

DrayTek

Vigor2765 Series

35b Security Router



USER'S GUIDE

V1.3

Vigor2765 Series 35b Security Router

User's Guide

Version: 1.3

Firmware Version: V4.3.1

(For future update, please visit DrayTek web site)

Date: June 3, 2021

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 8, 10 and Explorer are trademarks of Microsoft Corp.
- Apple and Mac OS are registered trademarks of Apple Inc.
- Other products may be trademarks or registered trademarks of their respective manufacturers.

Safety Instructions

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

Warranty

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

Be a Registered Owner

- Web registration is preferred. You can register your Vigor router via <https://myvigor.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.

<https://www.draytek.com>

Table of Contents

Part I Installation	1
I-1 Introduction	2
I-1-1 Indicators and Connectors	3
I-1-1-1 Vigor2765 / Vigor2765ac	3
I-1-1-2 Vigor2765Vac	5
I-2 Hardware Installation	7
I-2-1 Installing Vigor Router	7
I-2-2 Wall-Mounted Installation	8
I-2-3 Installing USB Printer to Vigor Router	9
I-3 Accessing Web Page	16
I-4 Changing Password	18
I-5 Dashboard	19
I-5-1 Virtual Panel	19
I-5-2 Name with a Link	20
I-5-3 Quick Access for Common Used Menu	21
I-5-4 GUI Map	22
I-5-5 Web Console	23
I-5-6 Config Backup	23
I-5-7 Manual Download	24
I-5-8 Logout	24
I-5-9 Online Status	25
I-5-9-1 Physical Connection	25
I-5-9-2 Virtual WAN	27
I-6 Quick Start Wizard	28
I-6-1 For WAN1 (ADSL)	29
I-6-2 For WAN2 (Ethernet)	34
I-6-3 For WAN3 (USB)	43
I-7 Service Activation Wizard	45
I-8 Registering Vigor Router	47
Part II Connectivity	51
II-1 WAN	52
Web User Interface	54
II-1-1 General Setup	54
II-1-1-1 WAN1 (ADSL/ VDSL)	55
II-1-1-2 WAN2 (Ethernet)	56
II-1-1-3 WAN3 (USB)	57
II-1-2 Internet Access	58
II-1-2-1 Details Page for PPPoE/ PPPoA in WAN1 (Physical Mode: ADSL)	60
II-1-2-2 Details Page for MPoA/ Static or Dynamic IP in WAN1 (Physical Mode: ADSL)	63
II-1-2-3 Details Page for PPPoE in Ethernet WAN	67
II-1-2-4 Details Page for Static or Dynamic IP in Ethernet WAN	70

II-1-2-5 Details Page for PPTP/ L2TP in Ethernet WAN	73
II-1-2-6 Details Page for 3G/ 4G USB Modem (PPP mode) in USB WAN	75
II-1-2-7 Details Page for 3G/ 4G USB Modem (DHCP mode) in USB WAN	77
II-1-2-8 Details Page for IPv6 – Offline in WAN1/ WAN2/ WAN3	79
II-1-2-9 Details Page for IPv6 – PPP in WAN1/ WAN2	80
II-1-2-10 Details Page for IPv6 – TSPC in WAN1/ WAN2/ WAN3	82
II-1-2-11 Details Page for IPv6 – AICCU in WAN1/ WAN2/ WAN3	83
II-1-2-12 Details Page for IPv6 – DHCPv6 Client in WAN1/ WAN2	85
II-1-2-13 Details Page for IPv6 – Static IPv6 in in WAN1/ WAN2	86
II-1-2-14 Details Page for IPv6 – 6in4 Static Tunnel in WAN1 / WAN2	88
II-1-2-15 Details Page for IPv6 – 6rd in WAN1 / WAN2	90
II-1-3 Multi-PVC/VLAN	92
II-1-4 WAN Budget	100
II-1-4-1 General Setup	100
II-1-4-2 Status	103
Application Notes	104
A-1 How to configure IPv6 on WAN interface?	104
II-2 LAN	109
Web User Interface	111
II-2-1 General Setup	111
II-2-1-1 Details Page for LAN1 – Ethernet TCP/ IP and DHCP Setup	113
II-2-1-2 Details Page for LAN2/ 3/ 4	115
II-2-1-3 Details Page for IP Routed Subnet	117
II-2-1-4 Details Page for LAN1~ LAN4 – IPv6 Setup	118
II-2-1-5 DHCP Server Option	122
II-2-2 VLAN	124
II-2-3 Bind IP to MAC	128
II-2-4 LAN Port Mirror	130
II-2-5 Wired 802.1x	130
II-3 NAT	132
Web User Interface	133
II-3-1 Port Redirection	133
II-3-2 DMZ Host	137
II-3-3 Open Ports	140
II-3-4 Port Triggering	142
II-3-5 ALG	144
II-4 Applications	145
Web User Interface	147
II-4-1 Dynamic DNS	147
II-4-2 LAN DNS / DNS Forwarding	151
II-4-3 DNS Security	154
II-4-3-1 General Setup	154
II-4-3-2 Domain Diagnose	155
II-4-4 Schedule	156
II-4-5 RADIUS	158
II-4-6 UPnP	161
II-4-7 IGMP	162

II-4-7-1 General Setting	162
II-4-7-2 Working status	163
II-4-8 Wake on LAN	164
II-4-9 SMS / Mail Alert Service	165
II-4-9-1 SMS Alert	165
II-4-9-2 Mail Alert	166
II-4-10 Bonjour	167
Application Notes	170
A-1 How to Configure Customized DDNS?	170
II-5 Routing	174
Web User Interface	175
II-5-1 Static Route	175
II-5-1-1 Static Route for IPv4	175
II-5-1-2 Static Route for IPv6	179
II-5-2 Route Policy	181
Application Notes	190
A-1 How to set up Address Mapping with Route Policy?	190
A-2 How to use destination domain name in a route policy?	192
Part III Wireless LAN	195
III-1 Wireless LAN	196
Web User Interface	199
III-1-1 Wireless Wizard	199
III-1-2 General Setup	203
III-1-3 Security	205
III-1-4 Access Control	207
III-1-5 WPS	208
III-1-6 WDS (for WLAN 5 GHz)	211
III-1-7 Advanced Setting	213
III-1-8 Station Control	217
III-1-9 Bandwidth Management	218
III-1-10 AP Discovery	219
III-1-11 Airtime Fairness	220
III-1-12 Band Steering	222
III-1-13 Roaming	226
III-1-14 Station List	227
III-2 Mesh Network	229
III-2-1 Mesh Wizard	230
III-2-2 Mesh Setup	234
III-2-3 Mesh Status	236
III-2-4 Mesh Discovery	237
III-2-5 Basic Config Sync	238
III-2-6 Support List	240

Part IV VoIP	241
IV-1 VoIP	242
Web User Interface	244
IV-1-1 VoIP Wizard	244
IV-1-2 General Settings	246
IV-1-3 SIP Accounts	248
IV-1-3-1 Alias List	251
IV-1-4 DialPlan	253
IV-1-4-1 Phone Book	253
IV-1-4-2 Digit Map	255
IV-1-4-3 Call Barring	257
IV-1-4-4 Regional	259
IV-1-5 Phone Settings	261
IV-1-6 Status	265
IV-1-7 Diagnostics	267
IV-1-7-1 Caller ID	267
IV-1-7-2 Tone	268
Part V VPN	269
V-1 VPN and Remote Access	270
Web User Interface	271
V-1-1 VPN Client Wizard	271
V-1-2 VPN Server Wizard	278
V-1-3 Remote Access Control	288
V-1-4 PPP General Setup	289
V-1-5 SSL General Setup	290
V-1-6 IPsec General Setup	292
V-1-7 IPsec Peer Identity	294
V-1-8 VPN Matcher Setup	296
V-1-9 OpenVPN	298
V-1-9-1 General Setup	298
V-1-9-2 Client Config.	300
V-1-9-3 Import Certificate	302
V-1-10 Remote Dial-in User	303
V-1-11 LAN to LAN	307
V-1-12 Connection Management	315
Application Notes	316
A-1 How to Build a LAN-to-LAN VPN Between Vigor Routers via IPsec Main Mode	316
V-2 Certificate Management	321
Web User Interface	322
V-2-1 Local Certificate	322
V-2-2 Trusted CA Certificate	327
V-2-3 Certificate Backup	330
V-2-4 Self-Signed Certificate	331

Part VI Security	333
VI-1 Firewall	334
Web User Interface	336
VI-1-1 General Setup	336
VI-1-2 Filter Setup	341
VI-1-3 Defense Setup	350
<i>VI-1-3-1 DoS Defense</i>	<i>350</i>
<i>VI-1-3-2 Spoofing Defense</i>	<i>353</i>
VI-1-4 Diagnose	354
VI-2 CSM (Central Security Management)	357
Web User Interface	358
VI-2-1 APP Enforcement Profile	358
VI-2-2 APPE Signature Upgrade	360
VI-2-3 URL Content Filter Profile	361
VI-2-4 Web Content Filter Profile	365
VI-2-5 DNS Filter Profile	368
Application Notes	370
<i>A-1 How to Create an Account for MyVigor</i>	<i>370</i>
<i>A-2 How to Block Facebook Service Accessed by the Users via Web Content Filter / URL Content Filter</i>	<i>375</i>
Part VII Management	381
VII-1 System Maintenance	382
Web User Interface	383
VII-1-1 System Status	383
VII-1-2 TR-069	385
<i>VII-1-2-2 Reporting Configuration</i>	<i>387</i>
<i>VII-1-2-3 Export Parameters</i>	<i>388</i>
VII-1-3 Administrator Password	388
VII-1-4 User Password	392
VII-1-5 Login Page Greeting	395
VII-1-6 Configuration Backup	397
VII-1-7 SysLog/Mail Alert	400
VII-1-8 Time and Date	403
VII-1-9 SNMP	404
VII-1-10 Management	406
VII-1-11 Panel Control	411
VII-1-12 Self-Signed Certificate	416
VII-1-13 Reboot System	418
VII-1-14 Firmware Upgrade	419
VII-1-15 Firmware Backup	420
VII-1-16 Dashboard Control	421
VII-2 Bandwidth Management	422

Web User Interface	423
VII-2-1 Sessions Limit	423
VII-2-2 Bandwidth Limit	425
VII-2-3 Quality of Service	427
VII-2-4 APP QoS	433
VII-3 User Management	434
Web User Interface	435
VII-3-1 General Setup	435
VII-3-2 User Profile	437
VII-3-3 User Group	442
VII-3-4 User Online Status	443
VII-4 Hotspot Web Portal	445
Web User Interface	445
VII-4-1 Profile Setup	445
<i>VII-4-1-1 Login Method</i>	<i>446</i>
<i>VII-4-1-2 Steps for Configuring a Web Portal Profile</i>	<i>446</i>
VII-4-2 Quota Management	463
Application Notes	466
<i>A-1 How to allow users login to Vigor's Hotspot with their social media accounts (e.g., Facebook & Google)</i>	<i>466</i>
<i>A-2 How to allow hotspot clients to get login PIN code via SMS?</i>	<i>474</i>
VII-5 Central Management (AP)	482
Web User Interface	483
VII-5-1 Status	483
VII-5-2 WLAN Profile	485
VII-5-3 AP Maintenance	490
VII-5-4 Traffic Graph	491
VII-5-5 Load Balance	492
VII-6 Central Management (External Devices)	494
Part VIII Others	495
VIII-1 Objects Settings	496
Web User Interface	497
VIII-1-1 IP Object	497
VIII-1-2 IP Group	500
VIII-1-3 IPv6 Object	501
VIII-1-4 IPv6 Group	503
VIII-1-5 Service Type Object	505
VIII-1-6 Service Type Group	507
VIII-1-7 Keyword Object	509
VIII-1-8 Keyword Group	511
VIII-1-9 File Extension Object	512

VIII-1-10 SMS/Mail Service Object	514
VIII-1-11 Notification Object	519
VIII-1-12 String Object	520
VIII-1-13 Country Object	521
VIII-1-14 Objects Backup/Restore	522
Application Notes	524
<i>A-1 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection</i>	524
VIII-2 USB Application	528
Web User Interface	529
VIII-2-1 USB General Settings	529
VIII-2-2 USB User Management	530
VIII-2-3 File Explorer	533
VIII-2-4 USB Device Status	534
VIII-2-5 Temperature Sensor	535
VIII-2-6 Modem Support List	537
VIII-2-7 SMB Client Support List	538
Application Notes	539
<i>A-1 How can I get the files from USB storage device connecting to Vigor router?...</i>	539

Part IX Troubleshooting 542

IX-1 Diagnostics	543
Web User Interface	544
IX-1-1 Dial-out Triggering	544
IX-1-2 Routing Table	545
IX-1-3 ARP Cache Table	546
IX-1-4 IPv6 Neighbour Table	547
IX-1-5 DHCP Table	548
IX-1-6 NAT Sessions Table	549
IX-1-7 DNS Cache Table	550
IX-1-8 Ping Diagnosis	551
IX-1-9 Data Flow Monitor	553
IX-1-10 Traffic Graph	556
VIII-1-11 VPN Graph	557
IX-1-12 Trace Route	558
IX-1-13 Syslog Explorer	559
IX-1-14 IPv6 TSPC Status	561
IX-1-15 DSL Status	562
IX-1-16 DoS Flood Table	563
IX-1-17 Route Policy Diagnosis	564
IX-2 Checking If the Hardware Status Is OK or Not	566
IX-3 Checking If the Network Connection Settings on Your Computer Is OK or Not	567

IX-4 Pinging the Router from Your Computer	570
IX-5 Checking If the ISP Settings are OK or Not.....	572
IX-6 Problems for 3G/4G Network Connection	573
IX-7 Backing to Factory Default Setting If Necessary	574
IX-8 Contacting DrayTek	575
Part X Telnet Commands.....	576
Accessing Telnet of Vigor2765	577

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.

Vigor2765 series is a VDSL2 35b router. It integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

By adopting hardware-based VPN platform and hardware encryption of AES/DES/3DES, the router increases the performance of VPN greatly and offers several protocols (such as IPSec/PPTP/L2TP) with up to 2 VPN tunnels.



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

Object-based firewall is flexible and allows your network be safe. In addition, Vigor2765 Series supports USB interface for connecting USB printer to share printer, USB storage device for sharing files, or for 3G/4G WAN.



I-1-1 Indicators and Connectors

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

I-1-1-1 Vigor2765 / Vigor2765ac



LED	Status	Explanation
 (Activity)	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
 (DSL)	On	The DSL port is connected.
	Blinking (Slowly)	The router is ready.
	Blinking (Quickly)	The router is trying to connect to Internet.
 (Wireless LAN On/Off/WPS)	On (Green)	The wireless access point is ready.
	Blinking (Green)	The data is transmitting via wireless connection based on the rate of 2.4GHz.
	Blinking (Orange)	Blinks with one second cycle for two minutes. The WPS function is active.
	Off	The wireless access point is turned off.
 (Wireless LAN On/Off/WPS)	On (Green)	The wireless access point is ready.
	Blinking (Green)	The data is transmitting via wireless connection based on the rate of 5GHz.
	Blinking (Orange)	Blinks with one second cycle for two minutes. The WPS function is active.
 (LAN1/2/3/4)	On	The LAN port is connected.
	Blinking	The data is transmitting.
	Off	The LAN port is disconnected.
 (USB)	On	A USB device is connected and active.
	Blinking	The data is transmitting.

Vigor2765



Vigor2765ac



Interface	Description
WLAN ON/OFF/WPS	WLAN On - Press the button and release it within 2 seconds. When the wireless function is ready, the green LED will be on. WLAN Off - Press the button and release it within 2 seconds to turn off the WLAN function. When the wireless function is not ready, the LED will be off. WPS - When WPS function is enabled by web user interface, press this button for more than 2 seconds to wait for client's device making network connection through WPS.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
USB1-USB2	Connector for a USB device (for 3G/4G USB Modem or printer).
P1-P4	Connectors for local networked devices.
DSL	Connector for accessing the Internet.
I / O	Power Switch.
PWR	Connector for a power adapter.

I-1-1-2 Vigor2765Vac



LED	Status		Explanation
 (Activity)	Blinking		The router is powered on and running normally.
	Off		The router is powered off.
 (DSL)	Orange	On	The DSL link up, waiting for the Internet connection.
		Blinking	Slowly - The DSL connection is ready for training. Quickly - The DSL connection is synchronizing.
	Green	On	The router is ready to access to the Internet through DSL link.
		Blinking	The data is transmitting.
 	On		The phone connected to this port is off-hook.
	Off		The phone connected to this port is on-hook.
	Blinking		A phone call comes.
 (Wireless LAN On/Off/WPS)	On (Green)		The wireless access point is ready.
	Blinking (Green)		The data is transmitting via wireless connection based on the rate of 2.4GHz.
	Blinking (Orange)		Blinks with one second cycle for two minutes. The WPS function is active.
	Off		The wireless access point is turned off.
 (Wireless LAN On/Off/WPS)	On (Green)		The wireless access point is ready.
	Blinking (Green)		The data is transmitting via wireless connection based on the rate of 5GHz.
	Blinking (Orange)		Blinks with one second cycle for two minutes. The WPS function is active.
  ~ (LAN1/2/3/4)	On		The LAN port is connected.
	Blinking		The data is transmitting.
	Off		The LAN port is disconnected.
 (USB)	On		A USB device is connected and active.
	Blinking		The data is transmitting.

Vigor2765Vac



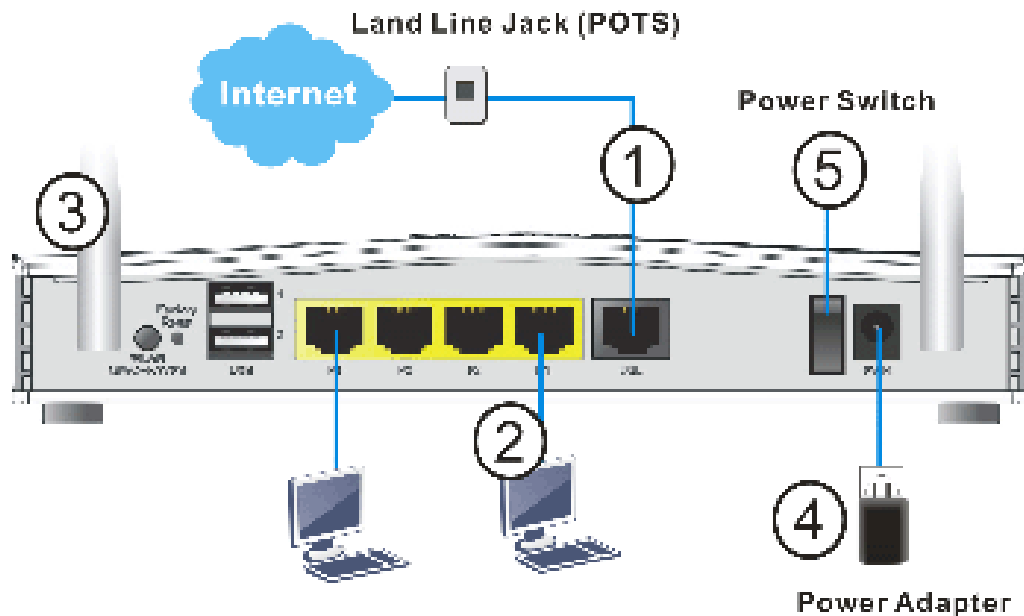
Interface	Description
WLAN ON/OFF/WPS	WLAN On - Press the button and release it within 2 seconds. When the wireless function is ready, the green LED will be on. WLAN Off - Press the button and release it within 2 seconds to turn off the WLAN function. When the wireless function is not ready, the LED will be off. WPS - When WPS function is enabled by web user interface, press this button for more than 2 seconds to wait for client's device making network connection through WPS.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
USB1-USB2	Connector for a USB device (for 3G/4G USB Modem or printer).
P1-P4	Connectors for local networked devices.
DSL	Connector for accessing the Internet.
Phone2/Phone1	Connector of analog phone for VoIP communication.
I/O	Power Switch.
PWR	Connector for a power adapter.

I-2 Hardware Installation

I-2-1 Installing Vigor Router

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

1. Connect the DSL interface to the land line jack with a DSL line cable.
2. Connect one port of 4-port switch to your computer with a RJ-45 cable. This device allows you to connect 4 PCs directly.
3. Connect detachable antennas to the router.
4. Connect one end of the power cord to the power port of this device. Connect the other end to the wall outlet of electricity.
5. Power on the router.
6. Check the ACT and DSL, LAN LEDs to assure network connection.

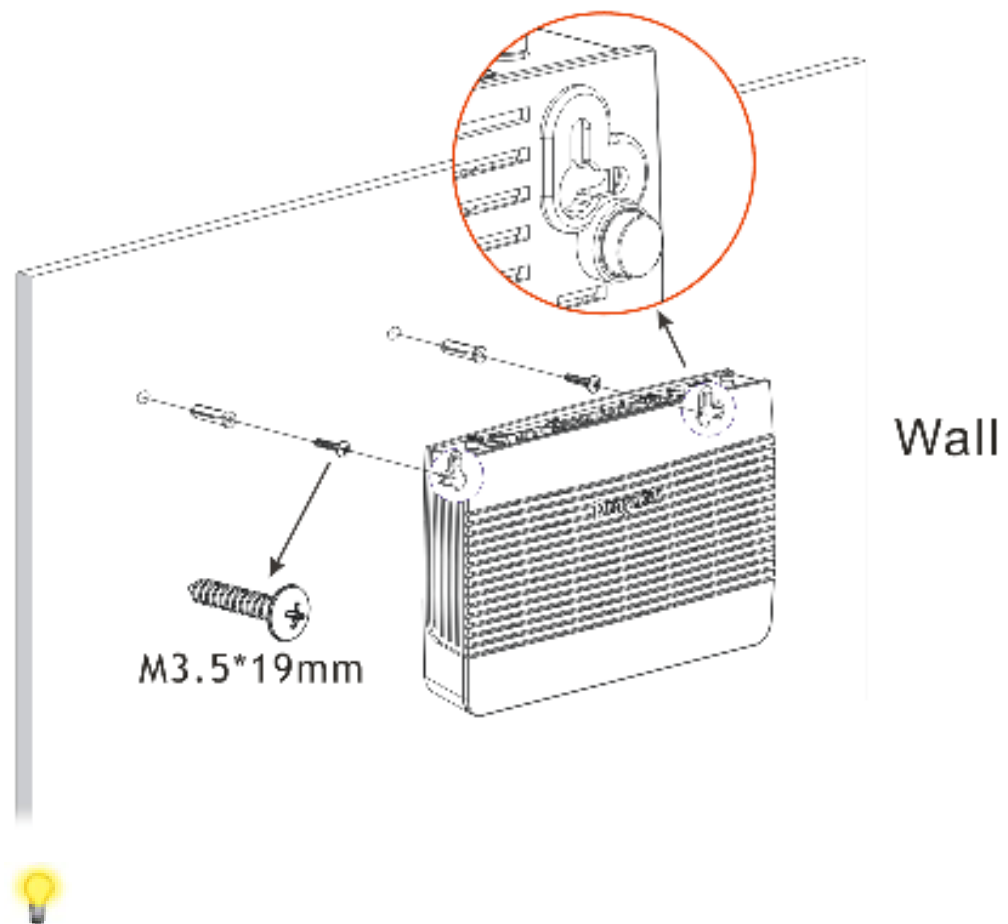


(For the detailed information of LED status, please refer to section I-1-1 Indicators and Connectors.)

