for each other.</p> <p><i>ssid_num</i>: Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. <i>enable</i>: It means to enable such function. 0: disable and 1:enable.</p>
<i>isolate vpn [ssid_num enable]</i>	<p>It means to isolate the wireless connection from VPN.</p> <p><i>ssid_num</i>: Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. <i>enable</i>: It means to enable such function. 0: disable and 1:enable.</p>
<i>isolate show</i>	It means to display the status of wireless isolation.

Example

```

> wl_dual config mode 11a
Current mode is 11a
% <Note> Please restart 5G wireless after you set the channel
> wl_dual config channel 60
Current channel is 60
% <Note> Please restart 5G wireless after you set the channel.
> wl_dual config preamble 1
Long preamble is enabled
% <Note> Please restart 5G wireless after you set the parameters.

```

```

> wl_dual config ssid 1 enable dray
SSID Enable Hide_SSID Name
 1    1     0         dray
% <Note> Please restart 5G wireless after you set the parameters.
> wl_dual config ssid show
SSID Enable Hide_SSID Name
 1    1     0         dray
 2    0     0         DrayTek_5G_Guest
 3    0     0
 4    0     0

```

Telnet Command: `wl_dual restart`

This command allows you to restart wireless setting (5GHz).

Example

```

> wl_dual restart
5G wireless restart.....

```

Telnet Command: `wl_dual security`

This command allows users to configure security settings for the wireless connection (5GHz).

Syntax

`wl_dual security` [*SSID_NUMBER*] [*mode*][*key*][*index*]

`wl_dual security show`

Syntax Description

Parameter	Description
<i>Security</i> [<i>SSID_NUMBER</i>] [<i>mode</i>][<i>key</i>][<i>index</i>]	<p><i>SSID_NUMBER</i>: Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4.</p> <p><i>mode</i>: Available settings are:</p> <p>disable: No security.</p> <p>wpa1x: WPA/802.1x Only</p> <p>wpa21x: WPA2/802.1x Only</p> <p>wpamix1x: Mixed (WPA+WPA2/802.1x only)</p> <p>wep1x: WEP/802.1x Only</p> <p>wpapsk: WPA/PSK</p> <p>wpa2psk: WPA2/PSK</p> <p>wpamixpsk: Mixed (WPA+WPA2)/PSK</p> <p>wep: WEP</p> <p><i>key, index</i>: Moreover, you have to add keys for <i>wpapsk</i>, <i>wpa2psk</i>, <i>wpamixpsk</i> and <i>wep</i>, and specify index number of schedule profiles to be followed by the wireless connection.</p> <p>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.</p>
<i>show</i>	It means to display current mode selection for each SSID.

Example

```
> wl_dual security 1 wpa2psk 123456789e
% <Note> Please restart 5G wireless after you set the parameters.

> wl_dual security show
%% 5G Wireless LAN Security Settings:
% SSID1
%% Mode: WPA2/PSK
% SSID2
%% Mode: Disable
% SSID3
%% Mode: Disable
% SSID4
%% Mode: Disable
```

Telnet Command: wl_dual stalist

This command is used to display the wireless station which accessing Internet via Vigor router.

Syntax

```
wl_dual stalist
```

Example

```
> wl_dual stalist
5G Wireless Station List :

Index  Status  IP Address      MAC Address      Associated with

Status Codes :
C: Connected, No encryption.
E: Connected, WEP.
P: Connected, WPA.
A: Connected, WPA2.
B: Blocked by Access Control.
N: Connecting.
F: Fail to pass WPA/PSK authentication.
```

Telnet Command: wl_dual wds

This command allows users to configure WDS for wireless connection (5GHz).

Syntax

```
wl_dual wds mode [value]
wl_dual wds security [value]
wl_dual wds ap [value]
wl_dual wds hello [value]
wl_dual wds status
```

```

wl_dual wds show
wl_dual wds mac add [index addr]
wl_dual wds mac clear/disable/enable [index/all]
wl_dual wds flush

```

Syntax Description

Parameter	Description
<code>mode [value]</code>	It means to specify connection mode for WDS. [value]: Available settings are : d: Disable b: Bridge r: Repeater
<code>security [value]</code>	It means to configure security mode with encrypted keys for WDS. <i>mode</i> : Available settings are: disable: No security. wep: WEP wpapsk [key]: WPA/PSK wpa2psk [key]: WPA2/PSK <i>key</i> : Moreover, you have to add keys for <i>wpapsk</i> , <i>wpa2psk</i> , and <i>wep</i> , and specify index number of schedule profiles to be followed by the wireless connection. WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8-63 ASCII text string or 64 Hexadecimal digit format. e.g., <pre>wl_dual wds security disable wl_dual wds security wep 12345 wl_dual wds security wpa2psk 12345678</pre>
<code>ap [value]</code>	It means to enable or disable the AP function. Value: 1 - enable the function. 0 - disable the function.
<code>hello [value]</code>	It means to send hello message to remote end (peer). Value: 1 - enable the function. 0 - disable the function.
<code>status</code>	It means to display WDS link status for 5GHz connection.
<code>show</code>	It means to display current WDS settings.
<code>mac add [index addr]</code>	<code>add [index addr]</code> - Add the peer MAC entry in Repeater/Bridge WDS MAC table.
<code>mac clear/disable/enable [index/all]</code>	<code>clear/disable/enable [index/all]</code> - Clear, disable, enable the specified or all MAC entries in Repeater/Bridge WDS MAC table. e.g, <pre>wl_dual wds mac enable 1</pre>
<code>flush</code>	It means to reset all WDS setting.

Example

```

> wl_dual wds status
Please enable WDS hello function first.

> wl_dual wds hello 1
% <Note> Please restart router after you set the parameters.
> wl dual wds mode b
> wl dual wds security wep

```

```

>
>
> wl_dual wds show
5G Wireless WDS Setting

Mode : Bridge
Security : WEP
AP Function : Enable
Send Hello Function : Enable

Bridge :
Index  Enable  MAC Address
  1      0    00:00:00:00:00:00
  2      0    00:00:00:00:00:00
  3      0    00:00:00:00:00:00
  4      0    00:00:00:00:00:00

Repeater :
Index  Enable  MAC Address
  5      0    00:00:00:00:00:00
  6      0    00:00:00:00:00:00
  7      0    00:00:00:00:00:00
  8      0    00:00:00:00:00:00
> wl_dual wds wep 12345
% <Note> Please restart router after you set the parameters.

```

Telnet Command: `wl_dual wps`

This command allows users to configure WPS for wireless connection (5GHz).

Syntax

`wl_dual wps enable [value]`

`wl_dual wps pbc`

`wl_dual wps pin [code]`

`wl_dual wps show`

Syntax Description

Parameter	Description
<code>enable [value]</code>	It means to enable WPS. 1 - enable 0 - disable
<code>pbc</code>	It means to start WPS by pressing the WLAN ON/OFF WPS button on Vigor router.
<code>pin [code]</code>	It means to start WPS by using client PIN code. [code]: Client PIN code (digit number).
<code>show</code>	It means to display current WPS settings.

Example

```

> wl_dual wps enable 1
WPS is enabled.

```

```

> wl_dual wps pin 88563337
WPS has triggered by PIN code.
The AP will wait for WPS request from your client for 2 minutes...

```

Telnet Command: `wl_dual set8021x`

This command allows you to configure the external or internal server used by Vigor router for wireless authentication (5GHz).

Syntax

```
wl_dual set8021x -t [0/1]
```

```
wl_dual set8021x -v
```

Syntax Description

Parameter	Description
-t	Specify the type (external or internal) of wireless authentication server. 0 - Indicate the external RADIUS server. 1- Indicate the local 802.1x server.
-v	View the settings of 802.1x.

Example

```

> wl_dual set8021x -t 1
% <Note> Please restart 5G wireless after you set the parameters.
> wl_dual set8021x -v
802.1X type is : Local 802.1X
>

```

Telnet Command: `wl_dual apcli`

This command allows users to configure AP client mode for wireless connection (5GHz).

Syntax

```
wl_dual apcli show
```

```
wl_dual apcli enable [value]
```

```
wl_dual apcli security [mode]
```

```
wl_dual apcli ssid [ssid_name]
```

```
wl_dual apcli bssid
```

Syntax Description

Parameter	Description
<i>show</i>	Display current status of wireless AP client.
<i>enable [value]</i>	It means to enable wireless 5GHz AP client mode. 1 - enable 0 - disable
<i>Security [mode]</i>	There are several modes to be selected: Disable - disable the security settings. wpa-psk [key] - WPA Pre-shared Key will be used. Keys must start with 0x to be identified as a Hexadecimal number key. WPA keys

	<p>must be in 8-63 ASCII string or 64 Hexadecimal digit format.</p> <p>wpa2psk [key] - WPA2 Pre-shared Key will be used. Keys must start with 0x to be identified as a Hexadecimal number key. WPA keys must be in 8-63 ASCII string or 64 Hexadecimal digit format.</p> <p>wpamixpsk [key] - WPA Mixed Pre-shared Key will be used. Keys must start with 0x to be identified as a Hexadecimal number key. WPA keys must be in 8-63 ASCII string or 64 Hexadecimal digit format.</p> <p>wep [key] [index] - WEP key will be used. You need to type the key string and specify the index number of the profile to be applied. WEP keys must be in 5/13 ASCII string or 10/26 Hexadecimal digit format.</p>
<i>ssid</i> [<i>ssid_name</i>]	Specify the SSID for wireless 5GHz AP client.
<i>bssid</i>	Type the MAC address for wireless 5GHz AP client.

Example

```

> wl_dual apcli enable 1
Wireless 5G AP-Clinet is enabled
Vigor> wl_dual apcli show
% Wireless 5G AP-Clinet is enabled
% Current SSID is
%% Security Mode: disable
% Wireless 5G client is disconnected
%% data rate=---, mode=---, signal=0%
> wl_dual apcli ssid carrie
% <Note> Please restart wireless 5g after you set the parameters.
Current SSID is carrie

```

Telnet Command: wl_dual artfns

This command allows users to configure airtime fairness function for wireless (5GHz) connection.

Syntax

`wl_dual artfns enable [value]`

`wl_dual artfns trg_num [value]`

`wl_dual artfns show`

`wl_dual artfns status`

Syntax Description

Parameter	Description
<i>enable</i> [value]	It means to enable wireless airtime fairness function. 1 - enable 0 - disable
<i>Trg_num</i> [value]	Set a threshold when the active station number achieves this number, the airtime fairness function will be applied. Available values will be 2 to 64.
<i>show</i>	Display current status (enable or disable) and triggering client number for airtime fairness function.
<i>status</i>	Display whether the function of airtime fairness is enabled or disabled.

Example

```
> wl_dual artfns show
airtime fairness for 5G: disable
trg_num: 2
> wl_dual artfns status
airtime fairness for 5G is disabled !!!

> wl_dual artfns enable 0
> wl_dual artfns trg_num 2
> wl_dual artfns show
airtime fairness for 5G: disable
trg_num: 2
> wl_dual artfns status
airtime fairness for 5G is disabled !!!
```

Telnet Command: wl_dual drayrs

This command allows the user to configure settings for Roaming for wireless clients.

Syntax

wl_dual drayrs set [mode] [rs_low] [rs_low_security] [delta]

wl_dual drayrs restart

wl_dual drayrs show

Syntax Description

Parameter	Description
<i>set [mode] [rs_low] [rs_low_security] [delta]</i>	Select a mode for roaming. 0 - disable 1 - Strictly Minimum RSSI 2 - Minimum RSSI rs_low - Set a value of Strictly Minimum RSSI (62-86). rs_low_security - Set a value of Minimum RSSI (62-86). delta - Set a value of Adjacent AP RSSI (1-20).
<i>restart</i>	Restart to activate roaming function.
<i>show</i>	Display current configuration of roaming function.

Example

```
> wl_dual drayrs show
% Mode : Disable
% rs_low      : -73
% rs_low_secure : -66
% delta      : 5
> wl_dual drayrs set 1 68 66 2
> wl_dual drayrs show
% Mode : Strictly Minimum RSSI
% rs_low      : -68
% rs_low_secure : -66
% delta      : 2
```

Telnet Command: radius

This command allows you to configure detailed settings for RADIUS server

Syntax

radius enable [0/1]

radius authport [port number]

radius set_auth_method [method idx]

radius client [add] [idx] -i [address] -m [mask] -p [prefix] -l [length] -s [secret]

radius client [del] [idx]

radius show

radius set_dot1x_phase1 -e [method_idx]

radius set_dot1x_phase1 -d [method_idx]

radius set_dot1x_phase2 -e [method_idx]

radius set_dot1x_phase2 -d [method_idx]