I-2-2 Wall-Mounted Installation

Vigor2765 has keyhole type mounting slots on the underside.

1. A template is provided on the Vigor2765 packaging box to enable you to space the screws correctly on the wall.
2. Place the template on the wall and drill the holes according to the recommended instruction.
3. Fit screws into the wall using the appropriate type of wall plug.



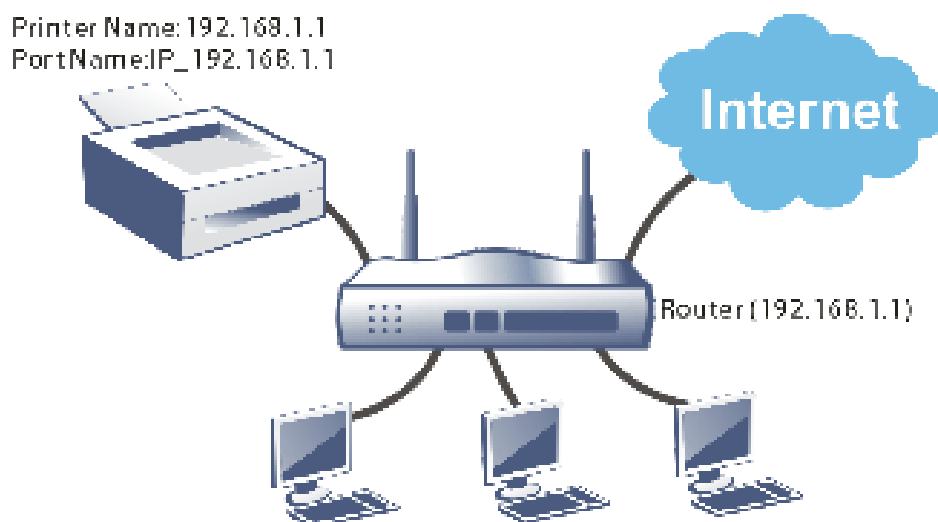
Note

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

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

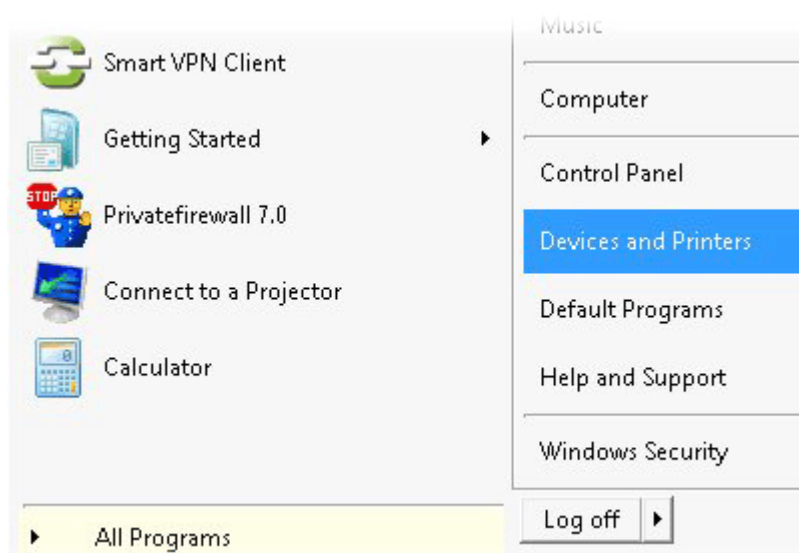
I-2-3 Installing USB Printer to Vigor Router

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

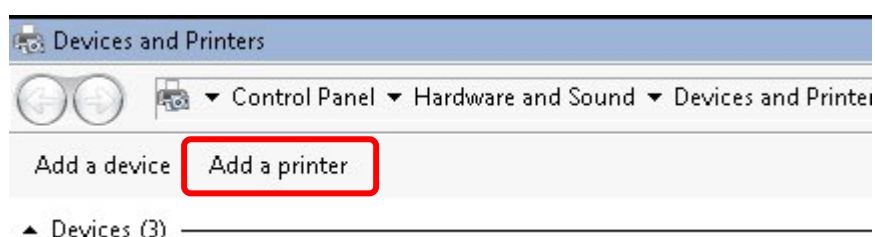


Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

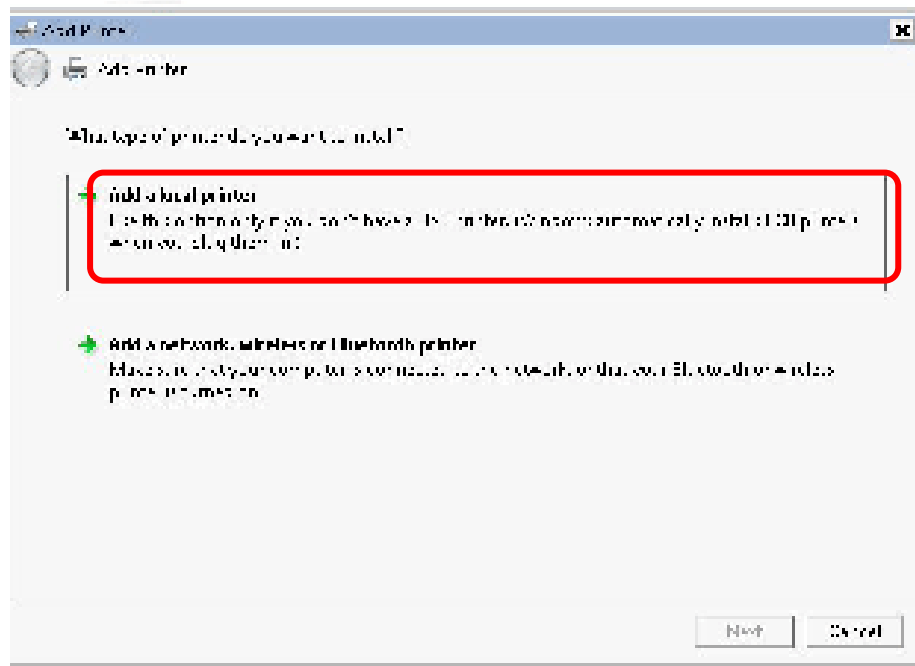
1. Connect the printer with the router through USB/parallel port.
2. Open **All Programs >> Getting Started >> Devices and Printers**.



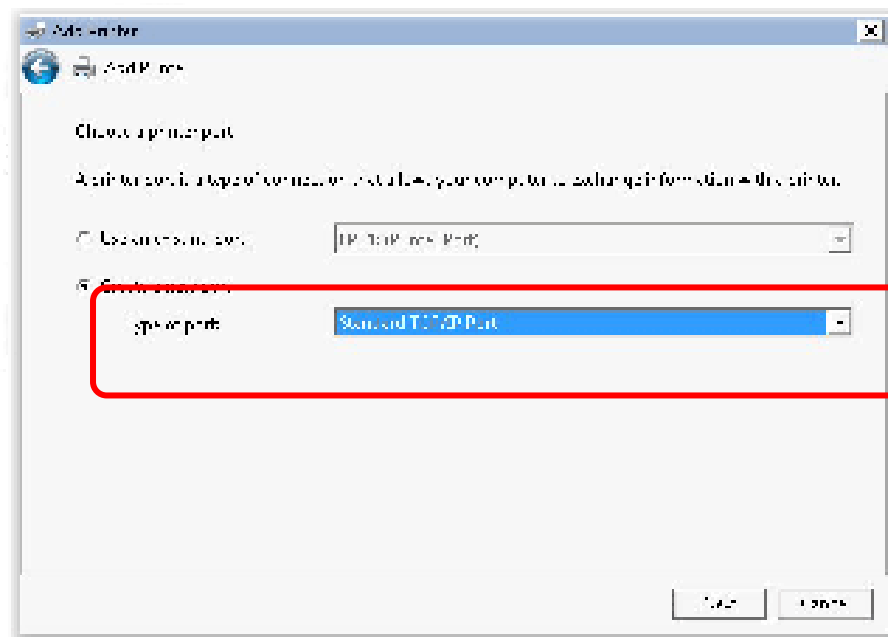
3. Click **Add a printer**.



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



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



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

Add Interface

Type a protocol hostname or IP address:

Device type: TCP/IP Device

Hostname or IP Address: 192.168.1.1

Port name: 192.168.1.1

☐ Query the interface and summarize the data that show on it

Next Cancel

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

Add Interface

Additional port information required

The network card found on the network is the following:

1. The network card name
2. The network card manufacturer
3. The network card type or chipset
4. The address of the network card in memory

Please click the radio button corresponding to the Basic function of the network card. Then, select the address and port name for this card on the network. If you select the standard network card type, the device type will be:

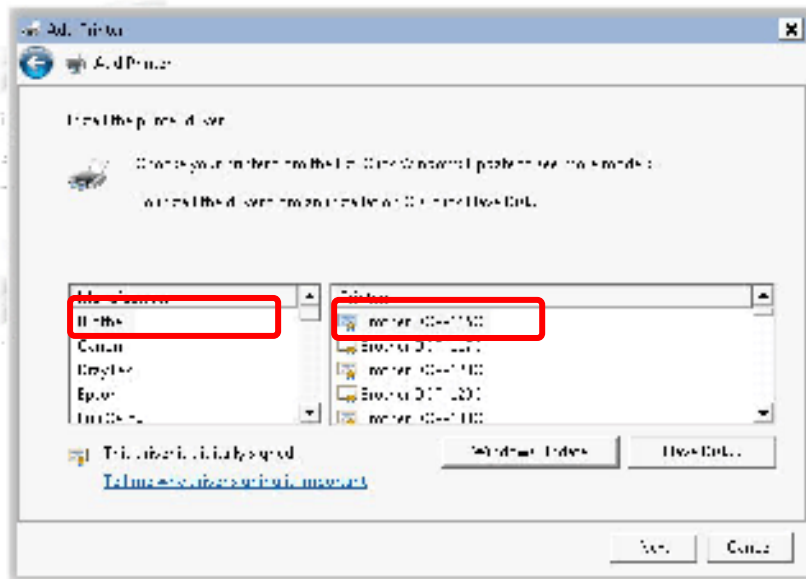
Device Type:

☒ Standard: Generic Network Card

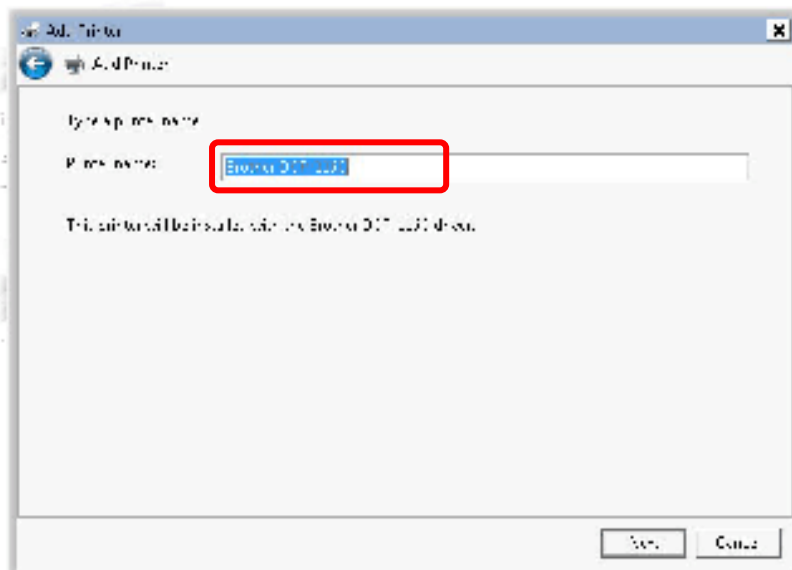
☐ Custom: Settings...

Next Cancel

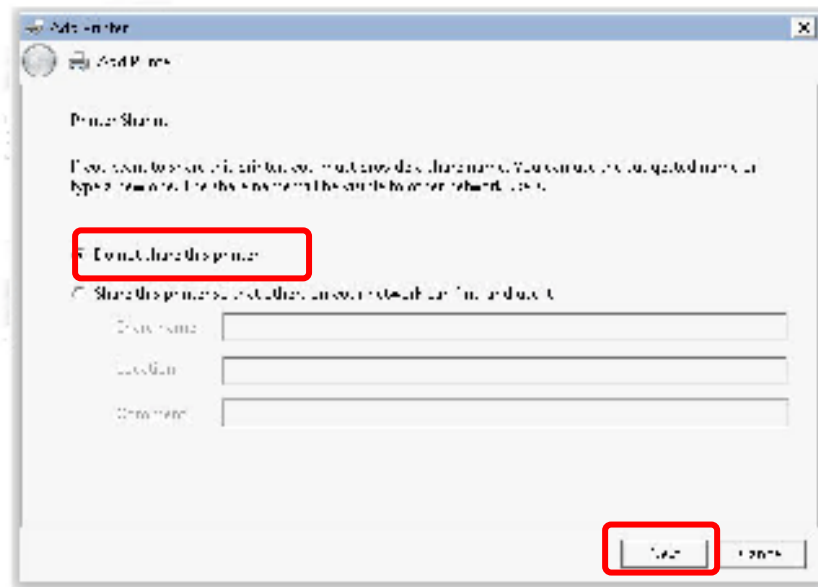
8. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.



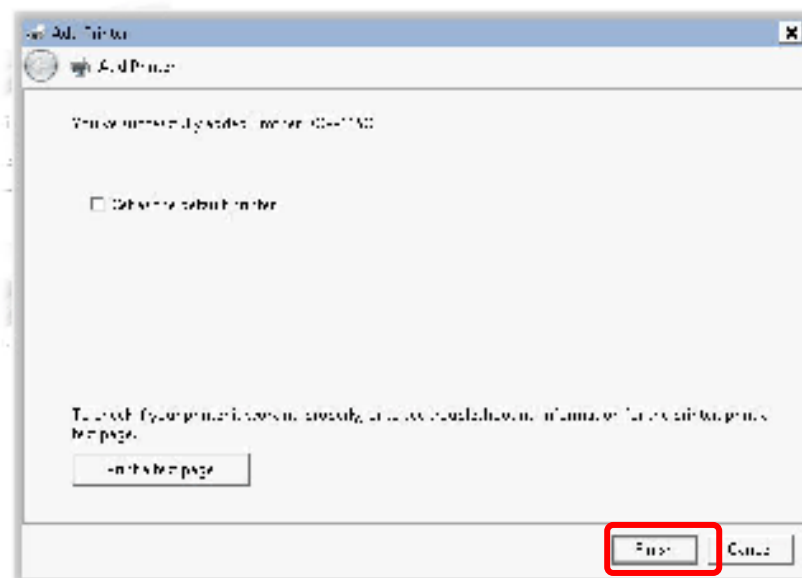
9. Type a name for the chosen printer. Click **Next**.



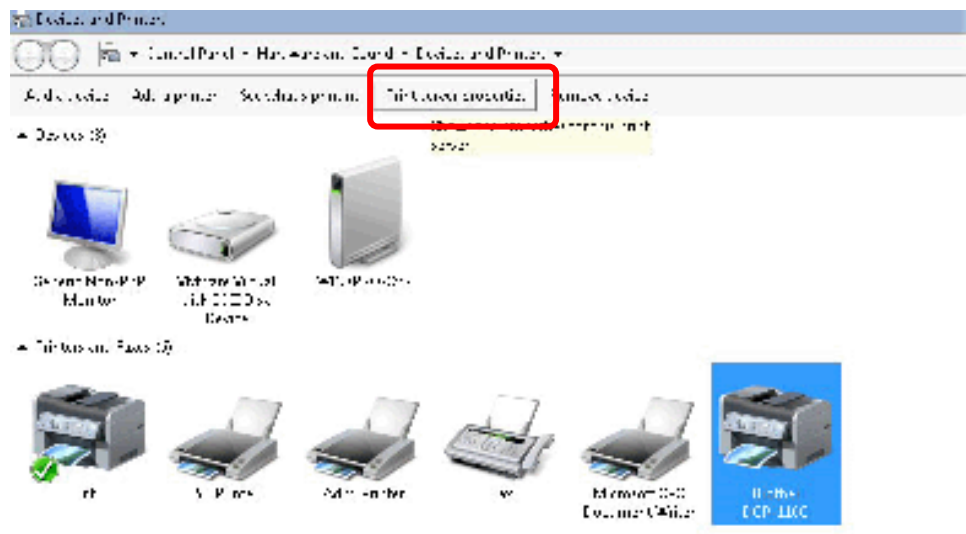
10. Choose **Do not share this printer** and click **Next**.



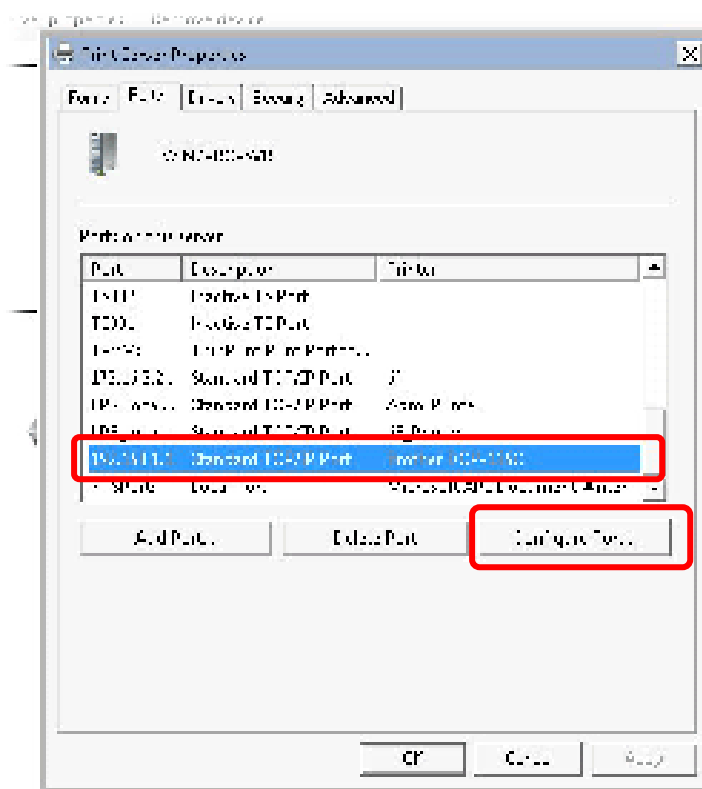
11. Then, in the following dialog, click **Finish**.



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.

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.



The image shows the login interface for a DrayTek Vigor2765 Series router. At the top, there is a red banner with the "DrayTek" logo on the left and "Vigor2765 Series" on the right. Below the banner is a black bar with the word "Login" in white. The main area is white and contains two input fields: "Username" and "Password". Below these fields is a grey "Login" button. Under the button, there is a "Security Warning" message: "Security Warning: You are logging in without encryption which is not recommended. To login securely [click here](#)." At the bottom, there is a small copyright notice: "Copyright © 2000-2010 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.

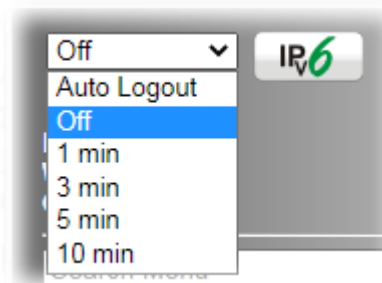
4. Now, the **Main Screen** will appear.



Info

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

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



I-4 Changing Password

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

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

System Maintenance >> Administrator Password Setup

Administrator Password

Old Password	Max: 63 characters
New Password	Max: 63 characters
Confirm Password	Max: 63 characters

Password Strength:

Strong password requirements:
1. Have at least one upper-case letter and one lower-case letter
2. Including non-alphanumeric characters is a plus.

☒ Enable Admin account login to Web UI from the Internet
☐ Enable Advanced Authentication method when login from "WAN"
☐ Time-based One-time Password (TOTP)
☒ Mobile one Time Passwords(mOTP)

Pin Code: Secret:

☐ 2 Step Authentication
Send Auth code via

4. Enter the login password (the default is “admin”) on the field of **Old Password**. Type **New Password** and **Confirm Password**. Then click **OK** to continue.
5. Now, the password has been changed. Next time, use the new password to access the Web user interface for this router.



The image shows the login page for a DrayTek Vigor2765 Series router. At the top, there is a red banner with the DrayTek logo and the text 'Vigor2765 Series'. Below the banner, the word 'Login' is displayed in a black box. The main area contains two input fields: 'Username' and 'Password'. Below these fields is a 'Login' button. A security warning message is displayed below the button: 'Security Warning: You are logging in without encryption which is not recommended. To login securely click here.' At the bottom, there is a small copyright notice: 'Copyright © 2020 DrayTek, Inc. All Rights Reserved'.



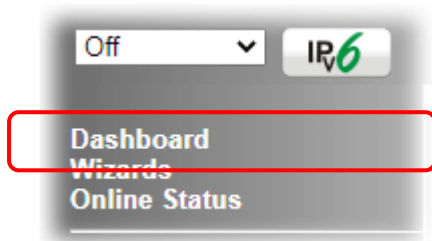
Info

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

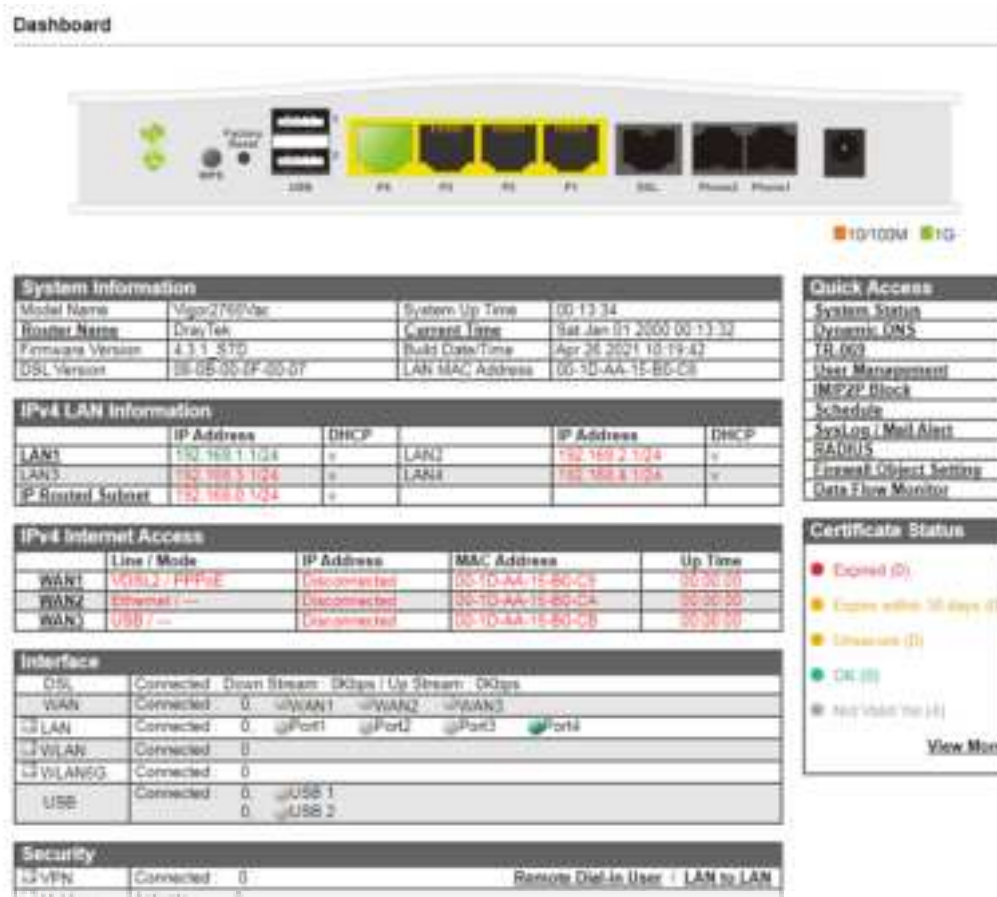
I-5 Dashboard

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:



I-5-1 Virtual Panel

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

Dashboard



For detailed information about the LED display, refer to [I-1-1 LED Indicators and Connectors](#).

I-5-2 Name with a Link

A name with a link (e.g., [Router Name](#), [Current Time](#), [WAN1~4](#) and etc.) below means you can click it to open the configuration page for modification.

System Information			
Model Name	Vigor2765NSe	System Up Time	00:14:51
Router Name	Unlink	Current Time	Sat Jul 01 2020 00:14:49
Firmware Version	6.3.1-STD	Build Date/Time	Apr 29 2021 10:15:17
MAC Address	00:1D:AA:15:8B:C4	LAN MAC Address	00:1D:AA:15:8B:C9

IPv4 LAN Information					
	IP Address	DHCP		IP Address	DHCP
LAN1	192.168.1.124	v	LAN3	192.168.2.124	v
LAN2	192.168.3.124	v	LAN4	192.168.4.124	v
IP Routed Subnet	192.168.0.124	v			

IPv4 Internet Access				
	Link / Mode	IP Address	MAC Address	Up Time
WAN1	DSL2/PPPoE	Disconnected	00:1D:AA:15:8B:C9	00:00:00
WAN2	Firewall / ...	Disconnected	00:1D:AA:15:8B:C4	00:00:00
WAN3	USB / ...	Disconnected	00:1D:AA:15:8B:C9	00:00:00

Interface	
DSL	Connected : Down Stream : UKbps / Up Stream : UKbps
WAN	Connected : 0 / WAN1 / WAN2 / WAN3
LAN	Connected : 0 / Port1 / Port2 / Port3 / Port4
WLAN	Connected : 0
WLAN2G	Connected : 0
USB	Connected : 0 / USB 1 / USB 2

Security	
VPN	Connected : 0 / Remote Dial in User / LAN to LAN
MyVPN	Activated : 0
DoS	Attack Detected
RunCA	

VoIP			
Port	Profile	Reg.	In/Out
Phone1	igmp	No	On
Phone2	igmp	No	On

System Resource	
Current Status	CPU Usage: 4%
	Memory Usage: 70%

Quick Access	
System Status	
Dynamic DNS	
TR 069	
User Management	
IMPP2P Block	
Schedule	
Syslog / Mail Alert	
RADIUS	
Firewall Object Setting	
Data Flow Monitor	

Certificate Status	
Expired (0)	
Expire within 30 days (0)	
Unknown (0)	
OK (0)	
Not Valid Yet (4)	

[View More](#)

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	
RADIUS	
Firewall Object Setting	
Data Flow Monitor	

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

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

Interface	
ETH	Connected : 0 Down Stream : 0Kbps / Up Stream : 0Kbps
WAN	Connected : 0, WAN1, WAN2, WAN3
LAN	Connected : 0, Port1, Port2, Port3, Port4
WLAN	Connected : 0
WLAN5G	Connected : 0
USB	Connected : 0, USB 1, USB 2
Security	
VPN	Connected : 0 Remote Dial-in User / LAN to LAN
MyVigor	Activate : 0
DoS	Attack Detected :
RootCA	

Note that there is a plus () icon located on the left side under Interface/Security. Click it to review detailed information for LAN, WLAN, VPN, MyVigor, DoS, and/or RootCA used presently.

Security				
VPN	Connected : 0 Remote Dial-in User / LAN to LAN			
MyVigor	Activate : 0			
DoS	Attack Detected :			
RootCA				
	Service	Status	Start Date	Expire Date
	RootCA1	Not Valid Yet	Aug 13 07:08:41 2020 GMT	Apr 22 07:08:41 2034 GMT

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

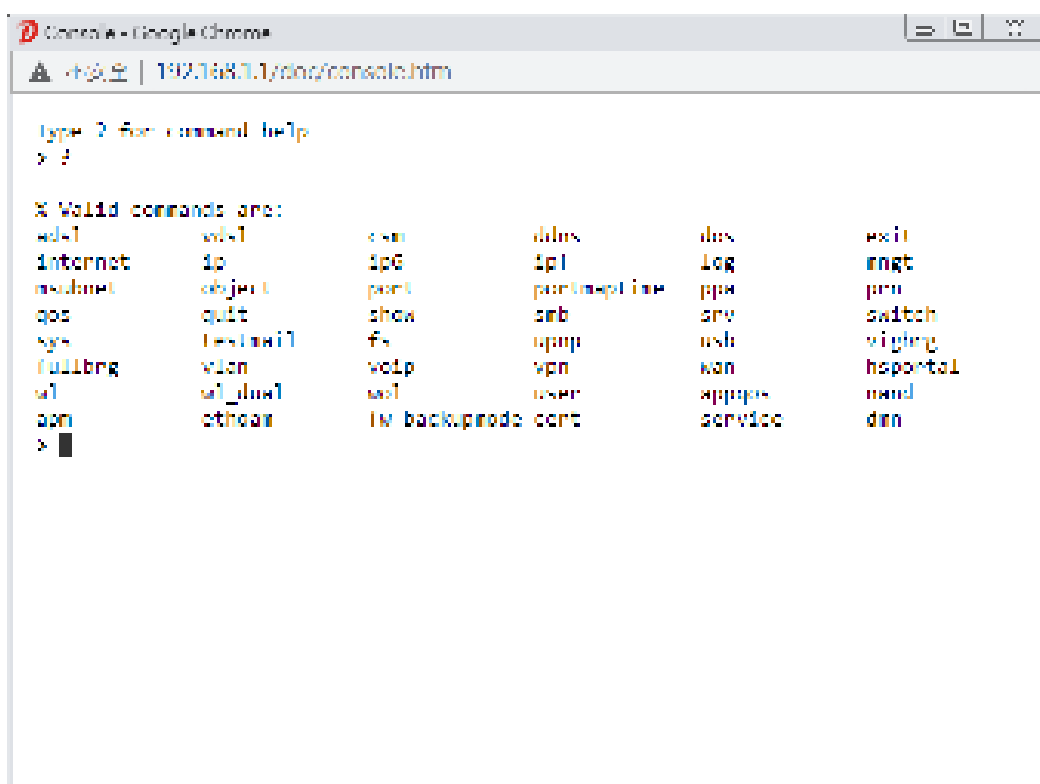
Dashboard			Certificate Management	Local Certificate
Wireless	Quick Start Wizard			Trusted CA Certificate
	Service Activation Wizard			Certificate Backup
	VPN Client Wizard			Self-Signed Certificate
	VPN Server Wizard	WAP		General Settings
	Wireless Wizard			SIP Accounts
	Mesh Wizard			VoIP Plan
	VoIP Wizard			Phone Settings
Online Status				Status
	Physical Connection			Diagnosis
	Virtual WAN	Mesh		Mesh Setup
WAN	General Setup			Mesh Status
	Internet Access			Mesh Discovery
	Multi-PVC/M-AN			Basic Config Setup
	WAN Duplex			Support List
LAN		Wireless LAN (2.4 GHz)		General Setup
	General Setup			Security
	VLAN			Access Control
	Link Up to WAN			WPS
	LAN Port Mirror			Advanced Setting
	Wireless LAN			Station Control
Integrated Web Portal	Profile Setup			Bandwidth Management
	Config Management			AP Discovery
Routing				Antenna Firmware
	Static Route			Load Balancing
	Route Policy			Roaming
NAT		Wireless LAN (5 GHz)		Station List
	Port Redirection			General Setup
	NAT Rule			Security
	Open Ports			
	Port Forwarding			

I-5-5 Web Console



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

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



I-5-6 Config Backup



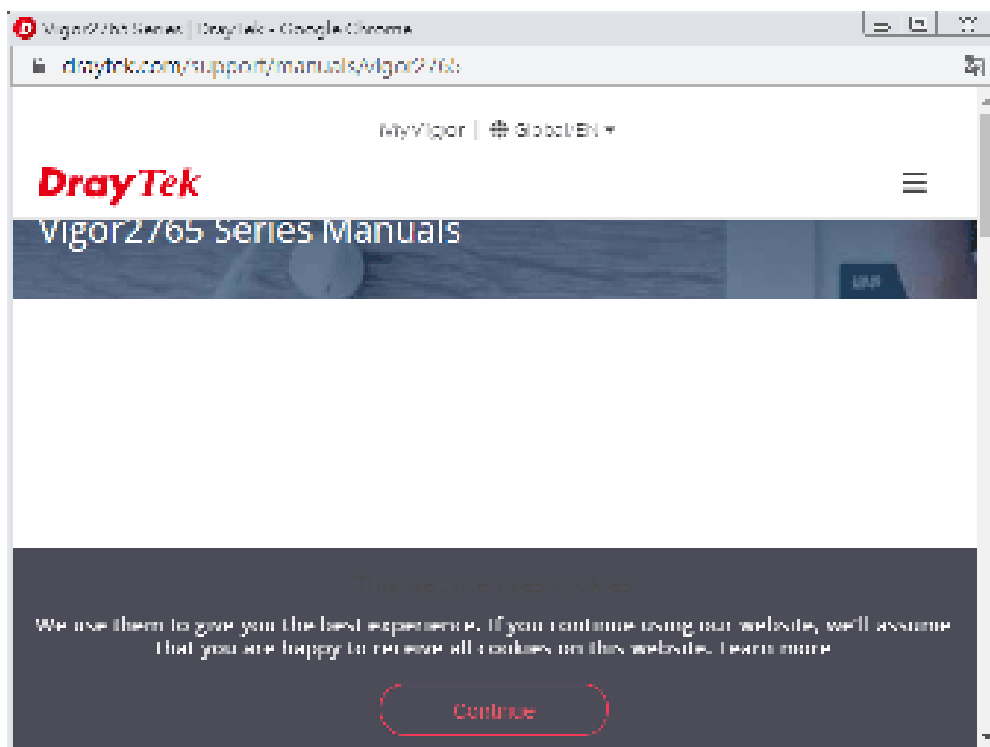
There is one way to store current used settings quickly by clicking the **Config Backup** icon. It allows you to backup current settings as a file. Such configuration file can be restored by using **System Maintenance>>Configuration Backup**.

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

I-5-7 Manual Download



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



I-5-8 Logout



Click this icon to exit the web user interface.

I-5-9 Online Status

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

I-5-9-1 Physical Connection

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

Physical Connection for IPv4 Protocol

Online Status

Physical Connection			System Uptime: 1 day 5:29:14		
IPv4		IPv6			
LAN Status					
IP Address	TX Packets	RX Packets	Router Primary DNS:	Router Secondary DNS:	
192.168.1.1	5,030	15,414	8.8.8.8	8.8.4.4	
WAN 1 Status					Dial PPPoE
Enable	Line	Name	Mode	Up Time	
Yes	VDSL2		7775E	00:00:00	
IP	GW IP	TX Bytes	TX Rate(bps)	RX Bytes	RX Rate(bps)
---	---	0 (B)	0	0 (B)	0
WAN 2 Status					
Enable	Line	Name	Mode	Up Time	
No	Ethernet		---	00:00:00	
IP	GW IP	TX Bytes	TX Rate(bps)	RX Bytes	RX Rate(bps)
---	---	0 (B)	0	0 (B)	0
WAN 3 Status					
Enable	Line	Name	Mode	Up Time	Signal
Yes	USB		---	00:00:00	-
IP	GW IP	TX Bytes	TX Rate(bps)	RX Bytes	RX Rate(bps)
---	---	0 (B)	0	0 (B)	0
Line 1 Information (vDSL2 Firmware Version: 7708L7_A/B/C)					
Profile	State	UP Speed	Down Speed	SNR Upstream	SNR Downstream
TRADING		0 (Kbps)	0 (Kbps)	0 (dB)	0 (dB)

Physical Connection for IPv6 Protocol

Online Status

Physical Connection		System Uptime: 2 days 20:16:18	
IPv4		IPv6	
LAN Status			
IP Address: 192.168.1.100 (192.168.1.100)			
TX Packets: 1,111,111		RX Packets: 1,111,111	
TX Bytes: 1,111,111		RX Bytes: 1,111,111	
WAN1 IPv6 Status			
Enable: No		Mode: No Line	
IP:		Up Time: Gateway IP	
WAN2 IPv6 Status			
Enable: No		Mode: No Line	
IP:		Up Time: Gateway IP	
WAN3 IPv6 Status			
Enable: No		Mode: No Line	
IP:		Up Time: Gateway IP	

Detailed explanation (for IPv4) is shown below:

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

Item	Description
	interface.

Detailed explanation (for IPv6) is shown below:

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



Info

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

I-5-9-2 Virtual WAN

Such page displays the virtual WAN connection information.

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

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

I-6 Quick Start Wizard

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

Quick Start Wizard

Enter login password

Please enter an alphanumeric string as your Password (Max 83 characters)

Old Password	
New Password	
Confirm Password	

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.

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

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

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

Quick Start Wizard

WAN Interface

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

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

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

I-6-1 For WAN1 (ADSL)

WAN1 is specified for ADSL or VDSL2 connection.

Quick Start Wizard

WAN Interface

WAN Interface:	WAN1
Display Name:	
Physical Mode:	ADSL/VDSL2
DSL Mode:	Auto
Physical Type:	Auto negotiation
VLAN Tag insertion (ADSL):	Disable
VLAN Tag insertion (VDSL2):	Disable

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

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

PPPoE/PPPoA

PPPoE stands for **Point-to-Point Protocol over Ethernet**. It relies on two widely accepted standards: PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet can share a common connection.

PPPoE is used for most of DSL modem users. All local users can share one PPPoE connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode.

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

Quick Start Wizard

Connect to Internet

WAN 1	Protocol		PPPoE / PPPoA
For ADSL Only:			
Encapsulation	PPPoE L2/L3/NAT		
VPI	0	Auto detect	
VCI	33		
Fixed IP	☐ Yes ☒ No (Dynamic IP)		
IP Address			
Subnet Mask			
Default Gateway			
Primary DNS	0.0.0.0		
Second DNS	8.8.8.8		

Available settings are explained as follows:

Item	Description
Protocol / Encapsulation	Choose PPPoE/PPPoA for WAN1 interface.
VPI	Enter the value provided by ISP. Auto detect – Click this button to have the VPI and VCI to be detected by the system automatically
VCI	Type in the value provided by ISP.
Fixed IP	Click Yes to enable Fixed IP feature.
IP Address	Enter the IP address if Fixed IP is enabled.
Subnet Mask	Enter the subnet mask for the IP address.
Default Gateway	Enter the default gateway of the DSL Internet connection, if Fixed IP is enabled.
Primary DNS	Enter the primary IP address for the router.
Second DNS	Enter secondary IP address for necessity in the future.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

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

Quick Start Wizard

Set PPPoE / PPPoA

WAN 1	
Service Name (optional)	040067888@inet.net
Username	84005768
Password	*****
Confirm Password	*****

Available settings are explained as follows:

Item	Description
Service Name (Optional)	Enter the description of the specific network service.
User Name	Enter the valid user name (maximum 63 characters) provided by the ISP in this field.
Password	Enter a valid password provided by the ISP.
Confirm Password	Retype the password.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

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

Quick Start Wizard

Please confirm your settings

WAN Interface	WAN1
Physical Mode	Static IP
MTU	1500
Primary IP / Subnet Mask	192.168.1.10 / 255.255.255.0
Gateway	192.168.1.1
Primary DNS	192.168.1.1
Secondary DNS	192.168.1.1

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

Quick Start Wizard Setup OK!

- Now, you can enjoy surfing on the Internet.

MPoA / Static or Dynamic IP

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

Available settings are explained as follows:

Item	Description
Protocol	There are two modes offered for you to choose for WAN1 interface. Choose MPoA as the protocol.
For ADSL Only	Such field is provided for ADSL only. You have to choose encapsulation and type the values for VPI and VCI. Or, click Auto detect to find out the best values.
Fixed IP	Click Yes to enable Fixed IP feature.
IP Address	Enter the IP address if Fixed IP is enabled.
Subnet Mask	Enter the subnet mask.
Default Gateway	Enter the IP address as the default gateway.
Primary DNS	Enter the primary IP address for the router.
Secondary DNS	Enter the secondary IP address for necessity in the future.

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

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

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN1
Physical Mode:	Static / PPPoE
VLAN:	1
MAC:	00
Port 1 / Description:	LAN - RJ45 10/100
Fixed IP:	No
Primary DNS:	1.1.1.1
Secondary DNS:	1.1.1.2

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

Quick Start Wizard Setup OK!

- Now, you can enjoy surfing on the Internet.

I-6-2 For WAN2 (Ethernet)

WAN2 is dedicated to physical mode in Ethernet. Please select the appropriate Internet access type according to the information from your ISP. For example, you should select PPPoE mode if the ISP provides you PPPoE interface.

Quick Start Wizard

WAN Interface

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

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
Display Name	Type a name for the router.
VLAN Tag insertion	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. Disable - Disable the function of VLAN with tag. Tag value - Type the value as the VLAN ID number. The range is form 0 to 4095. Priority - Type the packet priority number for such VLAN. The range is from 0 to 7.

PPPoE

PPPoE stands for **Point-to-Point Protocol over Ethernet**. It relies on two widely accepted standards: PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet can share a common connection.

PPPoE is used for most of DSL modem users. All local users can share one PPPoE connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode.

1. Choose **WAN2** as the WAN Interface and click the **Next** button. The following page will be open for you to specify Internet Access Type.

Quick Start Wizard

Connect to Internet

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

☒ PPPoE
☐ PPPoP
☐ L2TP
☐ Static IP
☐ DHCP

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

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

Quick Start Wizard

PPPoE Client Mode

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

Service Name (Optional)

Username

Password

Confirm Password

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

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. 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:

Auto Interface	Auto
Physical Mode	Bridge
Physical Type	Auto negotiation
Internet Address	192.1

Click Back to modify changes if necessary. Click Finish to save the current settings and proceed to the next screen.

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

Quick Start Wizard Setup OK!

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

PPTP/L2TP

1. Choose **WAN2** as the WAN Interface and click the **Next** button. The following page will be open for you to specify Internet Access Type.

Quick Start Wizard

Connect to Internet

WAN2
Select one of the following Internet Access types provided by your ISP:

☐ PPPoE
☒ PPTP
☐ L2TP
☐ Static IP
☐ DHCP

< Back Next > Finish Cancel

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

Quick Start Wizard

PPTP Client Mode

WAN2
Enter the username, password, WAN IP configuration and PPTP server IP provided by your ISP:

Username:

Password:

Confirm Password:

WAN IP Configuration

☐ Obtain an IP address automatically
☒ Specify an IP address

IP Address:

Subnet Mask:

Gateway:

Primary DNS:

Second DNS:

PPTP Server:

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
Username	Assign a specific valid user name provided by the ISP. The maximum length of the user name you can set is 63 characters.
Password	Assign a valid password provided by the ISP. The maximum length of the password you can set is 62 characters.
Confirm Password	Retype the password.
WAN IP Configuration	Obtain an IP address automatically - the router will get an

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

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

Auto. IP Address	Auto
Physical Mask	255.0.0.0
Physical Type	Static IP Address
Internet Address	192.168.1.1

Click Back to modify changes if necessary. Click Finish to save the current settings and proceed to the next screen.

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.

Static IP

1. Choose **WAN2** as the WAN Interface and click the **Next** button. The following page will be open for you to specify Internet Access Type.

Quick Start Wizard

Connect to Internet

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

☐ PPPoE
☐ PPTP
☐ L2TP
☒ Static IP
☐ DHCP

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

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

Quick Start Wizard

Static IP Client Mode

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

WAN IP	192.168.3.100
Subnet Mask	255.255.255.0
Gateway	192.168.3.1
Primary DNS	8.8.8.8
Secondary DNS	8.8.4.4 (optional)

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

Available settings are explained as follows:

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

Cancel	Click it to give up the quick start wizard.

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

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN2
Physical Mode:	1: Ethernet
Physical Type:	Static IP
Static IP:	Static IP

Click **Back** to modify settings if necessary. Otherwise, click **Finish** to save the current settings and enter the Main menu.

Back Next Finish Cancel

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

Quick Start Wizard Setup OK!

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

DHCP

1. Choose **WAN2** as WAN Interface and click the **Next** button. The following page will be open for you to specify Internet Access Type.

Quick Start Wizard

Connect to Internet

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

☐ PPPoE
☐ PPTP
☐ L2TP
☐ Static IP
☒ DHCP

< Back Next > Finish Cancel

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

Quick Start Wizard

DHCP Client Mode

WAN 2
If your ISP requires you to enter a specific host name or specific MAC address, please enter it in

Host Name (optional)

MAC (optional)

< Back Next > Finish Cancel

Available settings are explained as follows:

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

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

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN2
Physical Mode:	Ethernet
Physical Type:	Auto Negotiation
Internet Access:	DHCP

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

Back

Cancel

Finish

Cancel

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

Quick Start Wizard Setup OK!

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

I-6-3 For WAN3 (USB)

WAN3/WAN4 is dedicated to physical mode in USB.