Syntax Description

Parameter	Description
<i>enable</i> [0/1]	Enable (1) or disable (0) the RADIUS server.
<i>authport</i> [port number]	Configure the port number for authentication. Port number: Available range is from 0 to 65535. Default value is "1812".
<i>set_auth_method</i> [method idx]	Specify which method will be used for authentication. Method idx: "0" is "Only PAP"; "1" is "PAP/CHAP/MS-CHAP/MS-CHAPv2".
<i>client add</i>	Specify a client to be authenticated by RADIUS server by typing required information as follows: -i [address]: client IPv4 address(domain) -m [mask]: client IPv4 mask -p [prefix]: client IPv6 prefix -l [length]: client IPv6 prefix length -s [secret]: shared secret ex: radius client add 1 -i 192.168.1.1 -m 255.255.255.0 -s 123
<i>client [del] [idx]</i>	<i>del</i> - Delete related settings for selected client. <i>idx</i> - Specify the index number of client profiles.
<i>show</i>	Display the status of RADIUS server.
<i>enable_dot1x</i> [0/1]	Enable (1) or disable (0) the 802.1X Authentication function of RADIUS Server. Default is disabled.
<i>set_dot1x_phase1</i> [method_idx]	Set the phase1 method for 802.1X authentication of RADIUS server. <i>method_idx</i> - Specify which method will be used. At present, dot1x_phase1 can only support PEAP now. So only "1" can be used for it.
<i>set_dot1x_phase2</i> [method_idx]	Set the phase2 method for 802.1X authentication of RADIUS server. <i>method_idx</i> - Specify which method will be used. Dot1x_phase2 can only support MS-CHAPv2 now. So only "1" can be used for it.
-e	Set method for dot1x_phase1 or dot1x_phase2.
-d	Delete method for dot1x_phase1 or dot1x_phase2.

Example

```
> radius client add 1 -i 192.168.1.1 -m 255.255.255.0 -s 123
```

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.

Telnet Command: local_8021x

The command is used to configure general settings for Local 802.1X server built in Vigor router.

Syntax

```
local_8021x enable [0/1]
local_8021x set_localdot1x_phase1 options...
local_8021x set_localdot1x_phase2 options...
local_8021x show
```

Syntax Description

Parameter	Description
<i>enable</i>	Enable or disable the configuration. 0: disable. 1: enable.
set_localdot1x_phase1	Only support PEAP now. The method_idx for such phase1 is "1".
set_localdot1x_phase2	Only support MS-CHAPv2 now. The method_idx for such phase2 is "1".
options	-e [method_idx]: set method. e.g, local_8021x set_localdot1x_phase1 -e 1 -d: delete mehod. e.g, local_8021x set_localdot1x_phase1 -d
show	Display current settings of local 802.1x server.

Example

```
> local_8021x show
% Local 802.1X enable: enable
% phase1 support method: [PEAP]
% phase2 support method: [None]
```

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
<i>MAC Address</i>	It means the MAC address of the host.
<i>IP address</i>	It means the LAN IP address of the host. If you want to wake up LAN host by using IP address, be sure that that IP address has been bound with the MAC address (IP BindMAC).
<i>on/off/any</i>	It means to enable or disable the function of WOL from WAN. on: enable off: disable any: It means any source IP address can pass through NAT and wake up the LAN client. This command will allow the user to choose whether WoL packets can be passed from the Internet to the LAN network from a specific WAN interface.
<i>[idx][ip address] [mask]</i>	It means the index number (from 1 to 4). These commands will allow the user to configure the LAN clients that the user may wake up from the Internet through the use of the WoL packet. <i>ip address</i> - It means the WAN IP address. <i>mask</i> - It means the mask of the IP address.

Example

```
> wol fromWan on
> wol fromWan_Setting 1 192.168.1.45 255.255.255.0
>
```

Telnet Command: user

The command is used to create new user account profiles.

Syntax

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]

Syntax Description

Parameter	Description
<i>set</i>	It means to configure general setup for the user management.
<i>edit</i>	It means to modify the selected user profile.
<i>account</i>	It means to set time and data quota for specified user account.
<i>User Set</i>	
<i>-e</i>	Enable User management function.
<i>-d</i>	Disable User management function.
<i>-a</i> [Profile idx][User name][IP_Address]	It means to pass an IP Address. <i>Profile idx</i> - type the index number of the selected profile. <i>User name</i> - type the user name that you want it to pass. <i>IP_Address</i> - type the IP address that you want it to pass.
<i>-l all</i> <i>-l userl</i> <i>-l ip</i>	Show online user. <i>all</i> - all of the users will be displayed on the screen. <i>user name</i> - 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.
<i>-o</i>	It means to show user account information. e.g., <i>-o</i>
<i>-c</i> [user name] <i>-c all</i>	Clear the user record. <i>user name</i> - type the user name that you want to get clear corresponding record. <i>all</i> - all of the records will be removed.
<i>-buser</i> [user name] <i>-b ip</i> [ip address]	Block specifies user or IP address. <i>user name</i> - type the user name that you want to block. <i>ip address</i> -- type the IP address that you want to block.
<i>-u user</i> [user name] <i>-u ip</i> [ip address]	Unblock specifies user or IP address. <i>user name</i> - type the user name that you want to unblock. <i>ip address</i> -- type the IP address that you want to unblock.
<i>-r</i> [user name all]	Remove the user record. <i>user name</i> - type the name of the user profile. <i>all</i> - all of the user profile settings will be removed.
<i>-q</i>	It means to trigger the alert tool to do authentication.
<i>-s</i>	It means to set login service. 0:HTTPS 1:HTTP e.g., <i>-s 1</i>
<i>User edit</i>	

<i>PROFILE_IDX</i>	Type the index number of the profile that you want to edit.
<i>-e</i>	Enable User profile function.
<i>-d</i>	Disable User profile function.
<i>-n</i>	It means to set a user name for a profile. e.g., <i>-n forttest</i>
<i>-p</i>	It means to configure user password. e.g., <i>-p 60forttest</i>
<i>-t</i>	It means to enable /disable time quota limitation for user profile 0:Disable 1:Enable
<i>-u</i>	It means to enable /disable data quota limitation for user profile 0:Disable 1:Enable
<i>-i</i>	It means to set idle time. e.g., <i>-i 60</i>
<i>-q</i>	set time quota It means to set time quota of the user profile. e.g., <i>-q 200</i>
<i>-r</i>	It means to set data quota. e.g., <i>-r 1000</i>
<i>-w</i>	It means to specify the data quota unit (MB/GB). e.g., <i>-w MB</i>
<i>-s</i>	It means to set schedule index. Available settings are" sch_idx1,sch_idx2,sch_idx3, and sch_idx4.
<i>-m</i>	It means to set the maximum login user number. e.g., <i>-m 200</i>
<i>-x</i>	It means to set external server authentication 0: None 1: LDAP 2: Radius 3: TACAS e.g., <i>-x 2</i>
<i>-v</i>	It means to view user profile(s).
<i>User account</i>	
<i>USER_NAME</i>	It means to type a name of the user account.
<i>-d</i>	It means to enable /disable data quota limitation for user account. 0:Disable 1:Enable
<i>-q</i>	It means to set account time quota. e.g., <i>-q 200</i>
<i>-r</i>	It means to set account data quota. e.g., <i>-r 1000</i>
<i>-t</i>	It means to enable /disable time quota limitation for user account. 0:Disable 1:Enable
<i>-w</i>	It means to set data quota unit (MB/GB).