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

Quick Start Wizard

WAN Interface

WAN Interface:	WAN3
Display Name:	
Physical Mode:	USB

Back Next Finish Cancel

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

Quick Start Wizard

Connect to Internet

WAN 3	
Internet Access :	3G/4G USB Modem(PPP mode)
3G/4G USB Modem(PPP mode)	
SIM PIN code	
Modem Initial String	AT&F0V1X1&D2&C150=0
	(Default: AT&F0V1X1&D2&C150=0)
APN Name	
	Apply

Back Next Finish Cancel

Available settings are explained as follows:

Item	Description
Internet Access	Choose one of the selections as the protocol of accessing the internet.
3G/4G USB Modem (PPP mode)	SIM Pin code -Type PIN code of the SIM card that will be used to access Internet. The maximum length of the pin code you can set is 15 characters. Modem Initial String - Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP. The maximum length of the string you can set is 47 characters. APN Name - APN means Access Point Name which is provided

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

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

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN3
Physical Mode:	USB
Internet Access:	PPP

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

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

Quick Start Wizard Setup OK!

- Now, you can enjoy surfing on the Internet.

I-7 Service Activation Wizard

Service Activation Wizard can guide you to activate WCF service (Web Content Filter) with a quick and easy way. **For the Service Activation Wizard is only available for admin operation, therefore, please type “admin/admin” on Username/Password while Logging into the web user interface.**

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

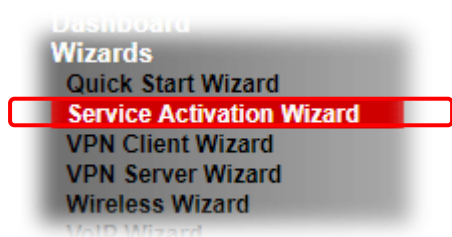
Now, follow the steps listed below to activate WCF feature for your router.



Info

Such function is available only for Admin Mode.

1. Open **Wizards>>Service Activation Wizard**.



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

Service Activation Wizard

Before this service type that you need to activate:

Web Content Filter (WCF) Services:

- ☒ WCF: [License Agreement](#)
Take your router and this will be provided with features and services. This will be activated and the configuration will be applied immediately and fully. You may cancel this configuration at any time.
- ☒ Dynamic DNS (DDNS): [License Agreement](#)
Take your router and activate this service. This will be activated and the configuration will be applied immediately and fully. You may cancel this configuration at any time.

APP Enforcement (APP) Services:

- ☒ APP: [License Agreement](#)
Configure APP Enforcement services.

Dynamic DNS (DDNS) Services:

- ☒ DDNS: [License Agreement](#)
This dynamic DNS service is provided by a third party. To activate the service, you must select this option to accept the license. This is a service that allows you to use the service that has been provided by a third party. You may cancel this configuration at any time.
- ☒ I agree to let the third party record the version or content or address of this router in order to activate the DDNS service.

Remember to read the license agreement of this service.

☒ I have read and accept the terms Agreement of this service.

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 (2010020111502701.draydns.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).

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.

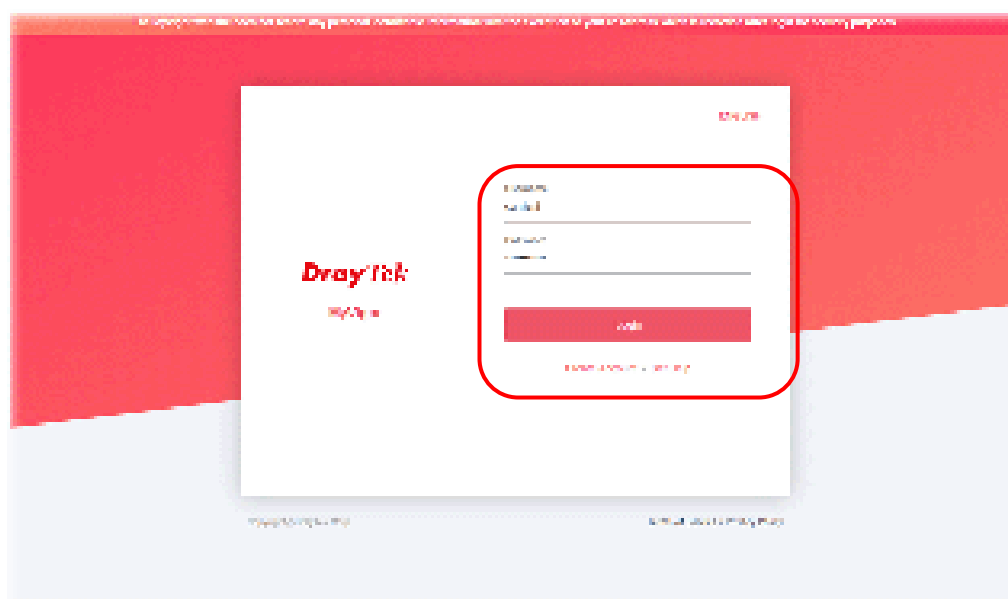


The image shows the login page for the DrayTek Vigor2765 Series router. At the top, there is a red banner with the DrayTek logo on the left and "Vigor2765 Series" on the right. Below the banner, the word "Login" is displayed in a black box. There are two input fields: "Username" and "Password". Below these fields is a "Login" button. A security warning message is displayed: "Security Warning: You are logging in without encryption which is not recommended. To login securely [click here](#)." At the bottom, there is a copyright notice: "Copyright © 2009-2012 DrayTek Corp. All Rights Reserved".

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



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



The image shows the DrayTek MyVigor login page. It features a red header with a copyright notice. The main content area has a white background with the DrayTek logo and "MyVigor" text. There is a login form with fields for "Username" and "Password", and a "Login" button. A red box highlights the login form area. At the bottom, there is a copyright notice: "Copyright © 2009-2012 DrayTek Corp. All Rights Reserved".



Info

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

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

Product register (Add Device)

Device Name	Vigor2765
Model	Vigor2765
MAC	1440B00287E8
Serial Number	2020122611165901

Submit

- When the following page appears, your router information has been added to the database. Your router has been registered to *myvigor* website successfully.

MyVigor MY PRODUCT HIGH AVAILABILITY SETTINGS CUSTOMER SURVEY AGENT

WCF APPS DryBONS

Cyren DPV

License Status: Active

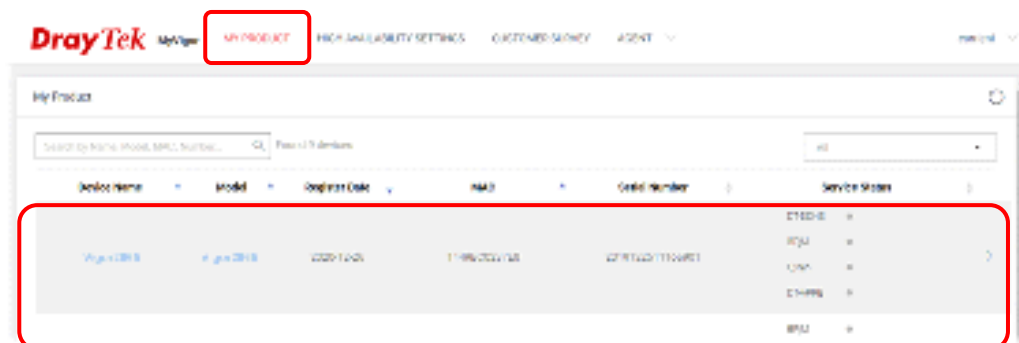
License Action: Activate License Force Sync

License History

Today 2019-12-26

Product Registration 2019-12-26

- 6 Clicking **MY PRODUCT** for viewing the general information of the registered router on MyVigor website.



This page is left blank.

Part II Connectivity



WAN

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



LAN

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

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



NAT

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



Applications

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



Routing

Static Route, Route Policy

II-1 WAN

It allows users to access Internet.

Basics of Internet Protocol (IP) Network

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

From 10.0.0.0 to 10.255.255.255

From 172.16.0.0 to 172.31.255.255

From 192.168.0.0 to 192.168.255.255

What are Public IP Address and Private IP Address

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

Get Your Public IP Address from ISP

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

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

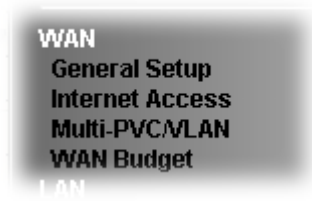
Network Connection by 3G/4G USB Modem

For 3G/4G mobile communication through Access Point is popular more and more, Vigor2765 adds the function of 3G/4G network connection for such purpose. By connecting 3G/4G USB Modem to the USB port of Vigor2765, it can support LTE/HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G/4G standard (HSUPA, etc). Vigor2765n 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 Vigor2765ac series.



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

Web User Interface



II-1-1 General Setup

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

This router supports multiple-WAN function. It allows users to access Internet and combine the bandwidth of the multiple WANs to speed up the transmission through the network. Each WAN port can connect to different ISPs, Even if the ISPs use different technology to provide telecommunication service (such as DSL, Cable modem, etc.). If any connection problem occurred on one of the ISP connections, all the traffic will be guided and switched to the normal communication port for proper operation. Please configure WAN1, WAN2, WAN3 and WAN4 settings.

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

WAN == General Setup

Index	Enable	Physical Mode/Type	Active Mode
WAN1	☒	VDSL2	Always On
WAN2	☐	LAN Port 4	Follow
WAN3	☒	USB	Follow

Note:

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

OK

Cancel

Available settings are explained as follows:

Item	Description
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.
Active Mode	Display whether such WAN interface is Active device or backup device.

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

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

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

WAN >> General Setup

WAN 1

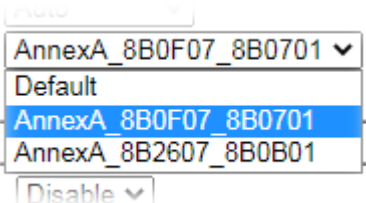
Enable:	Yes ▼	
Display Name:		
Physical Mode:	VDSL2	
DSL Mode:	Auto ▼	
DSL Modem Code:	AnnexA_8B0F07_8B0701 ▼	
Antenna Mode:	Always On ▼	
VLAN Tag insertion	Customer (IEEE 802.1Q)	Service (IEEE 802.1Q)
ADSL	Disable ▼ Tag value: 0 (0-4095) Priority: 0 (0-7)	
VDSL2	Disable ▼ Tag value: 0 (0-4095) Priority: 0 (0-7)	Disable ▼ Tag value: 0 (0-4095) Priority: 0 (0-7)

Note:

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

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.
DSL Mode	Specify the physical mode (VDSL2 or ADSL) for such router manually.
DSL Modem Code	Choose the correct DSL modem code for ensuring the network connection.  If you have no idea about the selection, simply choose Default or contact the dealer for assistance.
VLAN Tag insertion (ADSL/VDSL)	Such feature is offered to the user with the environment supporting IEEE_802.1ad. In which, service is used for outer tag; customer is used for inner tag. Enable - Enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the WAN while sending them out.

	Please type the tag value and specify the priority for the packets sending by WAN1. 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. Disable - Disable the function of VLAN with tag.

II-1-1-2 WAN2 (Ethernet)

Ethernet is the Physical Mode for WAN2.

WAN => General Setup

WAN 2

Enable	Yes
Display Name	
Physical Mode	Ethernet
Physical Type	Auto negotiation
Active Mode	Failover
	WAN Failure
VLAN Tag insertion	Disable
	Tag value: Priority
	0 0
	(0-4095) (0-7)

Note:

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

OK Cancel

Available settings are explained as follows:

Item	Description
Enable	Choose Yes to invoke the settings for this WAN interface. Choose No to disable the settings for this WAN interface.
Display Name	Type the description for such WAN interface.
Physical Mode	Display the physical mode of such WAN interface.
Physical Type	You can change the physical type for WAN1/WAN2/WAN3 or choose Auto negotiation for determined by the system.
Active Mode	Always On - Choose it to make the WAN connection being activated always. Failover - Choose it to make the WAN connection as a backup connection. ● WAN Failure - When the active WAN failed, such WAN will be activated as the main network connection.
VLAN Tag insertion	Enable - Enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the WAN while sending them out. Please type the tag value and specify the priority for the packets sending by WAN1. 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.

	Disable - Disable the function of VLAN with tag.

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

II-1-1-3 WAN3 (USB)

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

WAN >> General Setup

WAN 3

Enable	Yes
Display Name	
Physical Mode	USB
Active Mode	☐ Failover ☒ WAN Failure

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.
Active Mode	Always On - Choose it to make the WAN connection being activated always. Failover - Choose it to make the WAN connection as a backup connection. WAN Failure - When the active WAN failed, such WAN will be activated as the main network connection.

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

II-1-2 Internet Access

For the router supports multi-WAN function, the users can set different WAN settings (for WAN1/WAN2/WAN3) for Internet Access. Due to different Physical Mode for WAN interface, the Access Mode for these connections also varies. Refer to the following figures.

WAN => Internet Access

Internet Access

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

DHCP Client Option

And,

WAN => Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode	Details Page	IPv6
WAN1		ADSL / VDSL2	PPPoE / PPPoA	Details Page	IPv6
WAN2		Ethernet	None	Details Page	IPv6
WAN3		USB	None	Details Page	IPv6
			PPPoE		
			Static or Dynamic IP		
			PPPoE2TP		

DHCP Client Option

And,

WAN => Internet Access

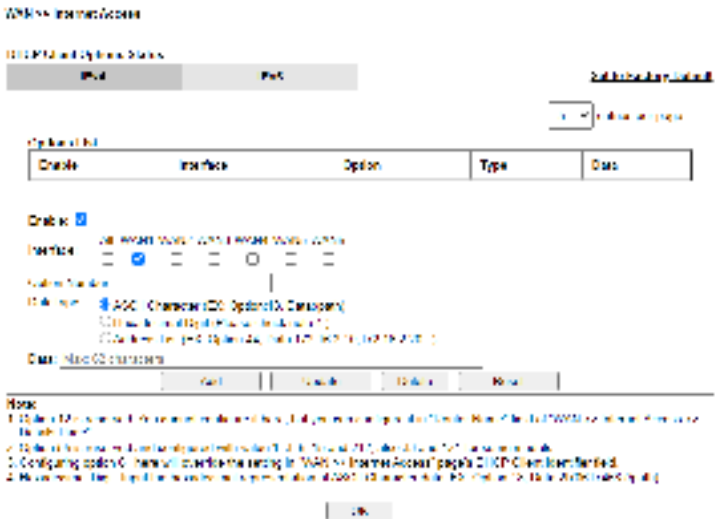
Internet Access

Index	Display Name	Physical Mode	Access Mode	Details Page	IPv6
WAN1		ADSL / VDSL2	PPPoE / PPPoA	Details Page	IPv6
WAN2		Ethernet	None	Details Page	IPv6
WAN3		USB	None	Details Page	IPv6
			None		
			3G/4G USB Modem(HPP mode)		
			3G/4G USB Modem(UTMP mode)		

DHCP Client Option

Available settings are explained as follows:

Item	Description
Index	Display the WAN interface.
Display Name	It shows the name of the WAN1/WAN2/WAN3 that entered in general setup.
Physical Mode	It shows the physical connection for WAN1-2 (Ethernet) /WAN3 (3G/4G USB Modem) according to the real network connection.
Access Mode	Use the drop down list to choose a proper access mode. The

	details page of that mode will be popped up. If not, click Details Page for accessing the page to configure the settings.
Details Page	This button will open different web page (based on IPv4) according to the access mode that you choose in WAN interface. Note that Details Page will be changed slightly based on physical mode.
IPv6	This button will open different web page (based on Physical Mode) to setup IPv6 Internet Access Mode for WAN interface. If IPv6 service is active on this WAN interface, the color of "IPv6" will become green.
DHCP Client Option	This button allows you to configure DHCP client options. DHCP packets can be processed by adding option number and data information when such function is enabled and configured.  Enable - 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 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 - Enter a number for such function. Data Type - Choose the type (ASCII or Hex or Address) for the data to be stored. Data - Enter 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>>Internet Access will be overwritten.

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

WAN >> Internet Access

WAN 1

PPPoE / PPPoA	MPoA / Static or Dynamic IP	IPv6
☒ Enable ☐ Disable		
ADSL Modem Settings		
Multi-PVC channel	Channel 1	
VPI	0	
VCI	33	
Encapsulating type	LLC/SNAP	
Protocol	PPPoE	
Modulation	Multimode	
ISP Access Setup		
Username	Max: 63 characters	
Password	Max: 62 characters	
More Options		
WAN Connection Detection		
Mode	PPP Detect	
MTU 1492 (Max: 1500) Path MTU Discovery		
PPPoE Setup		
PPP Authentication: PAP/CHAPv1/MS-CHAPv1/MS-CHAPv2		
IP Assignment (IPCP): ☐ Static ☒ Dynamic		
Fixed IP Address: WAN IP Alloc		
Dial Out Schedule Index(1-16) in Schedule Setup: Name: Name: Name:		
PPPoE Pass through ☐ For Wired LAN ☐ For Wireless LAN		
MAC Address ☒ Default MAC Address ☐ Use the following MAC Address: DD : DD : AA : 00 : 00 : 00		

Note:

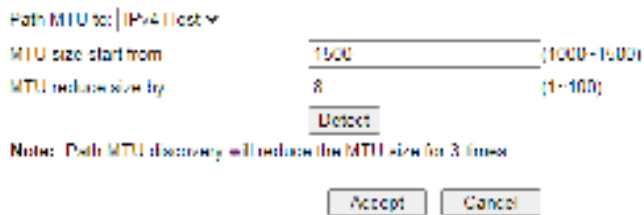
If PPPoE Pass-through for Wired LAN is checked while protocol is PPPoA, the router will behave like a modem which only serves the PPPoE client on the LAN.

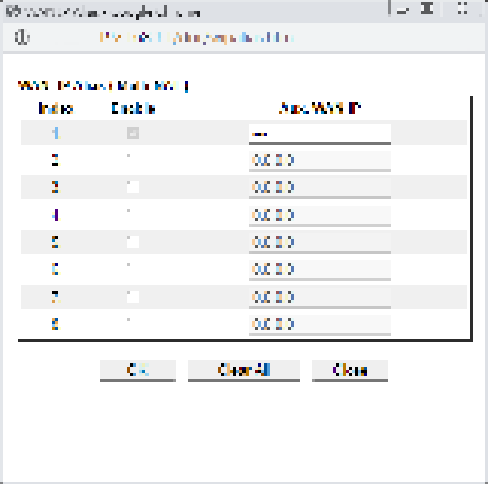
OK

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.
ADSL Modem Settings	Set up the DSL parameters required by your ISP. These settings configured here are specified for ADSL only. Multi-PVC channel - The selections displayed here are determined by the page of WAN >> Multi-PVC/VLAN. Select M-PVCs Channel means no selection will be chosen. VPI - Type in the value provided by ISP. VCI - Type in the value provided by ISP. Encapsulating Type - Drop down the list to choose the type provided by ISP. Protocol - Drop down the list to choose the one (PPPoE or PPPoA) provided by ISP. If you have already used Quick Start Wizard to set the protocol, then it is not necessary for you to change any settings in this group. Modulation -Default setting is Multimode. Choose the one that fits the requirement of your router.
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP.

	Username - Type in the username provided by ISP in this field. Password - Type in the password provided by ISP in this field. More Options - It shows optional settings for configuration. ● Service Name - Enter the description of the specific network service. ● Separate Account for ADSL - In default, WAN1 supports VDSL2/ADSL and uses the same PPPoE account and password for connection. If required, you can configure another account and password for ADSL connection by checking this box. If it is checked, the system will ask you to type another group of account and password additionally.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode - Choose ARP Detect or Ping Detect for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items. ● Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for ping. ● Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for ping. ● With the IP address(es) ping, Vigor router can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation. ● Ping Interval - Type the interval for the system to execute the PING operation. ● Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
MTU	It means Max Transmit Unit for packet. Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path. Click Detect to open the following dialog.  ● Path MTU to - 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.
PPP/MP Setup	PPP Authentication - Select PAP only or PAP/CHAP/MS-CHAP/MS-CHAPv2 for PPP. IP Assignment (IPCP)- Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Fixed IP - Click Yes to use this function and type in a fixed IP address in the box of Fixed IP Address. 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. 
Dial-Out 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 Applications >> Schedule web page and you can use the number that you have set in that web page.
PPPoE Pass-through	The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction. For Wired LAN - If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet. For Wireless LAN - It is available for <i>n</i> model. If you check this box, PCs on the same wireless network can use another set of PPPoE session (different with the Host PC) to access into Internet. 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.
MAC 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. Use the following MAC Address - Type in the MAC address for the router manually.

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

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

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

WAN >> Internet Access

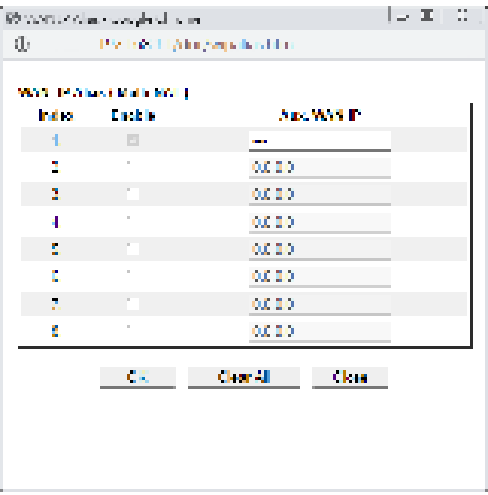
WAN 1

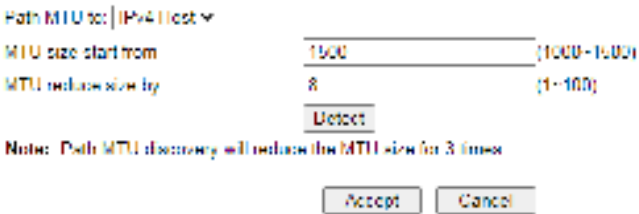
PPPoE / PPPoA	MPoA / Static or Dynamic IP	IPv8
☐ Enable ☒ Disable		
ADSL Modem Settings Multi-PVC channel: Channel 2 Encapsulation: 1482 Unidirectional LLC VPI: 0 VCI: 35 Modulation: Multimode		WAN Connection Detection Mode: ARP Detect
IP Network Settings ☐ Obtain an IP address automatically ☒ Specify an IP address IP Address: Subnet Mask: Gateway IP Address: WAN IP Alias		MTU: 1452 (Max: 1500) Full MTU Discovery RIP Routing ☐ Enable RIP Bridge Mode ☐ Enable Unidirectional Mode ☒ Enable Full Bridge Mode Unidirectional Subnet: LAN 1
DNS Server IP Address Primary Server: 0.0.0.0 Secondary Server: 8.8.4.4		MAC Address ☒ Default MAC Address ☐ Use the following MAC Address 00:1D:AA:15:80:C0

Note:
 1. Full Bridge Mode supports forwarding packets with VLAN tags.
 2. Full Unidirectional Mode doesn't support wireless LAN.