Example

```
> user account admin -d 1
Enable the [admin] data quota limited
```

Telnet Command: appqos

The command is used to configure QoS for APP.

Syntax

appqos view

appqos enable [0/1]

appqos traceable [-v | -e AP_INDEX CLASS | -d AP_INDEX]

appqos untraceable [-v | -e AP_INDEX CLASS | -d AP_INDEX]

Syntax Description

Parameter	Description
<i>view</i>	It means to display current status of APP QoS.
<i>enable[0/1]</i>	It means to enable or disable the function of APP QoS.
<i>traceable/ untraceable</i>	The APPs are divided into traceable and untraceable based on their properties.
<i>-v</i>	It means to view the content of all traceable APs. Use "appqos traceable -v" to display all of the traceable APS with specified index number. Use "appqos untraceable -v" to display all of the untraceable APS with specified index number.
<i>-e</i>	It means to enable QoS for application(s) and assign QoS class.
<i>AP_INDEX</i>	Each index number represents one application. Index number: 50, 51, 52, 53, 54, 58, 60, 62, 63, 64, 65, 66, 68 are used for 13 traceable APPs. Index number: 0-49, 55-59, 61, 67, 69, and 70-123 are used for 125 untraceable AP.
<i>CLASS</i>	Specifies the QoS class of the application, from 1 to 4 1:Class 1, 2:Class 2, 3:Class 3, 4:Other Class
<i>-d</i>	It means to disable QoS for application(s).

Example

```
> appqos enable 1
APP QoS set to Enable.
> appqos traceable -e 68 2
TELNET: ENABLED, QoS Class 2.
```

Telnet Command: nand bad /nand usage

"NAND usage" is used to display NAND Flash usage; "nand bad" is used to display NAND Flash bad blocks.

Syntax

nand bad

nand usage

Example

```
>nand usage
Show NAND Flash Usage:
Partition      Total          Used           Available      Use%
cfg            4194304        7920           4186384        0%
bin_web       33554432      11869493      21684939      35%
cfg-bak       4194304        7920           4186384        0%
bin_web-bak  33554432      11869493      21684939      35%
> nand bad
Show NAND Flash Bad Blocks:
Block  Address          Partition
1020   0x07f80000      unused
1021   0x07fa0000      unused
1022   0x07fc0000      unused
1023   0x07fe0000      unused
```

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 Vigor2862.

Syntax

apm show

apm clear

apm discover

apm query

Syntax Description

Parameter	Description
<i>show</i>	It displays current information of APM profile.
<i>clear</i>	It is used to remove all of the APM profile.
<i>discover</i>	It is used to search VigorAP on LAN.
<i>query</i>	It is used to query any VigorAP which has been registered to APM (Central AP Management) in Vigor2862. Information related to the registered AP will be send back to Vigor2862 for updating the web page of Central AP Management.

Example

```
> 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
<i>clone</i>	It is used to copy the same parameters settings from one profile to another APM profile.
<i>del</i>	It is used to delete a specified APM profile. The default (index #1) should not be deleted.
<i>reset</i>	It is used to reset to factory settings for WLAN profile.
<i>summary</i>	It is used to list all of the APM profiles with required information.
<i>show</i>	It is used to display specified APM profile.
<i>apply</i>	It is used to apply the selected APM profile onto specified VigorAP.
<i>from index</i>	Type an index number in this field. It is the original APM profile to be cloned to other APM profile.
<i>to index</i>	Type an index number in this file. It is the target profile which will clone the parameters settings from an existed APM profile.
<i>new name</i>	Type a name for a new APM profile.
<i>profile index</i>	Type the index number of existed profile.
<i>client index1/2/3/4/5</i>	It is useful for applying the selected APM profile to the specified VigorAP.

Example

```

> apm profile clone 1 2 forcarrie
(Done)

> apm profile summary
# Name          SSID          Security      ACL      RateCtrl(U/D)
-----
0 Default       DrayTek-LAN-A WPA+WPA2/PSK x         - / -
                DrayTek-LAN-B WPA+WPA2/PSK x         - / -
1 -             -             -             -         -
2 forcarrie     DrayTek       Disable       x         - / -
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
<i>show</i>	It means to display the information related to VigorAP registered Vigor2862.
<i>clear</i>	It means to remove the information related to VigorAP registered Vigor2862.

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]*

Syntax Description

Parameter	Description
<i>set</i>	It means to set the load balance configuration file for APM.
<i>Show</i>	It shows the configuration value.
<i>[value]</i>	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. Type

	<p>1 - enable disassociation, 0 - disable disassociation.</p> <p>[8] - The eighth number means to enable or disable disassociation by signal strength. Type 1 - enable disassociation, 0 - disable disassociation.</p> <p>[9] - The ninth number means to determine the unit of traffic limit (for upload) 1 - Mbps 0 - kbps</p> <p>[10] - The tenth number means to determine the unit of traffic limit (for download) 1 - Mbps 0 - kbps</p>
--	---

Example

```

> 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) : 0
10. Traffic limit unit (download) : 0
flag : 0
> apm lbcfg set 1 1 0 15 0 0 0 0 1 1
> apm lbcfg 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) : 1
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
<i>get</i>	It is used to get AP detection data from VigorAP (e.g., AP900).
<i>set</i>	It allows to set detect configuration to VigorAP.
<i>enable/disable AP Detection 1/0</i>	It is used to enable or disable the AP detection function. 0 - disable the function. 1 - enable the function.
<i>Refresh Time</i>	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 Sigantl(%) 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 from VigorAP.

Syntax

apm apsyslog [AP_Index]

Syntax Description

Parameter	Description
<i>AP_Index</i>	Specify the index number which represents VigorAP.

Example