Available settings are explained as follows:

Item	Description
Enable/Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
ADSL Modem Settings	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.
IP Network Settings	This group allows you to obtain an IP address automatically and allows you type in IP address manually. Obtain an IP address automatically - Click this button to obtain the IP address automatically. More Options - It shows optional settings for configuration. ● Router Name - Type in the router name provided by ISP. ● Domain Name - Type in the domain name that you have assigned. DHCP Client Identifier for some ISP - Check the box to specify username and password as the DHCP client identifier for some ISP. ● Username: Type a name as username. The maximum length of the user name you can set is 63 characters. ● Password: Type a password. The maximum length of the password you can set is 62 characters. 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. WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog. 
DNS Server IP Address	Type in the primary IP address for the router. If necessary, type in secondary IP address for necessity in the future.
WAN Connection Detection	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 or Always On for the system to execute for WAN detection. If you choose Ping

	Detect as the detection mode, you have to type required settings for the following items. ● Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation. ● Ping Interval - Type the interval for the system to execute the PING operation. ● Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
MTU	It means Max Transmit Unit for packet. Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path. Click Detect to open the following dialog.  ● Path MTU to - 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.
RIP Routing	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.
Bridge Mode	Enable Bridge Mode - If the function is enabled, the router will work as a bridge modem. Enable 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. ● Bridge Subnet - Make a bridge between the selected LAN subnet and such WAN interface.
MAC 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.

	Use the following MAC Address - Type in the MAC address for the router manually.

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

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

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

WAN >> Internet Access

WAN 1

PPPoE

Static or Dynamic IP

PPTP/L2TP

IPv6

☐ Enable
 ☒ Disable

ISP Access Setup

Username

Max: 63 characters

Password

Max: 62 characters

More Options

WAN Connection Detection

Mode

PPP Detect

MTU

1492

(Max:1500)

Path MTU Discovery

PPPMP Setup

PPP Authentication

PAP/CHAPMS<CHAPMS>CHAPv2

Idle Timeout

180

second(s)

IP Assignment (PUP)

☐ Static
 ☒ Dynamic

Fixed IP Address

WAN IP Alias

Dial-Out Schedule

Index(1-15) in Schedule Setup

→ None

→ None

→ None

→ None

TTL

☒ Change the TTL value

☒ Default MAC Address
 ☐ Use the following MAC Address

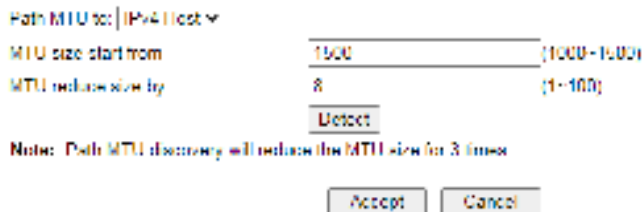
DD : DD : AA : 15 : 80 : CA

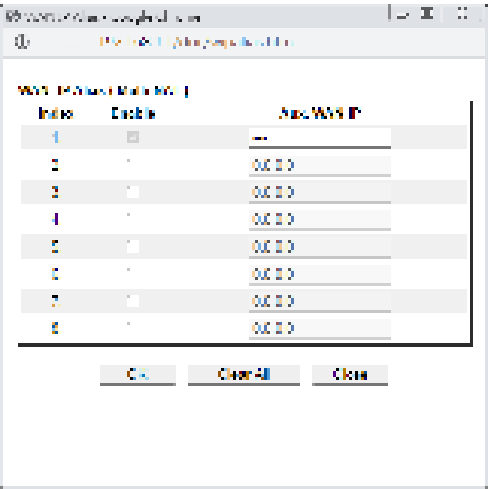
OK

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.
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP. Username - Type in the username provided by ISP in this field. The maximum length of the user name you can set is 63 characters. Password - Type in the password provided by ISP in this field. The maximum length of the password you can set is 62 characters. More Options - It shows optional settings for configuration. Service Name (Optional) - Enter the description of the specific network service.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode - Choose ARP Detect or Ping Detect for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the

	following items. ● Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation. ● Ping Interval - Type the interval for the system to execute the PING operation. ● Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
MTU	It means Max Transmit Unit for packet. Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path. Click Detect to open the following dialog.  ● 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.
PPP/MP Setup	PPP Authentication - Select PAP only or PAP/CHAP/MS-CHAP/MS-CHAPv2 for PPP. Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action. IP Assignment (IPCP) - Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Fixed IP - Click Yes to use this function and type in a fixed IP address in the box of Fixed IP Address. WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other

	than the current one you are using. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog. 
Dial-Out 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.
TTL	Change the TTL value – Enable or disable the TTL (Time to Live) for a packet transmitted through Vigor router. ● Enable - TTL value will be reduced (-1) when it passes through Vigor router. It will cause the client, accessing Internet through Vigor router, to be blocked by certain ISP when TTL value becomes “0”. ● Disable - TTL value will not be reduced. Then, when a packet passes through Vigor router, it will not be cancelled. That is, the client who sends out the packet will not be blocked by ISP. Default MAC Address - You can use Default MAC Address or specify another MAC address by typing on the boxes of MAC Address for the router. Specify a MAC Address – Type the MAC address for the router manually.

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

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

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

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

WAN >> Internet Access

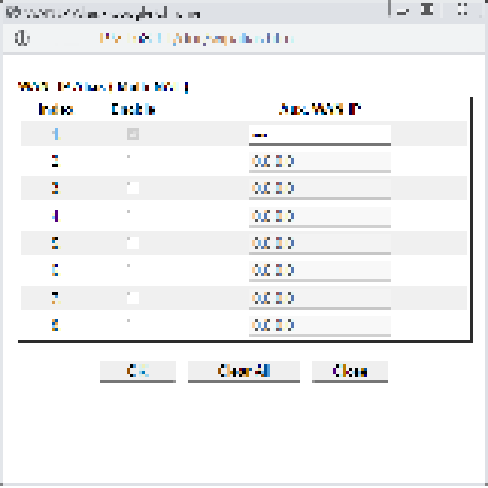
WAN 2

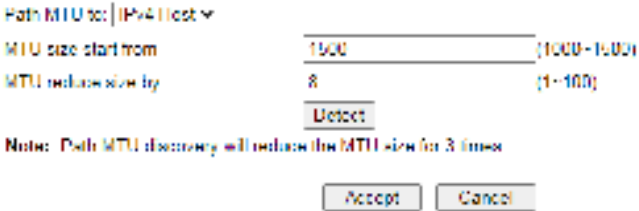
PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
☐ Enable ☒ Disable			
IP Network Settings ☐ Obtain an IP address automatically More Options (+) ☒ Specify an IP address IP Address: _____ Subnet Mask: _____ Gateway IP Address: _____ WAN IP Alias: [button]		Keep WAN Connection ☐ Enable PING to keep alive PING to the IP: _____ PING Interval: 0 minute(s)	
DNS Server IP Address Primary Server: 0.0.0.0 Secondary Server: 8.8.4.4		TTI ☒ Change the TTI value RIP Routing ☐ Enable RIP	
WAN Connection Detection Mode: ARP Detect w/		MAC Address ☒ Default MAC Address ☐ Use the following MAC Address 00 : 10 : AA : 15 : B0 : CA	
MTU 1500 Path MTU Discovery [button]			

[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.
IP Network Settings	This group allows you to obtain an IP address automatically and allows you type in IP address manually. Obtain an IP address automatically - Click this button to obtain the IP address automatically if you want to use Dynamic IP mode. More Options - It shows optional settings for configuration. ● Router Name: Type in the router name provided by ISP. ● Domain Name: Type in the domain name that you have assigned. DHCP Client Identifier for some ISP ● Enable: Check the box to specify username and password as the DHCP client identifier for some ISP. ● Username: Type a name as username. The maximum

	length of the user name you can set is 63 characters. ● Password: Type a password. The maximum length of the password you can set is 62 characters. Specify an IP address - Click this radio button to specify some data if you want to use Static IP mode. ● IP Address: Type the IP address. ● Subnet Mask: Type the subnet mask. ● Gateway IP Address: Type the gateway IP address. 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. 
DNS Server IP Address	Type in the primary IP address for the router if you want to use Static IP mode. If necessary, type in secondary IP address for necessity in the future.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode - Choose ARP Detect or Ping Detect or Always On for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items. ● Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for ping. ● Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for ping. With the IP address(es) ping, Vigor router can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation. ● Ping Interval - Type the interval for the system to execute the PING operation. ● Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
MTU	It means Max Transmit Unit for packet. Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path. Click Detect to open the following dialog.

	 ● Path MTU to - 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.
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.
TTL	Change the TTL value – Enable or disable the TTL (Time to Live) for a packet transmitted through Vigor router. ● Enable - TTL value will be reduced (-1) when it passess through Vigor router. It will cause the client, accessing Internet through Vigor router, be blocked by certain ISP when TTL value becomes “0”. ● Disable - TTL value will not be reduced. Then, when a packet passes through Vigor router, it will not be cancelled. That is, the client who sends out the packet will not be blocked by ISP.
RIP Routing	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.
MAC Address:	Default MAC Address: Click this radio button to use default MAC address for the router. Specify a MAC Address: Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the Specify a MAC Address and enter the MAC address in the MAC Address field.

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

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

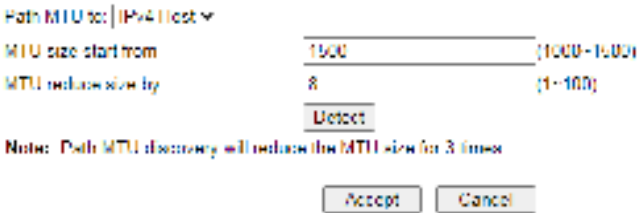
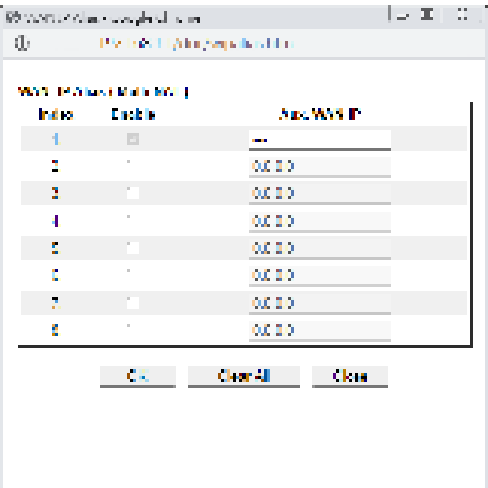
To use **PPTP/L2TP** as the accessing protocol of the internet, please click the **PPTP/L2TP** tab.
The following web page will be shown.

WAN :- Internet Access

[illegible]

Available settings are explained as follows:

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

	 ● 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.
PPP Setup	PPP Authentication - Select PAP only or PAP/CHAP/MS-CHAP/MS-CHAPv2 for PPP. Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action.
IP Address Assignment Method(IPCP)	WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.  Fixed IP - Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Click Yes to use this function and type in a fixed IP address in the box. Fixed IP Address -Type a fixed IP address.
WAN IP Network Settings	Obtain an IP address automatically - Click this button to obtain the IP address automatically. Specify an IP address - Click this radio button to specify

	some data. ● IP Address - Type the IP address. ● Subnet Mask - Type the subnet mask.

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

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

To use **3G/4G USB Modem (PPP mode)** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **3G/4G USB Modem (PPP mode)** for WAN5. The following web page will be shown.

WAN => Internet Access ?

WAN 1

3G/4G USB Modem(PPP mode) | 3G/4G USB Modem(DHCP mode) | IPv8

| Modem Support List |

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

SIM PIN code

Modem Init1 String
(Default: AT&I=LIVTX180280190=0)

APN Name Apply

Modem Init1 String2

Modem Init1 String
(Default: ATDT1999, COMMA: ATDT1999, ID: 3COMMA: ATDT199919)

Service Name (Optional)

PPP Username (Optional)

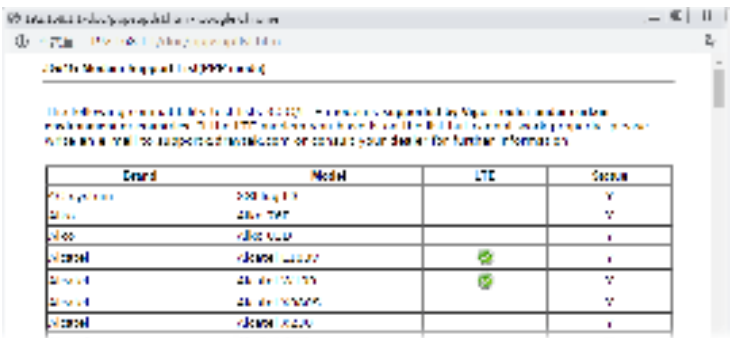
PPP Password (Optional)

PPP Authentication

Schedule Profile

WAN Connection Detection
 Mode

Available settings are explained as follows:

Item	Description
Modem Support List	It lists all of the modems supported by such router. 
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.
Schedule Profile	You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode - Choose PPP Detect or Ping Detect for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items. ● Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● TTL (Time to Live) - Set TTL value of PING operation. ● Ping Interval - 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-1-2-7 Details Page for 3G/4G USB Modem (DHCP mode) in USB WAN

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

WAN => Internet Access

WAN 3

☒ Enable
 ☐ Disable

SIM PIN code:

Network Mode: (Default: 4G/3G/2G)

APN Name:

LTL software version:

LTL firmware version:

WAN Connection Detection Mode:

Schedule Profile:

->

=> =>

MTU: (Default: 1500)

Push MTU Discovery:

Authentication:

Username: (Optional)

Password: (Optional)

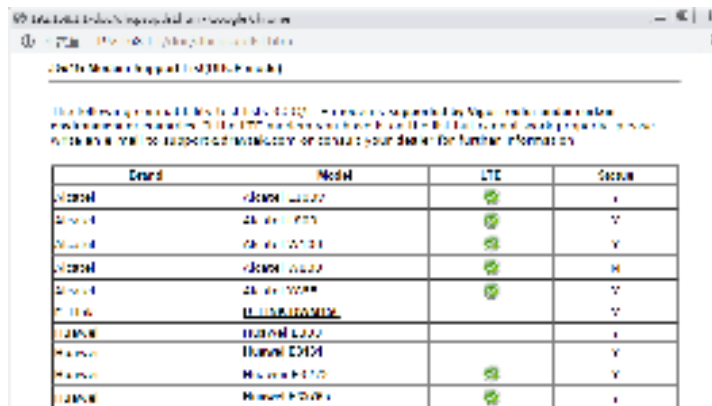
[Modem Support List](#)

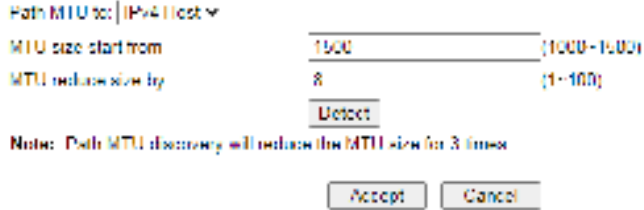
Note:

1. Please note that in some cases USB port connection will be terminated temporarily to activate the new configuration.
2. VPN feature may be affected when the value of MTU is changed, please also check your value of VPN mss by using "VPN mss set" command.

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

Available settings are explained as follows:

Item	Description																																												
Modem Support List	It lists all of the modems supported by such router.  The screenshot shows a web browser displaying the "Modem Support List" page. The page title is "Modem Support List". Below the title, there is a message stating: "The following are the modems supported by this router. If you have a modem that is not listed here, please contact your ISP or the manufacturer of the modem for further information." Below this message is a table with four columns: Brand, Model, LTE, and Status. <table><thead><tr><th>Brand</th><th>Model</th><th>LTE</th><th>Status</th></tr></thead><tbody><tr><td>Huawei</td><td>Huawei E3376</td><td></td><td>x</td></tr><tr><td>Huawei</td><td>Huawei E3377</td><td></td><td>y</td></tr><tr><td>Huawei</td><td>Huawei E3378</td><td></td><td>y</td></tr><tr><td>Huawei</td><td>Huawei E3379</td><td></td><td>x</td></tr><tr><td>Huawei</td><td>Huawei E3380</td><td></td><td>y</td></tr><tr><td>Huawei</td><td>Huawei E3381</td><td></td><td>y</td></tr><tr><td>Huawei</td><td>Huawei E3382</td><td></td><td>x</td></tr><tr><td>Huawei</td><td>Huawei E3383</td><td></td><td>y</td></tr><tr><td>Huawei</td><td>Huawei E3384</td><td></td><td>y</td></tr><tr><td>Huawei</td><td>Huawei E3385</td><td></td><td>x</td></tr></tbody></table>	Brand	Model	LTE	Status	Huawei	Huawei E3376		x	Huawei	Huawei E3377		y	Huawei	Huawei E3378		y	Huawei	Huawei E3379		x	Huawei	Huawei E3380		y	Huawei	Huawei E3381		y	Huawei	Huawei E3382		x	Huawei	Huawei E3383		y	Huawei	Huawei E3384		y	Huawei	Huawei E3385		x
Brand	Model	LTE	Status																																										
Huawei	Huawei E3376		x																																										
Huawei	Huawei E3377		y																																										
Huawei	Huawei E3378		y																																										
Huawei	Huawei E3379		x																																										
Huawei	Huawei E3380		y																																										
Huawei	Huawei E3381		y																																										
Huawei	Huawei E3382		x																																										
Huawei	Huawei E3383		y																																										
Huawei	Huawei E3384		y																																										
Huawei	Huawei E3385		x																																										
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 or Strict ARP Detect for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items. ● 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.
Schedule Profile	You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page
MTU	It means Max Transmit Unit for packet. Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path. Click Choose IP to open the following dialog.  ● 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.
Authentication	Select PAP only or PAP or CHAP for PPP authentication. Username - Type the username for authentication (optional). Password - Type the password for authentication (optional).

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

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

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

II-1-2-9 Details Page for IPv6 – PPP in WAN1/WAN2

During the procedure of IPv4 PPPoE connection, we can get the IPv6 Link Local Address between the gateway and Vigor router through IPv6CP. Later, use DHCPv6 or accept RA to acquire the IPv6 prefix address (such as: 2001:B010:7300:200::/64) offered by the ISP. In addition, PCs under LAN also can have the public IPv6 address for Internet access by means of the generated prefix.

No need to type any other information for PPP mode.

WAN >> Internet Access ?

WAN 1

PPPoE / PPPoA	MPoA / Static or Dynamic IP	IPv6
Internet Access Mode Connection Type: PPP ▼		
WAN Connection Detection Mode: Ping Detect ▼ Ping IP/Hostname: TTL (255/Unset): 0 RIPng Protocol ☐ Enable		

Note:
IPv6 WAN setting should be PPPoE / PPPoA client

OK
Cancel

Available settings are explained as follows:

Item	Description
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. Mode - Choose Always On or Ping Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always. ● Ping IP/Hostname - If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. ● TTL (Time to Live) -If you choose Ping Detect as detection mode, you have to type TTL value.
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					
2001:8010:7300:201:21D:AFF:FEA6:2568/64 (Global)					
FE80::21D:AFF:FEA6:2568/64 (Link)					
TX Packets		RX Packets		TX Bytes	
7		4		690	
				RX Bytes	
				329	
WAN2 IPv6 Status					
>> Drop PPP					
Enable		Mode		Up Time	
Yes		PPP		0:02:08	
IP		Gateway IP			
2001:8010:7300:201:21D:AFF:FEA6:256A/128 (Global)		FE80::90:1A00:242:AD52			
FE80::10:AFF:FEA6:256A/128 (Link)					
DNS IP					
2001:8000:168::1					
2001:8000:168::2					
TX Packets		RX Packets		TX Bytes	
7		9		544	
				RX Bytes	
				1126	



Info

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

II-1-2-10 Details Page for IPv6 – TSPC in WAN1/WAN2/WAN3

Tunnel setup protocol client (TSPC) is an application which could help you to connect to IPv6 network easily.

Please make sure your IPv4 WAN connection is OK and apply one free account from hexago (<http://gogonet.gogo6.com/page/freenet6-account>) before you try to use TSPC for network connection. TSPC would connect to tunnel broker and requests a tunnel according to the specifications inside the configuration file. It gets a public IPv6 IP address and an IPv6 prefix from the tunnel broker and then monitors the state of the tunnel in background.

After getting the IPv6 prefix and starting router advertisement daemon (RADVD), the PC behind this router can directly connect to IPv6 the Internet.

WAN => Internet Access ?

WAN 1

PPPoE / PPPoA	MPoA / Static or Dynamic IP	IPv6
Internet Access Mode		
Connection Type		TSPC
TSPC Configuration		
Username		Max: 63 characters
Password		Max: 19 characters
Tunnel Broker		
WAN Connection Detection		
Mode		Ping Detect
Ping IP/Hostname		
TTL (1-255, 0=Auto)		0

OK Cancel

Available settings are explained as follows:

Item	Description
Username	Type the name obtained from the broker. It is suggested for you to apply another username and password for http://gogonet.gogo6.com/page/freenet6-account . The maximum length of the name you can set is 63 characters.
Password	Type the password assigned with the user name. The maximum length of the name you can set is 19 characters.
Tunnel Broker	Type the address for the tunnel broker IP, FQDN or an optional port number.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. Mode - Choose Always On or Ping Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always. ● Ping IP/Hostname - If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. ● TTL (Time to Live) -If you choose Ping Detect as

detection mode, you have to type TTL value.

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

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

WAN >> Internet Access

WAN 1

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

Internet Access Mode

Connection Type: AICCU

AICCU Configuration

☐ Always On

Username: Max: 63 characters

Password: Max: 63 characters

Tunnel Broker: to.sixxs.net

Tunnel ID:

Subnet Prefix:

WAN Connection Detection

Mode: Ping Detect

Ping IP/Hostname:

TTL (1-255/Auto): 0

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

OK Cancel

Available settings are explained as follows:

Item	Description
Always On	Check this box to keep the network connection always.
Username	Type the name obtained from the broker. Please apply new account at http://www.sixxs.net/ . It is suggested for you to apply another username and password. 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-1-2-12 Details Page for IPv6 – DHCPv6 Client in WAN1/WAN2

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

WAN >> Internet Access



WAN 1

PPPoE / PPPoA MPoA / Static or Dynamic IP IPv6

Internet Access Mode

Connection Type: DHCPv6 Client

DHCPv6 Client Configuration

IAID (Identity Association ID): 1352172774

DUID (DHCP Unique ID): 0000001001das150dc9

Authentication Protocol: None

WAN Connection Detection

Mode: Ping Detect

Ping IP/Hostname:

TTL (1-255, 0 Auto): 0

RIPng Protocol

☐ Enable

Bridge Mode

☐ Enable Bridge Mode

☐ Enable Firewall

Bridge Subnet: LAN 1

OK Cancel

Available settings are explained as follows:

Item	Description
IAID	Type a number as IAID.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through NS Detect or Ping Detect. Mode - Choose Always On, Ping Detect or NS Detect for the system to execute for WAN detection. With NS Detect mode, the system will check if network connection is established or not, like IPv4 ARP Detect. Always On means no detection will be executed. The network connection will be on always. ● Ping IP/Hostname - If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. ● TTL (Time to Live) -If you choose Ping Detect as detection mode, you have to type TTL value.
RIPng Protocol	RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.
Bridge Mode	Enable Bridge Mode - If the function is enabled, the router will work as a bridge modem. Enable Firewall - It is available when Bridge Mode is enabled. When both Bridge Mode and Firewall check boxes are enabled, the settings configured (user profiles) under User Management will be ignored. And all of the filter rules defined and enabled in Firewall menu will be activated. Bridge Subnet - Make a bridge between the selected LAN

subnet and such WAN interface.

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

II-1-2-13 Details Page for IPv6 – Static IPv6 in in WAN1/WAN2

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

WAN >> Internet Access ?

WAN 1

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

Internet Access Mode
Connection Type: Static IPv6

Static IPv6 Address Configuration
IPv6 Address: / 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): 0

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 Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. Mode - Choose Always On or Ping Detect or NS Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always. ● Ping IP/Hostname - If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. ● TTL (Time to Live) -If you choose Ping Detect as detection mode, you have to type TTL value.
RIPng Protocol	RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.
Bridge Mode	Enable Bridge Mode - If the function is enabled, the router will work as a bridge modem. Enable Firewall - It is available when Bridge Mode is enabled. When both Bridge Mode and Firewall check boxes are enabled, the settings configured (user profiles) under User Management will be ignored. And all of the filter rules defined and enabled in Firewall menu will be activated. Bridge Subnet - Make a bridge between the selected LAN subnet and such WAN interface.

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

II-1-2-14 Details Page for IPv6 – 6in4 Static Tunnel in WAN1 / WAN2

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

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

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

WAN >> Internet Access ?

WAN 1

PPPoE / PPPoA MPoA / Static or Dynamic IP IPv6

Internet Access Mode

Connection Type: 6in4 Static Tunnel

6in4 Static Tunnel

Remote Endpoint IPv4 Address:

Fixed IPv6 Address: / 64 (default: 64)

LAN Routed Prefix: / 64 (default: 64)

Tunnel TTL: 255 (default: 255)

WAN Connection Detection

Mode: Ping Detect

Ping IP/hostname:

TTL (1-255 or Auto): 0

OK Cancel

Available settings are explained as follows:

Item	Description
Remote Endpoint IPv4 Address	Type the static IPv4 address for the remote server.
6in4 IPv6 Address	Type the static IPv6 address for IPv4 tunnel with the value for prefix length.
LAN Routed Prefix	Type the static IPv6 address for LAN routing with the value for prefix length.
Tunnel TTL	Type the number for the data lifetime in tunnel.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. Mode - Choose Always On or Ping Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always. ● Ping IP/Hostname - If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. ● TTL (Time to Live) -If you choose Ping Detect as detection mode, you have to type TTL value.

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

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

Online Status

Physical Connection

System Uptime: 0day 0:4:18

IPv4		IPv6	
LAN Status			
IP Address			
2001:4000:FF10:8314::2113:AA1F::1104/64 (Global)			
FE80::2113:AA1F::1104/64 (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
2001:4000:FF10:8314::2113/64 (Global)			:::0
FE80::30A8:651D/128 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
3	26	211	2302

II-1-2-15 Details Page for IPv6 – 6rd in WAN1 / WAN2

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

WAN => Internet Access



WAN 1

PPPoE / PPPoA	MPoA / Static or Dynamic IP	IPv6
Internet Access Mode		
Connection Type		6rd
6rd Settings		
6rd Mode		☐ Auto 6rd ☒ Static 6rd
Static 6rd Settings		
IPv4 Border Relay		
IPv4 Mask Length		0
6rd Prefix		
6rd Prefix Length		0
WAN Connection Detection		
Mode		Ping Detect w
Ping IP/hostname		
TTL (1-255.0 Auto)		0

OK

Cancel

Available settings are explained as follows:

Item	Description
6rd Mode	Auto 6rd – Retrieve 6rd prefix automatically from 6rd service provider. The IPv4 WAN must be set as "DHCP". Static 6rd - Set 6rd options manually.
IPv4 Border Relay	Type the IPv4 addresses of the 6rd Border Relay for a given 6rd domain.
IPv4 Mask Length	Type a number of high-order bits that are identical across all CE IPv4 addresses within a given 6rd domain. It may be any value between 0 and 32.
6rd Prefix	Type the 6rd IPv6 address.
6rd Prefix Length	Type the IPv6 prefix length for the 6rd IPv6 prefix in number of bits.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. Mode - Choose Always On or Ping Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always. ● Ping IP/Hostname - If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. ● TTL (Time to Live) -If you choose Ping Detect as detection mode, you have to type TTL value.

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

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

Online Status

Physical Connection

System Uptime: 0day 0:9:16

IPv4		IPv6	
LAN Status			
IP Address			
2001:E41:A065:1D00:21D:AAFF:FE03:11B4/64 (Global)			
FE80::21D:AAFF:FE03:11B4/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
15	113	1351	18040
WAN1 IPv6 Status			
Enable	Mode	Up Time	
Yes	6rd	0:09:06	
IP			Gateway IP
2001:E41:A065:1D01:21D:AAFF:FE03:11B5/128 (Global)			---
FE80::C0A0:651D/128 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
13	29	967	2620

II-1-3 Multi-PVC/VLAN

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

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

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

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

General

Channel	Enable	WAN type	VPI/VCI	ATM QoS	Multi-PVC Bridging	Virtual WAN Bridging	Virtual WAN Port
1	☒	ADSL	8/35	None	☒		
2	☒	Ethernet		None	☒		
3	☒	USB1		None	☒		
4	☐	ADSL	8/35	None	☐	☐	☐
5	☐	Ethernet		None	☐	☐	☐
6	☐	USB1		None	☐	☐	☐
7	☐	ADSL	8/35	None	☐	☐	☐
8	☐	Ethernet		None	☐	☐	☐
9	☐	USB1		None	☐	☐	☐
10	☐	ADSL	8/35	None	☐	☐	☐

Note:
Channel 1 to 4 are reserved for the default use.

OK Cancel

Available settings are explained as follows:

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

To configure a PVC channel, click its channel number.

WAN links for Channel 4, 5 and 6 are provided for router-borne application such as **TR-069**. The settings must be applied and obtained from your ISP. For your special request, please contact with your ISP and then click WAN link of Channel 5, 6 or 7 to configure your router.

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

Available settings are explained as follows:

Item	Description
Enable Channel 4/5/6	Enable - Select to enable this channel. Disable - Select to disable this channel.
WAN Type	Specify a WAN type of the PVC Channel/VLAN. ADSL - A PVC Channel will be created using an ADSL connection on WAN1.

	VDSL- A VLAN will be created using a VDSL connection on WAN1. Ethernet (WAN2) - A VLAN will be created on WAN2.
General Settings	VPI - (Available when WAN Type is ADSL) Virtual Path Identifier. Contact your ISP or carrier for the appropriate value. VCI - (Available when WAN Type is ADSL) Virtual Channel Identifier. Contact your ISP or carrier for the appropriate value. Protocol - (Available when WAN Type is ADSL) Access protocol used for the ADSL connection. Contact your ISP or carrier for the appropriate setting. ● PPPoA- Point-to-Point over ATM. ● PPPoE- Point-to-Point over Ethernet. ● MPoA- Multiprotocol over ATM. Encapsulation - (Available when WAN Type is ADSL) Encapsulation mode used for the ASDL connection. Contact your ISP or carrier for the appropriate setting. ● VC MUX- Virtual Circuit Multiplexing. ● LLC/SNAP- Logical Link Control/Subnetwork Access Protocol. Add VLAN Header - (Available when WAN type is ADSL) If selected, enable VLAN tagging on this PVC. ● VLAN Tag - Enter the value as the VLAN ID number. Valid settings are in the range from 1 to 4095. The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value. ● Priority - Choose the number to determine the packet priority for such VLAN. The range is from 0 to 7.
ATM QoS	Configures the Quality of Service (QoS) of the ATM circuit. QoS Type - Select a proper QoS type for the channel. ● UBR - Unspecified Bit Rate. ● CBR - Constant Bit Rate. ● ABR - Available Bit Rate. ● nrtVBR - Non-real-time Variable Bit Rate. ● rtVBR - Real-time Variable Bit Rate. Enter the values for PCR(Peak Cell Rate), SCR(Sustainable Cell Rate) and MBS(Maximum Burst Size) respectively.
Open Port-based Bridge Connection for this Channel	If selected, bridge this channel to one or more LAN ports. Physical Members - If selected, a channel is bridged to this LAN port. Wireless LAN - If selected, a channel is bridged to the wireless clients using the SSID. Note: LAN port P1 is reserved for NAT use and cannot be selected for bridging.
Open WAN Interface for this Channel	Check the box to enable relating function. WAN Application – ● Management - It can be specified for general management (Web configuration/telnet/TR069). If you choose Management, the configuration for this VLAN

	will be effective for Web configuration/telnet/TR069. ● IPTV - The IPTV configuration will allow the WAN interface to send IGMP packets to IPTV servers. ● VoIP - The VoIP configuration will allow the WAN interface created here to send SIP registration packets and other VoIP management packets.
WAN Connection Detection	Such function is available only when ADSL is selected as WAN Type. It allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode - Choose ARP Detect or Ping Detect for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items. ● Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. ● With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation. ● Ping Interval - Type the interval for the system to execute the PING operation. ● Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
PPPoE/PPPoA Client ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP. ISP Name - PPP Service Name. Enter if your ISP requires this setting; otherwise leave blank. Username - Name provided by the ISP for PPPoE/PPPoA authentication. Maximum length is 62 characters. Password - Password provided by the ISP for PPPoE/PPPoA authentication. Maximum length is 62 characters. ● PPP Authentication - The protocol used for PPP authentication. ● PAP only - Only PAP (Password Authentication Protocol) is used. ● PAP or CHAP - Both PAP and CHAP (Challenge-Handshake Authentication Protocol) can be used for PPP authentication. Router negotiates with the PPTP or L2TP server to determine which protocol to use. Always On - If selected, the router will maintain the PPPoE/PPPoA connection. Idle Timeout - Maximum length of time, in seconds, of idling allowed (no traffic) before the connection is dropped. ISP Address from ISP - Specifies how the WAN IP address of the channel configured. ● Fixed IP Yes - IP address entered in the Fixed IP Address field

	will be used as the IP address of the virtual WAN. No - Virtual WAN IP address will be assigned by the ISP's PPPoE/PPPoA server.
MPoA	Obtain an IP address automatically - Select this option if the router is to receive IP configuration information from a DHCP server. ● Router Name - Sets the value of DHCP Option 12, which is used by some ISPs. ● Domain Name - Sets the value of DHCP Option 15, which is used by some ISPs. Specify an IP address - Select this option to manually enter the IP address. ● IP Address - Type in the IP address. ● Subnet Mask - Type in the subnet mask. ● Gateway IP Address - Type in gateway IP address. DNS Server IP Address - Type in the primary IP address for the router if you want to use Static IP mode. If necessary, type in secondary IP address for necessity in the future.

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

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

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

☒ **Enable Channel 7:**

WAN Type: VDSL

General Settings

VLAN Header

VLAN tag: 0

Priority: 0

Note: Tag value must be set between 1~4095 and unique for each channel.
Only one channel can be untagged (equal to 0) at a time.

Bridge mode

☐ **Enable**

Physical Members

☐ P1 ☐ P2 ☐ P3 ☐ P4

Wireless LAN(2.4GHz)

☐ SSID1 ☐ SSID2 ☐ SSID3 ☐ SSID4

Wireless LAN(5GHz)

☐ SSID1 ☐ SSID2 ☐ SSID3 ☐ SSID4

Notes:

1. P1 is reserved for WAN use, and cannot be configured for bridge mode.
2. If the port be configured for bridge mode, the setting of the port in LAN or WLAN Configuration will not work.

OK Cancel

Available settings are explained as follows:

Item	Description
Enable Channel 7~10	Enable - Select to enable this channel. Disable - Select to disable this channel.
WAN Type	Specify a WAN type of the PVC Channel/VLAN. ADSL - A PVC Channel will be created using an ADSL connection on WAN1. VDSL - A VLAN will be created using a VDSL connection on WAN1. Ethernet (WAN2) - A VLAN will be created on WAN2.
General Settings	VPI - (Available when WAN Type is ADSL) Virtual Path Identifier. Contact your ISP or carrier for the appropriate value. VCI - (Available when WAN Type is ADSL) Virtual Channel Identifier. Contact your ISP or carrier for the appropriate value. Protocol - (Available when WAN Type is ADSL) Access protocol used for the ADSL connection. Contact your ISP or

	carrier for the appropriate setting. ● PPPoA- Point-to-Point over ATM. ● PPPoE- Point-to-Point over Ethernet. ● MPoA- Multiprotocol over ATM. Encapsulation - (Available when WAN Type is ADSL) Encapsulation mode used for the ADSL connection. Contact your ISP or carrier for the appropriate setting. ● VC MUX- Virtual Circuit Multiplexing. ● LLC/SNAP- Logical Link Control/Subnetwork Access Protocol. Add VLAN Header - (Available when WAN type is ADSL) If selected, enable VLAN tagging on this PVC. ● VLAN Tag - Enter the value as the VLAN ID number. Valid settings are in the range from 1 to 4095. The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value. ● Priority - Choose the number to determine the packet priority for such VLAN. The range is from 0 to 7.
ATM OoS	Configures the Quality of Service (QoS) of the ATM circuit. QoS Type - Select a proper QoS type for the channel. ● UBR - Unspecified Bit Rate. ● CBR - Constant Bit Rate. ● ABR - Available Bit Rate. ● nrtVBR - Non-real-time Variable Bit Rate. ● rtVBR - Real-time Variable Bit Rate. Enter the values for PCR(Peak Cell Rate), SCR(Sustainable Cell Rate) and MBS(Maximum Burst Size) respectively.
Bridge mode	Enable –Click it to enable Bridge mode for such channel. Physical Members –Group the physical ports by checking the corresponding check box(es) for applying the bridge connection.
Bridge mode	If selected, bridge this channel to one or more LAN ports. Physical Members - If selected, a channel is bridged to this LAN port. Wireless LAN - If selected, a channel is bridged to the wireless clients using the SSID. Note: LAN port P1 is reserved for NAT use and cannot be selected for bridging.

Advanced

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

The screenshot shows the 'Advanced' configuration page for a PVC channel. The page has a title bar with 'PVC Channel' and a 'Help' icon. Below the title bar, there are two tabs: 'Channel' and 'Advanced'. The 'Advanced' tab is selected. The main content area contains a table with the following columns: Channel, QoS Type, PCR, SCR, MBS, and PVC to PVC Binding. There are 8 rows for channels 1 through 8. Channel 3 is reserved for WAN 3 (USB) and is not configurable. Below the table, there are buttons for 'OK' and 'Cancel'.

Channel	QoS Type	PCR	SCR	MBS	PVC to PVC Binding
1	UBR	0	0	0	WAN 3 (USB)
2	UBR	0	0	0	WAN 3 (USB)
3	UBR	0	0	0	WAN 3 (USB)
4	UBR	0	0	0	WAN 3 (USB)
5	UBR	0	0	0	WAN 3 (USB)
6	UBR	0	0	0	WAN 3 (USB)
7	UBR	0	0	0	WAN 3 (USB)
8	UBR	0	0	0	WAN 3 (USB)

Below the table, there are buttons for 'OK' and 'Cancel'.

Available settings are explained as follows:

Item	Description
Channel	The channel number. Channels 3 is reserved for the WAN 3 (USB), and is not configurable.
QoS Type	Select a proper QoS type for the channel according to the information that your ISP provides. UBR- Unspecified Bit Rate. CBR- Constant Bit Rate. ABR- Available Bit Rate. nrtVBR-Non-real-time Variable Bit Rate. rtVBR- Real-time Variable Bit Rate.
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	If you wish to have this PVC channel use the same ADSL connection settings of another PVC channel, select that channel from the dropdown box.

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.

The WAN Budget feature allows you to conveniently keep track of Internet traffic volume. You can:

- set up calendar cycles to monitor;
- limit your Internet usage according to your ISP's quota;
- set up action(s) to take when the quota is exceeded.

II-1-4-1 General Setup

WAN >> WAN Budget 

General Setup			Status		
Index	Enable	Quota	When quota exceeded	Time cycle	Duration
WAN1	☐	100MB/200MB			00:00:00-00:00:00
WAN2	☐	100MB/200MB			00:00:00-00:00:00
WAN3	☐	100MB/200MB			00:00:00-00:00:00

Notes:

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 L3/WAN interfaces may be slightly inaccurate.

Item	Description
Index	The WAN port. Click to configure WAN Budget for a particular WAN.
Enable	v - WAN Budget is enabled on this WAN. x - WAN Budget is disabled on this WAN.
Quota	The current cycle's Internet usage is expressed as x/y where x is the cumulative usage and y is the upper limit. For example, 100MB/200MB means the usage thus far in this cycle is 100MB, and the upper limit is 200MB.
When quota exceeded	Actions to be taken once the quota is reached. Shutdown - WAN will be disabled. Mail Alert - Email will be sent to the administrator.
Time cycle	Reset frequency of the usage data. Monthly - The Monthly option in the Criterion and Action tab was used to set up the usage quota. User Defined : The User Defined option in the Criterion and Action tab was used to set up the usage quota.
Duration	Start and end timestamps of the current cycle.

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

WAN => WAN Budget

WAN 1

☒ Enable

Criterion and Action

Quota Limit MB

When quota exceeded

☐ Shutdown WAN interface
☒ Using Notification Object
☐ Set Mail Alert or SMS message

☒ Monthly
 ☐ Custom

☐ Use Cycle in hours
☒ Use Cycle in days

Usage counter resets at the beginning of each cycle.

Cycle duration days

Today is day in the cycle and data quota resets at

Notes:

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 55% and 100% of quota.

Available settings are explained as follows:

Item	Description
Enable	When selected, WAN Budget is enabled for this WAN.
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 object. ● Set Mail Alert - The system will send out a warning message to the administrator when the quota is running out. However, the connection charges will be calculated continuously. ● Set SMS message - The system will send out SMS message to the administrator when the quota is running out.
Monthly	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. ☒ Monthly ☐ Custom Select the day of a month when your (cellular) data resets. Data quota resets on day 1 at 00:00 Data quota resets on day ... - You can determine the starting day in one month.
Custom	This setting allows the user to define the billing cycle according to his request. The WAN budget will be reset with an interval of billing cycle.

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.

Use Cycle in hours -

Monthly	Custom

☒ Use Cycle in hours

☐ Use Cycle in days

Usage counter resets at the beginning of each cycle.

Cycle duration : days and hours

Today is day in the cycle.

- **Cycle duration:** Specify the days and hours to reset the traffic record. For example, 7 means the whole cycle is 7 days; 20 means the whole cycle is 20 days. When the time is up, the router will reset the traffic record automatically.
- **Today is day -** Specify the day in the cycle as the starting point which Vigor router will reset the traffic record. For example, "3" means the third day of the cycle duration.

Use Cycle in days -

Monthly	Custom

☐ Use Cycle in hours

☒ Use Cycle in days

Usage counter resets at the beginning of each cycle.

Cycle duration : days.

Today is day in the cycle and data quota resets at

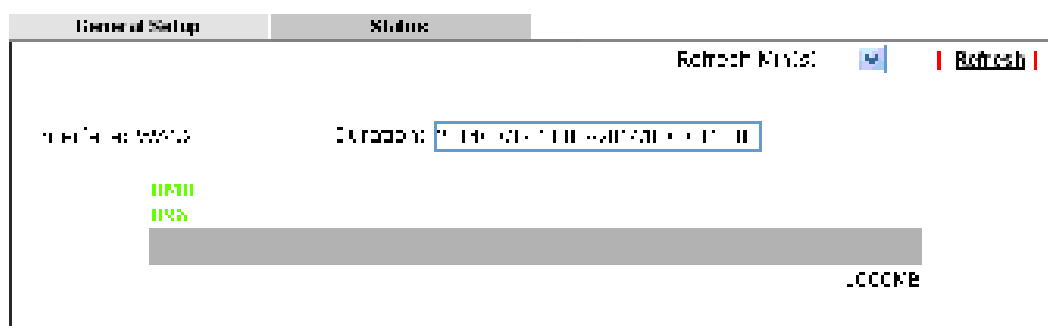
- **Cycle duration:** Specify the days to reset the traffic record. For example, 7 means the whole cycle is 7 days; 20 means the whole cycle is 20 days. When the time is up, the router will reset the traffic record automatically.
- **Today is day -** Specify the day and time for data quota rest in the cycle as the starting point which Vigor router will reset the traffic record. For example, "3" means the third day of the cycle duration.

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

II-1-4-2 Status

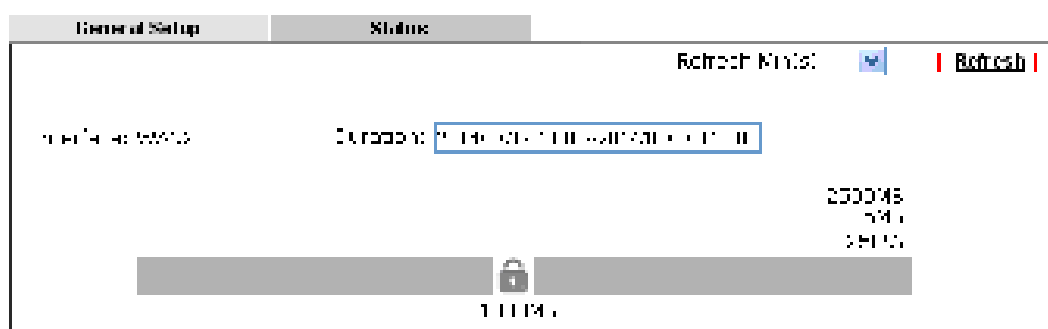
The status page displays the status WAN budget, including the duration and the usage.