```
> 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
<i>AP_Index</i>	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
%           2    2    5            1    0
%           3    2    5            1    0
```

Telnet Command: ha set

This command can be used to configure HA settings for Vigor routers.

Syntax

ha set [*-<command>* *<parameter>*] ...]

Syntax Description

Parameter	Description
[<i><command></i> <i><parameter></i>] ...]	The available commands with parameters are listed below. [...] means that you can type in several parameters in one line.
<i>-e</i> <i><1/0></i>	1: Enable the function of High Availability (HA). 0: Disable the function of High Availability (HA).
<i>-l</i> <i><1/0></i>	1: Enable the function of recording the operation record of HA in Syslog. 0: Disable the function of recording the operation record of HA in Syslog.
<i>-M</i> <i><1/0></i>	Specify the Redundancy Method for HA.

	1: Active-Standby 0: Hot-Standby
-v <1-255>	Specify the group ID (VHID) 1- 255: Setting range.
-R	Set HA settings to Factory Default.
-p <1-30>	Specify the Priority ID. 1-30: Setting range.
-k <key>	Specify the Authentication Key. Key: Max. 31 Characters.
-u <1/0>	Enable or disable the function of Update DDNS. 1: Enable. When a router changes HA status to primary, it will update DDNS automatically. 0: Disable.
-m <interface>	Specify the management interface. Interface: LAN1 ~ LAN6, DMZ.
-s	It means to get the newest status of other router (except the local router).
-y	It means sync local config to other router. Primary can executes this command. Secondary can not execute this commad.
-c <1/0>	Enable or disable the function of Config Sync. 1: Enable. 0: Disable.
-I -[M H D] <interval>	Set the Config Sync Interval for HA. Minimum interval is 15 minutes. -M: Minute. Setting range is 0/15/30/45. (e.g., ha set -I -M 30) -H: Hour. Setting range is from 0 to 23. (e.g., ha set -I -H 12) -D: Day. Setting range is from 0 to 30. (e.g., ha set -I -D 15)
-h -<4/6><Subnet> [<Virtual IP>]	Enable and set virtual IP to the subnet. 4: IPv4; 6: IPv6. Subnet: LAN1 to LAN6, DMZ. Virtual IP: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.1.0) For example, to enable a virtual IP to the sunet, simply type: <i>ha set -h LAN1 192.168.1.5</i>
-d -<4/6><Subnet>	Disable a virtual IP to the subnet. 4: IPv4; 6: IPv6. Subnet: LAN1 to LAN6, DMZ. For example, to disable a virtual IP to the subnet, just type: <i>ha set -h LAN1</i>
-o <1/0>	Run DARP protocol on IPv4 or IPv6. 0: IPv4 1: IPv6

Example

```
> > ha set -h -4 LAN1 192.168.1.1
% Enable IPv4 Virtual IP on LAN1
% Virtual IP can not be same as router IP (192.168.1.1)!!!
>
```

Telnet Command: ha show

This command can be used to show the *settings information* about config sync and general setup.

Syntax

ha show -c

ha show -g

Syntax Description

Parameter	Description
-c	Show the settings of config sync.
-g	Show the settings of general setup.

Example

```
> ha show -g
% High Availability      : Disable
% Redundancy Method    : Active-Standby
% Group ID              : 1
% Priority ID           : 10
% Preempt Mode         : Enable
% Update DDNS          : Disable
% Management Interface : LAN1
% Authentication Key   : draytek
% Syslog                : OFF
%
% [ Index | Enable | Virtual IP ]
% LAN1    On     192.168.1.0
% 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
% DMZ     -     0.0.0.0
%
% [ Index | Enable | Virtual IPv6 ]
% LAN1    On     FE80::200:5EFF:FE00:101
% LAN2    On     FE80::200:5EFF:FE00:101
% LAN3    On     FE80::200:5EFF:FE00:101
% LAN4    On     FE80::200:5EFF:FE00:101
% LAN5    On     FE80::200:5EFF:FE00:101
% LAN6    On     FE80::200:5EFF:FE00:101
% DMZ     On     FE80::200:5EFF:FE00:101
%
>
```

Telnet Command: ha status

This command is used to display *HA status information*.

Syntax

ha status -a [*Detail Level*]

ha status -m [*Detail Level*]

Syntax Description

Parameter	Description
-a	Show the status for all of the routers in HA group.
-m	Show the status of local router only.
<i>Detail Level</i>	0: Important status. 1: Important status, plus some information. 2: Show settings

Example

```
> ha status -m 2
% [Local Router] DrayTek
% IP              : 192.168.1.1 (FE80::21D:AAFF:FEC6:4C50)
% Status          : !
```

```

% High Availability : ! Disable
% Redundancy Method : Active-Standby
% Group ID : 1
% Priority ID : 10
% Update DDNS : Disable
% Protocol : IPv4
% Management Interface: LAN1
% Authentication Key : draytek
% Virtual IP: (Max. 7 Virtual IPs)
% ON LAN1 192.168.1.0
% Virtual IPv6: (Max. 7 Virtual IPv6s)
% ON LAN1 FE80::200:5EFF:FE00:101
% ON LAN2 FE80::200:5EFF:FE00:101
% ON LAN3 FE80::200:5EFF:FE00:101
% ON LAN4 FE80::200:5EFF:FE00:101
% ON LAN5 FE80::200:5EFF:FE00:101
% ON LAN6 FE80::200:5EFF:FE00:101
% ON DMZ FE80::200:5EFF:FE00:101
% Config Sync : Disable
% Config Sync Interval : 0 Day 0 Hour 15 Minute
% Cached Time : 0 (s)
>

```

Telnet Command: swm show

This command is used to display general setting of of VigorSwitch which connecting to Vigor router in LAN.

Syntax

swm show *[LAN_port]*

Syntax Description

Parameter	Description
<i>LAN_port</i>	Specify the LAN port number (1 to 6).

Example

```

> swm show

** If you connected a VigorSwitch but does not display here.
** Please check the LLDP is enabled and VLAN ID is matched on VigorSwitch.
*****
LAN Port Model Name MAC IP Address Con Port
-----
1 G1241 00507FF105FD 192.168.1.10 23
-----
Internal VLAN is [Enable]
Only show P1 related VLAN settings here.
VLAN Subn Tag VID Pri LAN WLAN(2.4G) WLAN(5G)
-----
0 LAN1 Off 0 0 P1,P2,P3,P4,P5,P6 none none
1 LAN1 On 20 0 P1,P2,P3,P4,P5,P6 none none
2 LAN1 On 100 0 P1,P2,P3,P4,P5,P6 none none

```

Telnet Command: swm get

This command is used to get configuration information of VigorSwitch which connecting to Vigor router in LAN. Before using such command, make sure VigorSwitch has been managed under Vigor router (refer to Telnet Command: swm profile for adding a VigorSwitch device onto Vigor router).

Syntax

swm get *[LAN_port]*

Syntax Description

Parameter	Description
<i>LAN_port</i>	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
<i>LAN_port</i>	Specify the LAN port number (1 to 6).

Example

```
> swm post 1
Start post cfg to LAN (1) external switch with current 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
<i>show</i>	Display recorded external switch MAC address list.
<i>clear</i>	Clear specific index of authentication record table. Index range: (1 - 30)

Example

```
> swm auth show
===== SWM Auth Records List=====
Index Model  Mac
-----
> swm auth clear 1

Clear index (1) swm auth record OK
```

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
<i>LAN_Port</i>	Setting range is from 1 to 6.
<i>VLAN_idx</i>	Index number range for VLAN is from 0 to 7.
<i>Port_Description</i>	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 current 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.

Before using such command, please use [swm show] to check valid VLAN index firstly.

Telnet Command: backupmode

This command is used to backup the firmware to the router. The firmware will be retrieved for rebooting Vigor router after it crashes over three times.

Syntax

`backupmode [<command><parameter>|...]`

Syntax Description

Parameter	Description
<i>[<command><parameter> ...]</i>	The available commands with parameters are listed below. <i>[...]</i> means that you can type in several commands in one line.
<i>-t n</i>	Set the backup time. n : 1 ~ 168 hours
<i>-m n</i>	Set the firmware backup mode. 1: Backup after timeout. 0: Backup after upgrade.
<i>-b</i>	Backup the firmware manually and immediately.

Example

```
> backupmode -b
Do Firmware backup now!!!.
```

Index

3

3G/4G USB Modem, 64
3G/4G USB Modem (DHCP mode), 58
3G/4G USB Modem (PPP mode), 57

6

6rd Mode, 114
6rd Prefix, 115
6rd Prefix Length, 115

8

802.1x ports, 156

A

Accelerate heaviest traffic sessions, 158
Access Control, 249
Access List, 424
Access Mode, 74
Access Mode-ADSL/VDSL2, 74
Access Mode-Ethernet / USB, 74
Activation, 429
Active Directory/LDAP, 191
Active Mode, 67, 68, 71
Active When, 68, 71, 73
Active-Standby, 204
Additional Filter, 193
Address Mapping, 217, 233
ADSL/VDSL2, 67
Advance Mode, 348
Advanced Setting, 257
Aggregation MSDU, 257

Airtime Fairness, 262
ake on LAN, 197
Always On, 68, 72, 92, 97, 104, 106, 107, 109, 111, 113, 115, 120
Analyze, 362
Anonymous, 191
AP Discovery, 98, 261
AP Maintenance, 524, 532
AP Map, 524, 533
APN Name, 57, 101, 103
APP Enforcement, 345
APP Enforcement Filter, 368
APP Enforcement Profile, 369
APP QoS, 446
APPE Module Version, 373
APPE Signature Upgrade, 373
Applications, 173
Apply the Class Rule, 158
APSD Capable, 258
ARP Cache Table, 616
ARP Detect, 76, 79, 83, 86, 90, 92, 97, 101, 103
ARP Table, 153
ATM OoS, 118, 120
Auth Type, 178
Authentication, 189
Authentication Information, 631
Authentication Key, 205
Authentication Mode, 253
Authentication Port, 188
Authentication Type, 156
Auto Adjustment, 260
Auto detect, 37
Auto Logout, 22
Auto ULA Prefix, 144
Auto-Update interval, 176

Aux. WAN IP, 168

B

Backup, 153

Band Steering, 264

Bandwidth Limit, 433, 437

Bandwidth Management, 260, 433

Base Distinguished Name, 193

Beacon Period, 540

Bind IP to MAC, 152

Bind to WAN, 323

Bind Type, 191

Bogus DNS Reply, 182

Bonjour, 200

Bridge, 254, 256

Bridge mode, 118

Bridge Mode, 80, 87, 93, 110, 112

Bridge Subnet, 87, 93, 110, 112

Brute Force Protection, 422

C

Cache, 380

Call Direction, 294

Call Filter, 340

Certificate Backup, 338

Certificate Management, 331

Change the TTL value, 91, 94

Channel, 98, 116, 242, 245

Channel Bandwidth, 257

Choose IP, 166

Codepage, 345

Comment, 153, 168

Common Name Identifier, 193

Config Backup, 31

Config Sync, 206

Configuration Backup, 412

Connection Management, 313

Connection Type, 178

Connectivity, 63

Country Code, 258

CPE Management, 506

CSM, 368

CSV file, 570

Current System Time, 184

D

Dashboard, 25, 525

Data Filter, 340

Data Flow Monitor, 622

Data Quota, 459

DataType, 74, 137

Daylight Saving, 418

Days in a week, 185

Default Lifetime, 146

Default MAC Address, 78, 80, 84, 91, 94

Default Preference, 146

Default Rule, 344

Destination IP, 224

Destination Port, 187

Details - PPPoE/PPPoA, 82

Details Page, 74

Details-3G/4G USB Mdem(PPP mode), 100

Details-3G/4G USB Modem(DHCP mode), 102

Details-IP Routed Subnet, 142

Details-IPv6-6in4 Static Tunnel, 113

Details-IPv6-6rd, 114

Details-IPv6-AICCU, 107

Details-IPv6-DHCPv6 Client, 109

Details-IPv6-Offline, 104

Details-IPv6-PPP, 104

Details-IPv6-Static IPv6, 111

Details-IPv6-TSPC, 105

Details-LAN IPv6, 143

Details-LAN-DMZ, 140
Details-LAN-Ethernet, 138
Details-MPoA/Static or Dynamic IP, 79, 85
Details-PPPoE, 76, 89
Details-PPTP/L2TP, 95
Details-Static IP or Dynamic IP, 91
Details-Static or Dynamic IP, 97
Determine Real WAN IP, 178
DFS Restrictions, 239
DHCP, 48, 54
DHCP Client Identifier, 80, 88, 94
DHCP Server Configuration, 138, 140, 142
DHCP Server IP Address, 138, 140
DHCP Table, 618
DHCPv6 (Stateful), 144
DHCPv6 Server, 145
Diagnose, 183, 228
Diagnostic, 614
Dial-out Triggering, 614
Digital Signature, 277, 291
Display Name, 71, 72, 74
DMZ Host, 165
DNS Cache Table, 620
DNS Filter, 345
DNS Filter Profile, 383
DNS Security, 182
DNS Server, 183
DNS Server IP Address, 81, 89, 94, 139, 141
DNS Server IPv6 Address, 145
Domain, 183
Domain Diagnose, 183
Domain Name, 94, 177, 227
DoS Defense, 341, 357
DoS Flood Table, 633, 635
Download Limit, 260
DrayTek Banner, 355
DSL Mode, 68

DSL Modem Code, 68
DSL Status, 629
Dynamic DNS, 173, 175
Dynamic DNS Account, 177
Dynamic IP, 97

E

Each / Shared, 438
Enable PING to keep alive, 92
Encapsulating, 86
Encapsulating Type, 82
Encapsulation, 117, 120
End IPv6 Address, 145
End Port, 169
ESP, 286
Event Code, 403
Event Log, 542
Extension WAN, 146
External Devices, 564
External RADIUS, 186
External TACACS+, 190