WAN >> WAN Budget



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

WAN >> WAN Budget



Application Notes

A-1 How to 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)
118.166.103.153	168.95.192.1	79	3	81	9

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

WAN >> Internet Access

Index	Display Name	Physical Mode	Access Mode	
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	PPPoE / PPPoA	IPv6
Internet Access Mode			
Connection Type			
Offline PPPoE TRIP ACCU UICPv6 Client Static IPv6 IPv4 Static Tunnel 6rd			
OK			

4. 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 2406:8000:4008:C04::66/123 (Global) FE80::21D:4008:FE04::47A2/64 (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		
2406:8000:4008:C04::66/123 (Global)	2406:8000:4008:C04::66		
2406:8000:4008:C04::66/123 (Global)			
FE80::21D:4008:FE04::47A2/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
5180	2612	445044	224316

5. 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: Unspecified ▾

Ping IPv6 Address:

Run

Result | [Clear](#) |

Pinging [ipv6.google.com](https://www.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			
☐ 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		manav@	
Password		*****	
Tunnel Broker		192.168.1.100	
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

Static or Dynamic IP

Internet Access Mode

Connection Type: Static IPv6

Static IPv6 Address Configuration

IPv6 Address: 2406:4000:71::71 / Prefix Length: 123

Add 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

Static or Dynamic IP

Internet Access Mode

Connection Type: Static IPv6

Static IPv6 Address Configuration

IPv6 Address: / Prefix Length: / Add Delete

Current IPv6 Address Table

Index	IPv6 Address/Prefix Length	Scope
1	2406:4000:71::71/123	Global
2	FE80::21D:AAFF:FECE:2DD2/64	Link

Static IPv6 Gateway configuration

IPv6 Gateway Address: 2406:4000:1::9LA:1

WAN Connection Detection

Mode: Always On

Bridge Mode

Enable Bridge Mode

Bridge Subnet: LAN 1

OK Cancel

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 ?

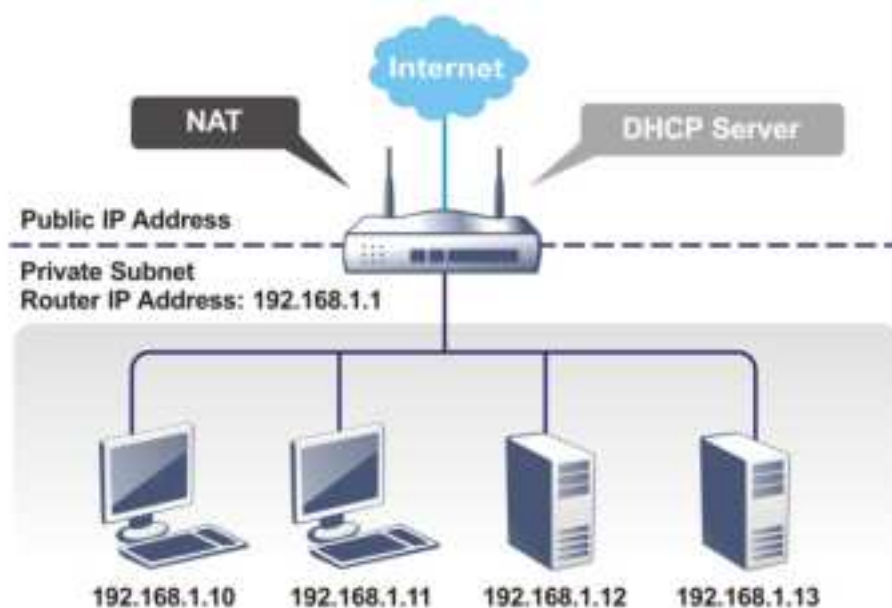
WAN 2

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
Internet Access Mode			
Connection Type 6in4 Static Tunnel			
6in4 Static Tunnel			
Remote Endpoint IPv4 Address 203.114.211.6			
6in4 IPv6 Address 3001::6:1008:2 / 64 (default: 64)			
LAN Routed Prefix 3001::6:1008:1 / 64 (default: 64)			
Tunnel TTL 255 (default: 255)			
WAN Connection Detection			
Mode Always On			

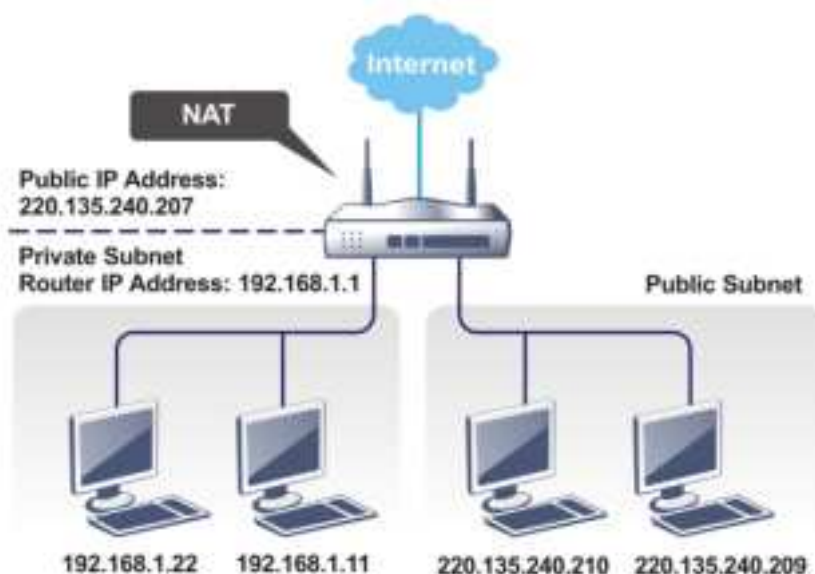
II-2 LAN

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)

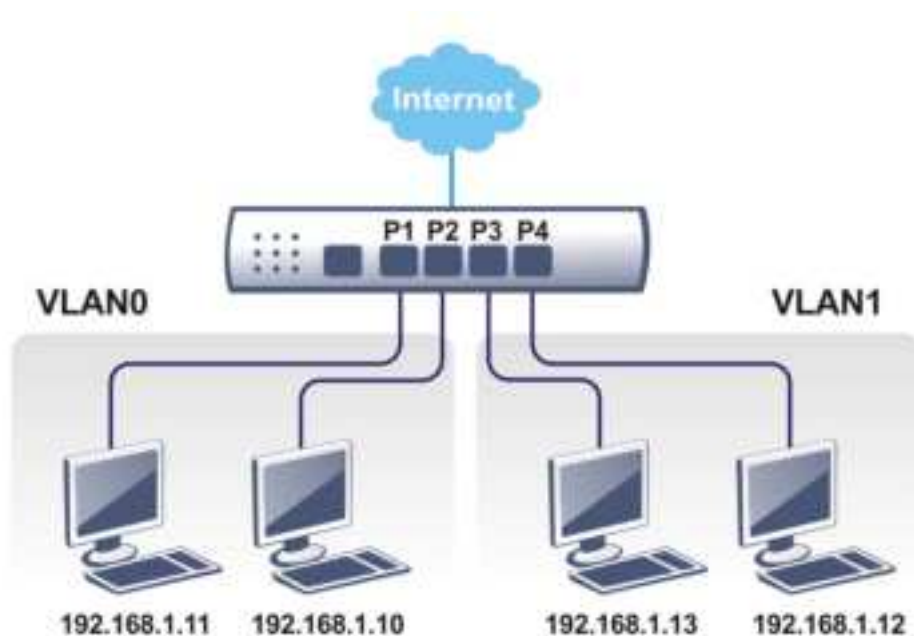
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

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

WAN
LAN
General Setup
VLAN
Bind IP to MAC
LAN Port Mirror
Wired 802.1X
Hotspot Web Portal

II-2-1 General Setup

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

There are several subnets provided by the router which allow users to divide groups into different subnets (LAN1 - LAN4). In addition, different subnets can link for each other by configuring **Inter-LAN Routing**. At present, LAN1 setting is fixed with NAT mode only. LAN2/3/4 can be operated under **NAT** or **Route** mode. IP Routed Subnet can be operated under Route mode.

LAN >> General Setup

General Setup

Index	Enable	DNAT	IP Address	Details Page	Pv6
LAN 1	☒	☒	192.168.1.1	Details Page	Pv6
LAN 2	☐	☒	192.168.2.1	Details Page	Pv6
LAN 3	☐	☒	192.168.3.1	Details Page	Pv6
LAN 4	☐	☒	192.168.4.1	Details Page	Pv6
IP Routed Subnet	☐	☒	192.168.0.1	Details Page	

DNAT Server Option

Notes:

Please enable LAN 2 - 4 on **LAN >> VLAN** page before configure them.

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

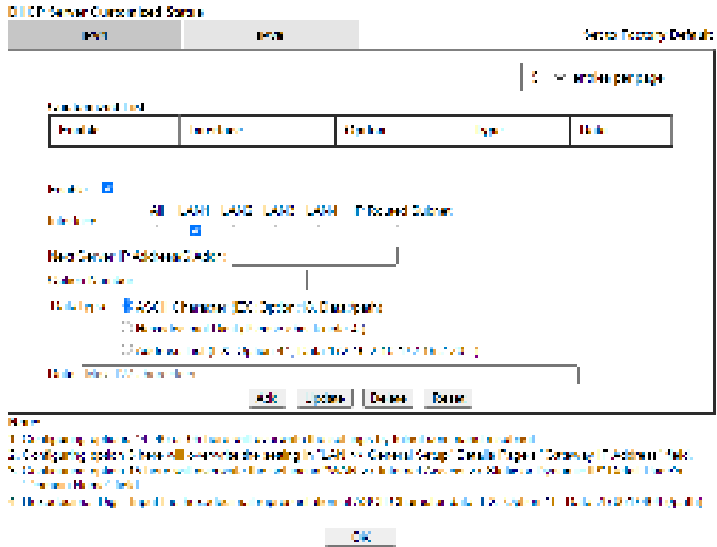
Inter-LAN Routing

Subnet	LAN 1	LAN 2	LAN 3	LAN 4
LAN 1	☒	☐	☐	☐
LAN 2	☐	☒	☐	☐
LAN 3	☐	☐	☒	☐
LAN 4	☐	☐	☐	☒

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. Enable - Basically, LAN1 status is enabled in default. LAN2 and IP Routed Subnet can be observed by checking the box of

	Status. DHCP- LAN1 is configured with DHCP in default. If required, please check the DHCP box for each LAN. IP Address - Display the IP address for each LAN item. Such information is set in default and you can not modify it. Details Page - Click it to access into the setting page. Each LAN will have different LAN configuration page. Each LAN must be configured in different subnet. IPv6 –Click it to access into the settings page of IPv6.
DHCP Server Option	DHCP packets can be processed by adding option number and data information when such function is enabled.  Enable/Disable - Enable/Disable the function of DHCP Option. Each DHCP option is composed by an option number with data. For example, Option number:100 Data: abcd When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets. Interface - Choose the interface for such option. Next Server IP Address/SIAddr - Type the IP address for the next server. Vigor router's DHCP server can redirect clients to a secondary server specified in such field. Option Number - Type a number for such function. Data Type - Choose the type (ASCII or Hex or address list) for the data to be stored. Data - Type the content of the data to be processed by the function of DHCP option.
Force router to use DNS server IP address	Force Vigor router to use DNS servers configured in LAN1/LAN2 instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).
Inter-LAN Routing	Check the box to link two or more different subnets (LAN and LAN).

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

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

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

LAN => General Setup

LAN 1 Ethernet TCP/IP and DHCP Setup		LAN 1 IPv6 Setup	
Network Configuration		DHCP Server Configuration	
For NAT Usage		☐ Disable ☒ Enable Server ☐ Enable Relay Agent	
IP Address	192.168.1.1	Start IP Address	192.168.1.10
Subnet Mask	255.255.255.0 / 24	IP Pool Count	200 (max: 253)
RIP Protocol Control	Disable	Gateway IP Address	192.168.1.1
		Lease Time	86400 (s)
		☒ Clear DHCP lease for inactive clients periodically	
		DNS Server IP Address	
		Primary IP Address	
		Secondary IP Address	

OK

Available settings are explained as follows:

Item	Description
Network Configuration	For NAT Usage, IP Address - Type in private IP address for connecting to a local private network (Default: 192.168.1.1). Subnet Mask - Type in an address code that determines the size of the network. (Default: 255.255.255.0 / 24) RIP Protocol Control, Disable - deactivate the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default) Enable –activate the RIP protocol.
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatches related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network. If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location. Disable Server –Let you manually assign IP address to every host in the LAN. Enable Relay Agent –Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to. ● 1st / 2nd 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.

	Enable Server - Let the router assign IP address to every host in the LAN. ● Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254. ● IP Pool Counts - Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253. ● Gateway IP Address - Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway. ● Lease Time - Enter the time to determine how long the IP address assigned by DHCP server can be used. ● Clear DHCP lease for inactive clients periodically - Whenever a DHCP client requests an IP address from the LAN DHCP server, the server will give out an IP to this client for a certain amount of time (e.g., 1 day). However, even if this client only uses the IP for say 5 minutes, the server still "reserves" 1 day for that client. Because a DHCP server only has a limited number of IPs to lease to its DHCP clients, soon enough all the IPs will be used out and then no one will be able to get any IPs from this server anymore. Therefore, this feature is used to get the IP back from inactive clients (i.e. doesn't use the IP but the server still reserves the IP for him).
DNS Server IP Address	DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address. Primary IP Address - You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field. Secondary IP Address - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field. The default DNS Server IP address can be found via Online Status:  If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache. If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the router forwards the DNS query packet to the

	external DNS server by establishing a WAN (e.g. DSL/Cable) connection.

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

II-2-1-2 Details Page for LAN2/3/4

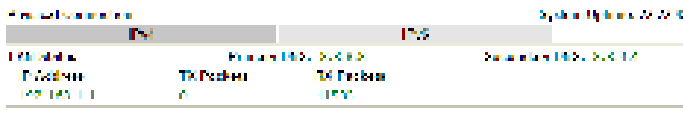
LAN => General Setup

LAN 2 Ethernet TCP/IP and DHCP Setup	LAN 2 IPv6 Setup
Network Configuration ☐ Enable ☒ Disable ☒ For NAT Usage ☐ For Routing Usage IP Address: 192.168.1.1 Subnet Mask: 255.255.255.0 / 24	DHCP Server Configuration ☐ Disable ☒ Enable Server ☐ Enable Relay Agent Start IP Address: 192.168.1.10 IP Pool Counts: 100 (max: 255) Gateway IP Address: 192.168.1.1 Lease Time: 255200 (s) ☒ Clear DHCP leases for inactive clients periodically DNS Server IP Address Primary IP Address: Secondary IP Address:

OK

Available settings are explained as follows:

Item	Description
Network Configuration	Enable/Disable - Click Enable to enable such configuration; click Disable to disable such configuration. For NAT Usage - Click this radio button to invoke NAT function. For Routing Usage - Click this radio button to invoke this function. IP Address - Type in private IP address for connecting to a local private network (Default: 192.168.1.1). Subnet Mask - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network. Disable – Let you manually assign IP address to every host in the LAN. Enable Server - Let the router assign IP address to every host in the LAN. ● 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. 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. ● 1st/2nd 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. Clear DHCP lease for inactive clients periodically - Whenever a DHCP client requests an IP address from the LAN DHCP server, the server will give out an IP to this client for a certain amount of time (e.g., 1 day). However, even if this client only uses the IP for say 5 minutes, the server still "reserves" 1 day for that client. Because a DHCP server only has a limited number of IPs to lease to its DHCP clients, soon enough all the IPs will be used out and then no one will be able to get any IPs from this server anymore. Therefore, this feature is used to get the IP back from inactive clients (i.e. doesn't use the IP but the server still reserves the IP for him).
DNS Server IP Address	DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address. Primary IP Address - You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field. Secondary IP Address - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field. The default DNS Server IP address can be found via Online Status: Online Status  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

Network Configuration ☐ Enable ☒ Disable For Routing Usage IP Address 192.168.0.1 Subnet Mask 255.255.255.0/24 RIP Protocol Control Disable	DHCP Server Configuration Start IP Address IP Pool Count 0 (max: 32) Lease Time 20s200 (s) ☐ Use LAN Port ☒ P1 ☒ P2 ☒ Use MAC Address <table border="1"><thead><tr><th>Index</th><th>Matched MAC Address</th><th>Given IP Address</th></tr></thead><tbody></tbody></table> MAC Address : : : : : Add Delete Edit Cancel	Index	Matched MAC Address	Given IP Address
Index	Matched MAC Address	Given IP Address		

Available settings are explained as follows:

Item	Description
Network Configuration	Enable/Disable - Click Enable to enable such configuration; click Disable to disable such configuration. For Routing Usage , IP Address - Type in private IP address for connecting to a local private network (Default: 192.168.1.1). Subnet Mask - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24) RIP Protocol Control , Disable - deactivate the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default) Enable – activate the RIP protocol.
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network. If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location. Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the

	1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254. IP Pool Counts - Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253. Lease Time - Enter the time to determine how long the IP address assigned by DHCP server can be used. Use LAN Port –Specify an IP for IP Route Subnet. If it is enabled, DHCP server will assign IP address automatically for the clients coming from P1. Please check the box of P1. 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 LAN1~ LAN4 – IPv6 Setup

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

LAN 1 Ethernet TCP/IP and DHCP Setup

LAN 1 IPv6 Setup

☒ Enable IPv6

WAN Primary Interface | WAN1 ▾

Static IPv6 Address

IPv6 Address	Prefix Length	
		Add Delete

Unique Local Address(ULA) configuration

Current IPv6 Address Table

Index	IPv6 Address/Prefix Length	Scope
1	2001::2001:Address:2001::/64	Link

DNS Server IPv6 Address

Deploy when WAN is up ▾

Primary DNS Server

Secondary DNS Server

Management

☒ SLAAC(stateless) ▾
 ☐ Other Option(0-10)

DHCPv6 Server

☒ Enable Server
 ☐ Disable Server

☐ IPv6 Address Random Allocation

☒ Auto IPv6 range

Start IPv6 Address

End IPv6 Address

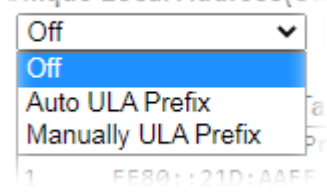
Advance setting

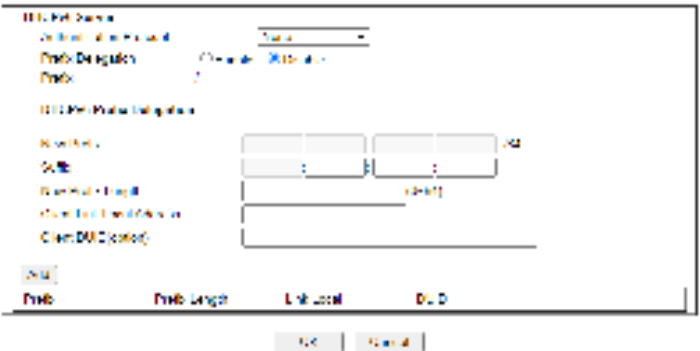
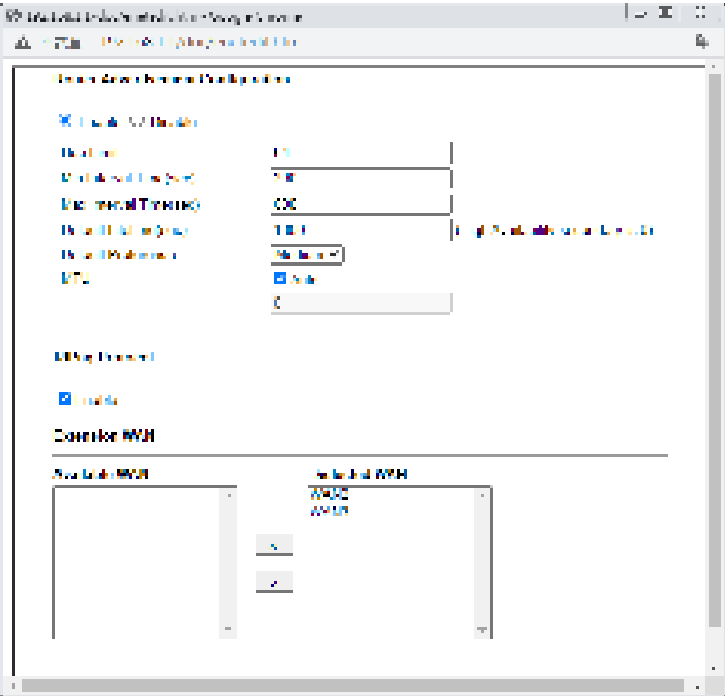
Advance setting

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

Available settings are explained as follows:

Item	Description
Enable IPv6	Check the box to enable the configuration of LAN 1 IPv6 Setup.
WAN Primary Interface	Use the drop down list to specify a WAN interface for IPv6.
Static IPv6 Address	IPv6 Address -Type static IPv6 address for LAN. Prefix Length – 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	Unique Local Addresses (ULAs) are private IPv6 addresses assigned to LAN clients. Off - ULA is disabled. Manually ULA Prefix - LAN clients will be assigned ULAs

	generated based on the prefix manually entered. Auto ULA Prefix - LAN clients will be assigned ULAs using an automatically-determined prefix. 
Current IPv6 Address Table	Display current used IPv6 addresses.
DNS Server IPv6 Address	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. Enable - The RA (router advertisement) packets will be sent to LAN PC with DNS server information no matter WAN connection is up or not. ● Primary DNS Server - Type the IPv6 address for Primary DNS server. ● Secondary DNS Server -Type another IPv6 address for DNS server if required. Disable - DNS server will not be used.
Management	Host under LAN can be assigned IP address from Vigor router via the following method. ● Off –No IP address is assigned. ● SLAAC(stateless) - The IP address (with Prefix) of the host shall be formed according to RA transmitted by Vigor router. ● DHCPv6(stateful) - The IP address of the host shall be assigned after communicating with DHCPv6 server for answering the request of client. Other Option (O-bit) - When selected, the Other Configuration flag is set, which indicates to LAN clients that IPv6 configuration information besides LAN IPv6 addresses is available from a DHCPv6 server. Setting the M-bit (see Management above) has the same effect as implicitly setting the O-bit, as DHCPv6 supplies all IPv6 configuration information, including what is indicated as available when the O-bit is set.
DHCPv6 Server	Disable Server - Click it to disable DHCPv6 server. Enable Server -Click it to enable DHCPv6 server. DHCPv6 Server could assign IPv6 address to PC according to the Start/End IPv6 address configuration. IPv6 Address Random Allocation - Check it to assign the DHCPv6 IP address randomly to prevent the attacks from the IPv6 reconnaissance techniques. Auto IPv6 range - When selected, the router's built-in DHCPv6 server decides the LAN IPv6 address range to be used. When deselected, LAN IPv6 addresses given out will be within the range as specified in the Start IPv6 Address and End IPv6 Address. ● Start IPv6 Address / End IPv6 Address - Enter the start

	and end address for IPv6 server. Advance setting - Click the Edit button to bring up the IPv6 Advanced Settings page. 
Advance setting	More options are offered under the Advance setting. Click Edit to open the pop-up window.  Router Advertisement Configuration - Click Enable to enable router advertisement server. The router advertisement daemon sends Router Advertisement messages, specified by RFC 2461, to a local Ethernet LAN periodically and when requested by a node sending a Router Solicitation message. These messages are required for IPv6 stateless auto-configuration. Disable - Click it to disable router advertisement server. Hop Limit - The value is required for the device behind the router when IPv6 is in use. Default value of hop limit field in Route Advertisement messages. Min/Max Interval Time (sec) - Minimum/ Maximum time, in seconds, between unsolicited multicast route advertisement messages sent by the RA server. Default Lifetime (sec) - Time, in seconds, that the router is to be used as the default router. Default Preference - Default preference value (Low,

	Medium, High) of the router sent in route advertisement messages. MTU - It means Max Transmit Unit for packet. If Auto is selected, the router determines the MTU value to send in route advertisement messages. RIPng Protocol - RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2. Extension WAN - In addition to the default WAN used for IPv6 traffic specified in the WAN Primary Interface in the LAN IPv6 Setup page, additional WANs can be selected to carry IPv6 traffic by enabling them in the Extension WAN section. Available WAN - Additional WANs available but not currently selected to carry IPv6 traffic. Selected WAN - Additional WANs selected to carry IPv6 traffic.