F

Failover, 68, 71, 72
Failover to/Failback, 217
File Explorer, 603
File Extension Object, 583
Filter Setup, 347
Firewall, 340
Firmware Upgrade, 428
Fixed IP, 78, 84, 91, 96, 120
Force NAT /Force Routing, 225
Force Update, 176
Fragment Length, 258
Function Support List, 545

G

Gateway IP Address, 80, 88, 94, 97, 138, 140
General Setup, 66
Google Map, 511
GRE, 299
Green Field, 257
Group ID, 196, 205
Guard Interval, 257
GUI Map, 29

H

Hardware Acceleration, 157
Hardware Installation, 11
Hide SSID, 246
High Availability, 203
High Availability Status, 629
Host Name, 49, 50
Hot-Standby, 204

I

ICMP, 309
Idle Timeout, 84, 91, 96, 120
IGMP, 195
IGMP Proxy, 195
IGMP Snooping, 195
IM, 370
Inbound Bandwidth, 441
Incoming Port, 172
Incoming Protocol, 172
Indicators and Connectors, 2, 9
Installation, i
Interface, 225
Inter-LAN Routing, 137
Internal RADIUS, 187
Internal Service User List, 431
Internet Access, 74

Internet Access-Advanced, 74
IP (Internet Protocol), 64
IP address, 97
IP Address, 80, 88, 94, 96, 138, 140
IP Address Assignment Method (IPCP), 91
IP Address Assignment Method(IPCP), 96
IP Address From ISP, 78, 84
IP Address List, 180
IP Based, 66
IP Bind List, 153
IP Filters, 340
IP Group, 572
IP Object, 568
IP Pool Counts, 138, 140, 142
IP Routed Subnet, 437
IPsec General Setup, 286
IPsec Peer Identity, 287
IPv4 Border Relay, 115
IPv4 Mask Length, 115
IPv6 Address, 111
IPv6 Gateway Address, 111
IPv6 Group, 575
IPv6 Neighbour Table, 617
IPv6 Object, 573
IPv6 TSPC Status, 628
Isolate, 246
ISP Access Setup, 77, 84, 89, 95
ISP Name, 120

K

keep alive, 294
Keep Alive Period, 403
Keep WAN Connection, 92
Keyword Group, 582
Keyword Object, 580

L

- LAN, 134
- LAN DNS / DNS Forwarding, 173, 179
- LAN Port Mirror, 155
- LAN Routed Prefix, 113
- LAN to LAN, 292
- Landing Page, 454, 458
- LAN-General Setup, 136
- LDAP /Active Directory Setup, 173
- Lease Time, 138, 140, 142
- Line Speed, 67, 68, 71, 72
- Load Balance, 68, 71, 72, 543
- Load Balance for AP, 524
- Load Balance Mode, 66
- Load-Balance, 223, 231
- Load-Balance /Route Policy, 223
- Local 802.1X, 431, 459
- Local 802.1X General Setup, 208
- Local Certificate, 277, 332
- Local IP Address, 168
- Log, 377
- Log & Alert, 514
- Login, 61
- Login Name, 178
- Login Page, 454
- Login Page Greeting, 410
- Logout, 31
- Long Preamble, 257

M

- Mail Alert, 199
- Mail Extender, 178
- Mail Service, 199
- Main Screen, 22
- Maintenance, 557
- Management, 421

- Management Interface, 205
- Manually ULA Prefix, 144
- MBS, 122
- Min/Max Interval Time, 146
- Mirror Port, 155
- Mode, 241, 247
- Modem Code Upgrade, 429
- Modem Dial String, 101
- Modem Initial String, 57, 101
- Modem Initial String2, 101
- Modem Setting (for ADSL only), 76, 79
- Modem Settings, 82
- Modem Settings (for ADSL only), 86
- Modem Support List, 100, 102, 607
- Modulation, 82, 86
- mOTP, 325
- MPoA (RFC1483/2684), 121
- MPoA / Static or Dynamic IP, 40
- MPPE, 284
- MTU, 77, 80, 83, 87, 90, 93, 95, 98, 103, 146
- Multicast via VPN, 325
- Multiple SSID, 238
- multiple-WAN, 66
- Multi-PVC channel, 82, 86
- Multi-PVC/VLAN, 116
- MyVigor, 59, 379

N

- Name Link, 27
- NAT, 160
- NAT Sessions Table, 619
- NAT Traversal, 194
- Neighbor AP Detection, 539
- Network Configuration, 138, 140, 142
- Network Interface, 222
- Network Mode, 103
- Next Server IP Address/SIAddr, 137

Notification Object, 590

NS Detect, 109

O

Objects Settings, 567

Online Statistics, 440

Open Ports, 168

Option Number, 74, 137

Outbound Bandwidth, 441

P

PAP, 285

Pass Phrase, 98

Password, 77, 84, 89, 94, 95, 106, 107, 120

Password Strength, 248, 407

Path MTU Discovery, 77, 80, 83, 87, 90, 93, 95, 103

PCR, 122

Peer ID, 282

Per Station Limit, 260

Physical Connection, 32

Physical Members, 118, 120

Physical Mode, 42, 67, 68, 71, 72, 74

Physical Type, 42, 67

PIN Code, 325

PinCode, 253

Ping Detect, 76, 79, 83, 86, 90, 92, 97, 101, 103, 104, 106, 107, 109, 111, 113, 115

Ping Diagnosis, 621

Ping Gateway IP, 76, 79, 83, 86, 90, 92, 97, 101, 103

Ping Interval, 76, 79, 83, 86, 90, 92, 97, 101, 103

PING Interval, 92

Ping IP/Hostname, 104, 106, 107, 109, 111, 113, 115

Ping Retry, 76, 79, 83, 86, 90, 92, 97, 101, 103

Policy, 457

Port Redirection, 161

Port Triggering, 170, 172

Port-based Bridge, 116

Port-Based VLAN, 147

PPP Authentication, 77, 84, 91, 96, 101, 120

PPP General Setup, 284

PPP Password, 101

PPP Setup, 96

PPP Username, 101

PPP/MP Setup, 91

PPPoE, 43

PPPoE Pass-through, 76, 83

PPPoE/PPPoA, 37

PPPoE/PPPoA Client, 120

PPTP/L2TP, 45

Prefix Len, 221

Prefix Length, 111

Pre-shared Key, 256

Pre-Shared Key (PSK), 248

Primary DNS Sever, 145

Primary IP Address, 139, 141

Primary/Secondary Ping IP, 76, 79, 83, 86, 90, 92, 97, 101, 103

Printer Server, 601

Priority, 36, 69, 71, 117, 149, 217, 228

Priority ID, 205

Private IP, 163

Private IP Address, 64

Private Port, 163

Production Registration, 61

Protocol, 82, 205, 371

Protocol Processing Engine (PPE), 157

Provider Host, 177

Public IP Address, 64

Public Port, 163

Push Button, 253

PVC to PVC Binding, 122

Q

QoS Type, 118, 120, 122

Quality of Service, 433, 439

Query Server, 380
Quick Access, 28
Quick Start Wizard, 35
Quota Limit, 123

R

RADIUS, 459
RADIUS/TACACS+, 173, 186
Rate Control, 135
Reboot System, 427
Recipient, 198
Redundancy Method, 204
Registering Vigor Router, 61
Regular DN, 192
Regular Mode, 191
Regular Password, 192
Relay Agent, 138, 140
Remote Access Control, 283
Remote Dial-in User, 289
Remote Endpoint IPv4 Address, 113
Repeater, 254, 256
Restore, 153
RIP Protocol, 80, 87, 93
RIPng Protocol, 105, 110, 112, 146
Rogue AP, 541
Rogue AP Detection, 539
Root CA, 336
Route Policy, 217
Router Advertisement Configuration, 146
Router Name, 94, 416
Routing, 217
Routing Information Protocol, 135
Routing Table, 615
RTS Threshold, 258
Rule-Based, 453

S

Scan, 261
Schedule, 173, 184, 246
SCR, 122
Secondary DNS Server, 145
Secondary IP Address, 139, 141
Security, 246
Security Key, 242
Security Mode, 51, 54, 98
Self-signed, 323
Self-Signed Certificate, 425
Sensor, 605
Server Address, 95
Server Certificate, 323
Server IP Address, 187
Server Response, 178
Service, 171
Service Activation Wizard, 59
Service API, 177
Service Name, 38, 89, 101, 163
Service Provider, 177, 586
Service Type, 177
Service Type Group, 578
Service Type Object, 576
Session Based, 66
Sessions Control, 344
Sessions Limit, 433, 435
Set to Factory Default, 175, 184, 218
Shared Secret, 187, 188, 190
SIM Pin code, 57
SIM PIN code, 101, 102
Simple Mode, 191
SLAAC(stateless), 144
Smart Bandwidth Limit, 438
SMB, 602
SMB Client Support List, 608
SMS / Mail Alert Service, 198

SMS Alert, 198
SMS Provider, 198
SMS/Mail Service Object, 585
SNMP, 419
Source IP, 163, 169, 171, 224
Specific Hosts, 158
Specify an IP address, 80
SPI, 341
SSID, 98, 243
SSL VPN, 322
Start IP Address, 138, 140, 142
Start IPv6 Address, 145
Start Port, 169
Static IP, 47
Static Route, 135, 218
Static Route for IPv6, 221
Station Control, 259
Station List, 239, 268, 269
Station Number, 543
Stations (STA), 238
Status, 526
Strict Bind, 152
Strict Security Firewall, 343
String Object, 592, 593
STUN, 403
Subnet, 149
Subnet Mask, 80, 88, 94, 96, 97, 138, 140
Subnet Prefix, 107
Support List, 558, 562, 563
Switch, 549
Switch Group, 555
Switch Hierarchy, 551
Switch Status, 549
Sync User Profile, 208
Syslog Alarm, 606
Syslog Explorer, 627
Syslog/Mail Alert, 416

System Maintenance, 399
System time set, 184

T

TACACS+, 329
Tag value, 36, 69, 71
Tagged VLAN, 147
TCP. [参閱](#)
Temperature Sensor, 539, 605
Time and Date, 418
Time Quota, 458
Time Schedule, 438
Time Server, 418
Time Zone, 418
Total Traffic, 542
TR-069, 402
Trace Route, 626
Traceable, 446
Traffic Graph, 538, 624
Traffic Threshold, 68, 71, 72
Triggering Port, 172
Triggering Protocol, 171
Trusted CA Certificate, 336
TSPC, 105
TTL (Time to Live), 76, 79, 83, 86, 90, 92, 97, 101, 103, 104, 106, 107, 109, 111, 113, 115
Tunnel Broker, 106, 107
Tunnel ID, 107
Tunnel TTL, 113
TX Power, 258

U

UDP, 309
Unique Local Address (ULA), 144
Update DDNS, 205
Upload Limit, 260
UPnP, 174, 194

URL Access Control, 377
URL Content Filter, 345, 368
URL Content Filter Profile, 375
USB, 57
USB Application, 599
USB Device Status, 604
USB General Settings, 600
USB User Management, 601
User Account, 324
User Group, 328, 460
User Management, 452
User Online Status, 461
User Password, 407
User Profile, 189, 208, 455
User-Based, 453
Username, 77, 84, 89, 94, 95, 106, 107, 120

V

VCI, 86
VID, 149
Virtual LAN, 135
Virtual Panel, 26
Virtual WAN, 34
VLAN, 147
VLAN Applications, 647
VLAN Configuration, 149
VLAN Tag, 116, 117, 120, 149
VLAN Tag insertion, 36, 42, 69, 71
VPI, 86
VPN, 271, 503
VPN and Remote Access, 272
VPN Backup, 303
VPN Client Wizard, 273
VPN Dial-Out Through, 277
VPN Graph, 625
VPN Load Balance, 303
VPN Management, 513

VPN Server Wizard, 279
VPN Trunk Management, 303

W

Wake by IP Address, 197
Wake on LAN, 174
WAN, 64
WAN Application-IPTV, 120
WAN Application-Management, 120
WAN Budget, 123
WAN Budget-Custom, 124
WAN Budget-Cycle duration, 124
WAN Budget-Status, 125
WAN Connection Detection, 76, 79, 83, 86, 90, 92, 97, 101, 103, 104, 106, 107, 109, 111, 113, 115
WAN Failure, 68, 71, 72
WAN Interface, 168, 177
WAN IP, 163
WAN IP Alias, 78, 80, 84, 88, 91, 94, 96
WAN IP Network Settings, 80, 88, 94, 96
WAN Type, 116, 117, 119
WAN-USB, 72
WDS, 254
Web Console, 30
Web Content Filter, 345, 368
Web Content Filter Profile, 379
Web Feature, 378
Weight, 66
WEP, 98, 239, 248
white/black list, 249
Wildcard, 178
Wired 802.1x, 156
Wireless 2.4/5G, 70
Wireless LAN, 237
Wireless Wizard, 241
Wizard Mode, 348
WLAN Isolation, 239

WLAN Profile, 527
WMM Capable, 258

WPA, 239, 248
WPS, 240, 251