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

II-2-1-5 DHCP Server Option

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

LAN >> General Setup

DHCP Server Customized Status

IPv4 IPv6 [Set to Factory Default](#)

5 entries per page

Enable	Interface	Option	Type	Data
☒	All LAN1 LAN2 LAN3 LAN4 IP Routed Subnet ☐ ☒ ☐ ☐ ☐ ☐			
Next Server IP Address/Address: Option Number: Data type: ☒ ASCII Character (LX:Option:10, Data:/path) ☐ Hexadecimal Digit (Please check note 4) ☐ Address List (LX:Option:44, Data:172.16.2.10,172.16.2.20...) Data: Max 127 characters				
Add Update Delete Reset				

Note:

1. Configuring option 44, 46 or 58 here will overwrite the settings by telnet command on router.
2. Configuring option 2 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.
4. Hexadecimal Digit: Input the hexadecimal representation of ASCII Character data. EX: Option 18, Data 000B174F8 (/path)

OK

Available settings are explained as follows:

Item	Description
Customized List	Shows all the DHCP options that have been configured in the system.

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

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

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

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

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

II-2-2 VLAN

Vigor router provides extremely high speed connectivity for the highest speed local data transfer of any server or local PCs. On the Wireless-equipped models (e.g., Vigor2765ac), 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 Vigor2765 series:

LAN >> VLAN Configuration 

VLAN Configuration

☒ Enable																
	LAN				Wireless LAN				Wireless LAN 5G				VLAN Tag			
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
VLAN0	☒	☒	☒	☒	☐	☐	☐	☐	☐	☐	☐	☐	LAN 1	☐	0	0
VLAN1	☐	☒	☒	☒	☐	☐	☐	☐	☐	☐	☐	☐	LAN 2	☐	0	0
VLAN2	☐	☐	☒	☒	☐	☐	☐	☐	☐	☐	☐	☐	LAN 3	☐	0	0
VLAN3	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	LAN 1	☐	0	0
VLAN4	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	LAN 1	☐	0	0
VLAN5	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	LAN 1	☐	0	0
VLAN6	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	LAN 1	☐	0	0
VLAN7	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	LAN 1	☐	0	0

☒ Permit untagged device in P1 to access other

OK Cancel 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	SSID1 – SSID4 – Check the SSID boxes to group them under the selected VLAN.
Wireless LAN 5G	SSID1 – SSID4 – Check the SSID boxes to group them under the selected VLAN. It is available for “ac” model.
Subnet	Choose one of them to make the selected VLAN mapping to the specified subnet only. For example, LAN1 is specified for VLAN0. It means that PCs grouped under VLAN0 can get the IP address(es) that specified by the subnet.
VLAN Tag	Enable - Check the box to enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the LAN while sending them out. Please type the tag value and specify the priority for the packets sending by LAN. VID - Type the value as the VLAN ID number. The range is from 0 to 4095. Priority - Type the packet priority number for such VLAN. The range is from 0 to 7.
Permit untagged device in P1 to access router	Select to allow untagged hosts connected to LAN port P1 to access the router. In case you have incorrectly configured VLAN functionality, you will still be able to access the router via the Web UI, and telnet and SSH shells to adjust the configuration.



Info

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

Inter-LAN Routing

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

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

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

Inter-LAN Routing

Subnet	LAN 1	LAN 2	LAN 3	LAN 4
LAN 1	☒	☐	☐	☐
LAN 2	☐	☒	☐	☐
LAN 3	☐	☐	☒	☐
LAN 4	☐	☐	☐	☒

OK

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

Vigor2765 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

	LAN												Subnet	VLAN Tag		
	LAN				Wireless LAN				Wireless LAN SS					Enable	VID	Priority
	P1	P2	P3	SSID1	SSID2	SSID3	SSID4	SSID1	SSID2	SSID3	SSID4					
VLAN0	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	LAN 1	☐	0	0	
VLAN1	☐	☒	☒	☐	☐	☐	☐	☐	☐	☐	☐	LAN 2	☐	0	0	
VLAN2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	LAN 1	☐	0	0	
VLAN3	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	LAN 1	☐	0	0	
VLAN4	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	LAN 1	☐	0	0	
VLAN5	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	LAN 1	☐	0	0	
VLAN6	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	LAN 1	☐	0	0	
VLAN7	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	LAN 1	☐	0	0	

OK

Clear

Cancel

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

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

Inter LAN Routing

Subnet	LAN 1	LAN 2	LAN 3	LAN 4
LAN 1	☒	☐	☐	☐
LAN 2	☒	☒	☐	☐
LAN 3	☐	☐	☒	☐
LAN 4	☐	☐	☐	☒

OK

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



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 Subject:

ARP Table | Select All | Sort | Refresh | Add/Update to IP Bind List

IP Address	Mac Address	Sort ID
192.168.1.1	00-24-40-00-00-4F	

IP Address:

Mac Address:

Comment:

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

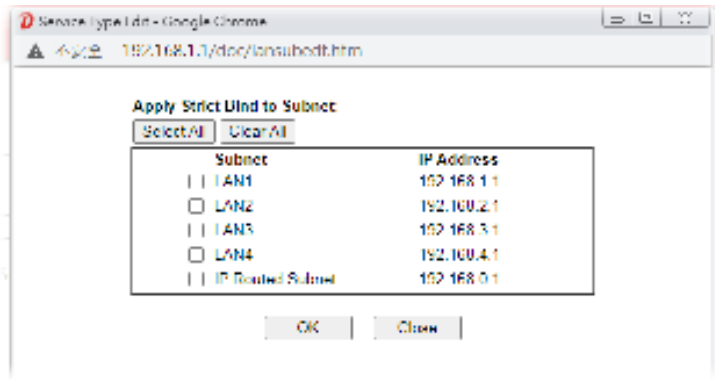
Index	IP Address	Mac Address	Sort ID	Comment

Note:

1. IP/MAC binding prevents DHCP Allocation.
2. If Strict Bind is enabled, unspecified LAN clients in the selected subnets cannot access the Internet.
3. Comment can not contain characters " " and "

Available settings are explained as follows:

Item	Description
Enable	Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.
Disable	Click this radio button to disable this function. All the settings on this page will be invalid.

Strict Bind	Click this radio button to block the connection of the IP/MAC which is not listed in IP Bind List. Apply Strict Bind to Subnet – Choose the subnet(s) for applying the rules of Bind IP to MAC. 
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/Update to IP Bind List	IP Address – Type the IP address that will be used for the specified MAC address. Mac Address – Type the MAC address that is used to bind with the assigned IP address. Comment – Type a brief description for the entry.
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
Mirror Port	☐	☐	☐	☐	
Mirrored Tx Port	☐	☐	☐	☐	☐
Mirrored Rx Port	☐	☐	☐	☐	☐

Note:

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

OK

Available settings are explained as follows:

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

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

II-2-5 Wired 802.1x

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

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

LAN >> Wired 802.1X

Wired 802.1X

LAN 802.1X:

☒ Enable

802.1X ports:

☐ P1

☐ P2

☐ P3

☐ P4

Notes:

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

OK

Available settings are explained as follows:

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

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

II-3 NAT

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

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

The benefit of the NAT includes:

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



Info

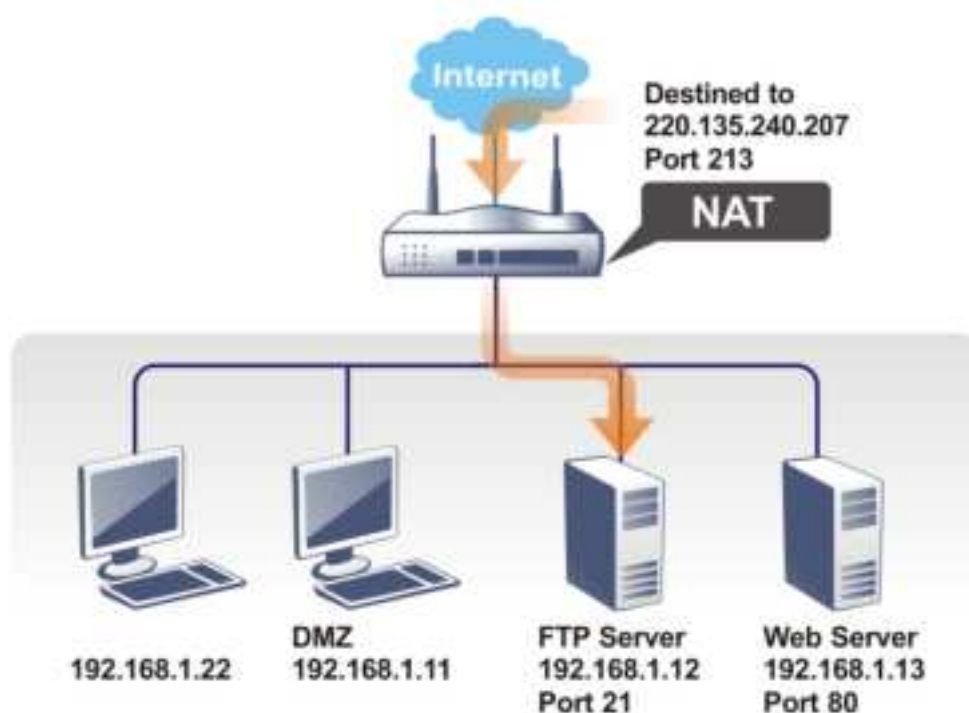
On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by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

Web User Interface



II-3-1 Port Redirection

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



The port redirection can only apply to incoming traffic.

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

Port Redirection

| [Set to Factory Default](#) |

Index	Enable	Service Name	WAN Interface	Protocol	Public Port	Source IP	Private IP
1.	☐		All			Any	
2.	☐		All			Any	
3.	☐		All			Any	
4.	☐		All			Any	
5.	☐		All			Any	
6.	☐		All			Any	
7.	☐		All			Any	
8.	☐		All			Any	
9.	☐		All			Any	
10.	☐		All			Any	
11.	☐		All			Any	
12.	☐		All			Any	
13.	☐		All			Any	
14.	☐		All			Any	
15.	☐		All			Any	
16.	☐		All			Any	
17.	☐		All			Any	
18.	☐		All			Any	
19.	☐		All			Any	
20.	☐		All			Any	

OK

Cancel

Backup settings:

Backup

Upload From File: 1.1.1.1 1.1.1.1

Recover

Note:

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

Each item is explained as follows:

Item	Description
Index	Display the number of the profile.
Enable	Check the box to enable the port redirection profile.
Service Name	Display the description of the specific network service.
WAN Interface	Display the WAN IP address used by the profile.
Protocol	Display the transport layer protocol (TCP or UDP).
Public Port	Display the port number which will be redirected to the specified Private IP and Port of the internal host.
Source IP	Display the IP object of the source IP.
Private IP	Display the IP address of the internal host providing the service.

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

NAI >> Port Redirection

Index No. 1

The screenshot shows the 'NAI Port Redirection' configuration window. The 'Enable' checkbox is checked. The 'Mode' is set to 'Single'. The 'Service Name' field is empty. The 'Protocol' is set to 'TCP'. The 'WAN Interface' is set to 'All'. The 'Public Port' is set to '0'. The 'Source IP' is set to 'IP Object'. The 'Private IP' is set to 'Any'. The 'Private Port' field is empty. There are buttons for 'OK', 'Clear', and 'Cancel'.

Note:

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

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable such port redirection setting.
Mode	Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select Range . In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered, the system will calculate and display the ending IP of private IP automatically.
Service Name	Enter the description of the specific network service.
Protocol	Select the transport layer protocol (TCP or UDP).
WAN Interface	Select the WAN interface used for port redirection. 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 any IP address/ IP Object / IP Group. IP Object - Use the drop down list to specify an IP object profile. IP Group - Use the drop down list to specify an IP group profile.
Private IP	Specify the private IP address of the internal host providing the service. If you choose Range as the port redirection mode, you will see two boxes on this field. Type a complete IP address in the first box (as the starting point). The second one will be assigned automatically later.
Private Port	Specify the private port number of the service offered by the internal host.

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

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

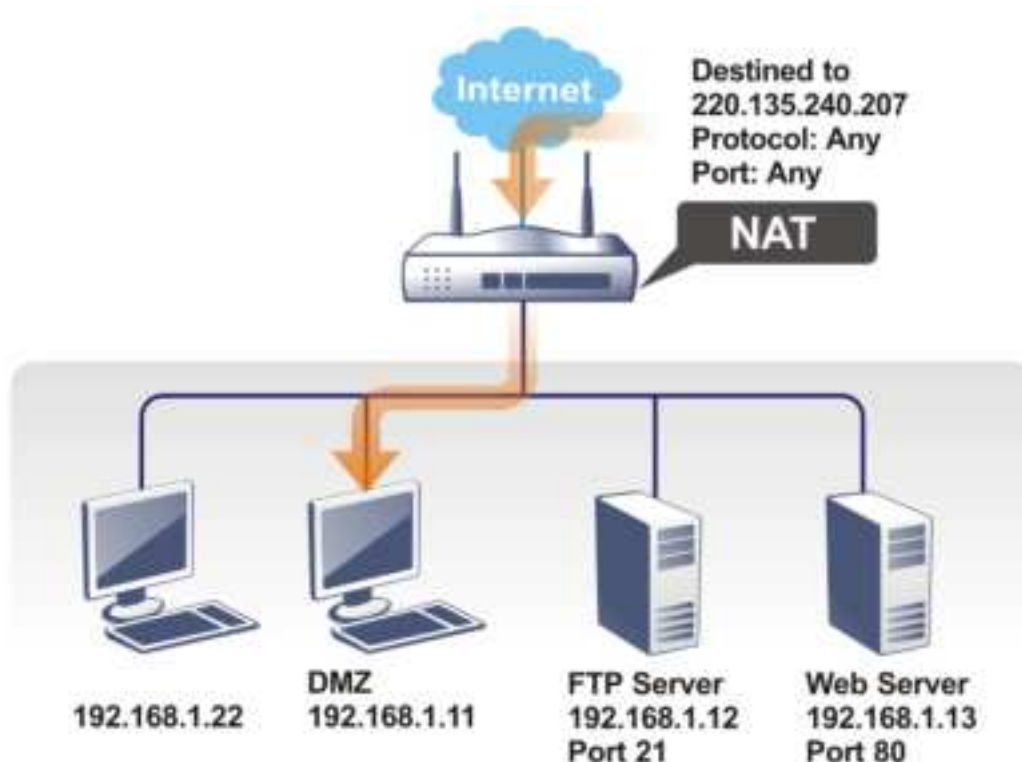
For example, the built-in web user interface in the router is with default port 80, which may conflict with the web server in the local network, `http://192.168.1.13:80`. Therefore, you need to **change the router's http port to any one other than the default port 80** to avoid conflict, such as 8080.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

System Maintenance >> Management

IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup																		
Router Name: ProxyTelnet ☐ Default Flexible Auto-Login ☐ Enable Validation Code in Internet/LAN Access Note: IFR and below version does NOT support ProxyOS CAPTCHA auth code. Internet Access Control ☐ Allow management from the Internet Domain name allowed: ☐ IIP Server ☐ HTTP Server ☒ Enforce HTTPS Access ☒ HTTPS Server ☐ Telnet Server ☐ TR069 Server ☐ SSH Server ☐ SNMP Server ☒ Flexible PING from the Internet Access List from the Internet ☐ Apply Access List to PING																				
Management Port Setup ☒ User Define Ports ☐ Default Ports <table><tbody><tr><td>Telnet Port</td><td> 23 </td><td>(Default: 23)</td></tr><tr><td>HTTP Port</td><td> 80 </td><td>(Default: 80)</td></tr><tr><td>HTTPS Port</td><td> 443 </td><td>(Default: 443)</td></tr><tr><td>FTP Port</td><td> 21 </td><td>(Default: 21)</td></tr><tr><td>TR069 Port</td><td> 3498 </td><td>(Default: 3498)</td></tr><tr><td>SSH Port</td><td> 22 </td><td>(Default: 22)</td></tr></tbody></table> Note: Ports 3498 and 3499 are used for Hotspot Web Portal. Brute Force Protection ☐ Enable brute force login protection ☐ FTP Server ☐ HTTPS Server ☐ HTTP Server ☐ Telnet Server ☐ TR069 Server			Telnet Port	23	(Default: 23)	HTTP Port	80	(Default: 80)	HTTPS Port	443	(Default: 443)	FTP Port	21	(Default: 21)	TR069 Port	3498	(Default: 3498)	SSH Port	22	(Default: 22)
Telnet Port	23	(Default: 23)																		
HTTP Port	80	(Default: 80)																		
HTTPS Port	443	(Default: 443)																		
FTP Port	21	(Default: 21)																		
TR069 Port	3498	(Default: 3498)																		
SSH Port	22	(Default: 22)																		

II-3-2 DMZ Host

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



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

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

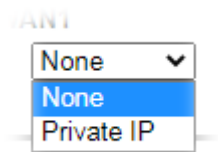
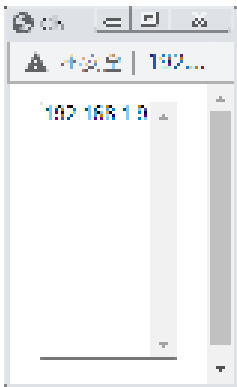
NAT => DMZ Host Setup

DMZ Host Setup

WAN1	WAN2	WAN3
WAN1		
Name		
Private IP		Choose IP

OK

Available settings are explained as follows:

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

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

MAN >> DMZ Host Setup

DMZ Host Setup

WAN1	WAN2	WAN3
WAN 2 Enable ☒ Private IP 192.168.1.0 Choose IP...		

OK

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

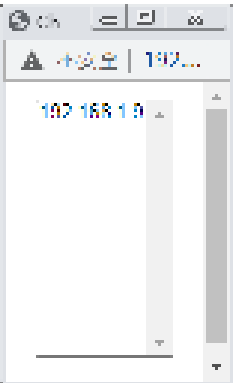
MAN >> DMZ Host Setup

DMZ Host Setup

WAN1	WAN2	WAN3															
WAN 1 <table border="1"> <thead> <tr> <th>Index</th> <th>Enable</th> <th>Aux. WAN IP</th> <th>Private IP</th> <th></th> </tr> </thead> <tbody> <tr> <td>1.</td> <td>☐</td> <td>---</td> <td>192.168.1.0</td> <td>Choose IP...</td> </tr> <tr> <td>2.</td> <td>☐</td> <td>192.168.1.50</td> <td>192.168.1.0</td> <td>Choose IP...</td> </tr> </tbody> </table>	Index	Enable	Aux. WAN IP	Private IP		1.	☐	---	192.168.1.0	Choose IP...	2.	☐	192.168.1.50	192.168.1.0	Choose IP...		
Index	Enable	Aux. WAN IP	Private IP														
1.	☐	---	192.168.1.0	Choose IP...													
2.	☐	192.168.1.50	192.168.1.0	Choose IP...													

OK Cancel

Available settings are explained as follows:

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

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

II-3-3 Open Ports

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

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

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

NAT >> Open Ports

Open Ports Setup

[Set to Factory Default](#)

Index	Enable	Comment	Source IP	Local IP Address
1.	☐		Any	
2.	☐		Any	
3.	☐		Any	
4.	☐		Any	
5.	☐		Any	
6.	☐		Any	
7.	☐		Any	
8.	☐		Any	
9.	☐		Any	
10.	☐		Any	

OK

Cancel

Backup settings:

Backup

Upload from file:

Upload from file

Upload from file

Restore

Note:

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

Available settings are explained as follows:

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

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

NAI => Open Ports => Edit Open Ports

Index No. 1

☒ Enable Open Ports

Comment

Source IP

Private IP

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

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.
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.

NAI => Open Ports

Open Ports Setup [Set to Factory Default](#)

Index	Enable	Comment	Source IP	Local IP Address
1.	☒	FP2	Any	192.168.1.0/8
2.	☐		Any	
3.	☐		Any	
4.	☐		Any	
5.	☐		Any	
6.	☐		Any	

II-3-4 Port Triggering

Port Triggering is a variation of open ports function.

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

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

TCP: 86400 sec.

UDP: 180 sec.

IGMP: 10 sec.

TCP WWW: 60 sec.

TCP SYN: 60 sec.

NAI :: Port Triggering

Port Triggering [Set to Factory Default](#)

Index	Enable	Comment	Triggering Protocol	Source IP	Triggering Port	Incoming Protocol	Incoming Port
1.	☐			Any			
2.	☐			Any			
3.	☐			Any			
4.	☐			Any			
5.	☐			Any			
6.	☐			Any			
7.	☐			Any			
8.	☐			Any			
9.	☐			Any			
10.	☐			Any			

1 10 11 20 Next

OK Cancel

Available settings are explained as follows:

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

Incoming Port	Display the port for the incoming data of such triggering profile.

Click the index number link to open the configuration page.

[NAT => Port Triggering](#)

No. 1

☒ **Enable**

Service: User Defined ▼

Comment:

Source IP: IP Object ▼ None ▼

Triggering Protocol: TCP ▼

Triggering Port:

Incoming Protocol: TCP ▼

Incoming Port:

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

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Enable	Check to enable this entry.
Service	Choose the predefined service to apply for such trigger profile. User Defined ▼ User Defined Real Player QuickTime WMP IRC AIM Talk ICQ PalTalk BitTorrent
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-3-5 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

	Protocol	Listen Port		TCP	UDP
☐ Disable	SIP	5060	(1-65535)	☒	☒
	RTSP	554	(1-65535)	☒	☒

OK

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-4 Applications

Dynamic DNS

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

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

LAN DNS / DNS Forwarding

The LAN DNS lets the network administrators host servers with privacy and security. When the network administrators of your office set up FTP, Mail or Web server inside LAN, you can specify specific private IP address (es) to correspondent servers. Thus, even the remote PC is adopting public DNS as the DNS server, the LAN DNS resolution on Vigor2765 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

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

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

UPnP

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

Wake on LAN

A PC client on LAN can be woken up by the router it connects. When a user wants to wake up a specified PC through the router, he/she must type correct MAC address of the specified PC on this web page of **Wake on LAN** (WOL) of this router.

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

Web User Interface



II-4-1 Dynamic DNS

Enable the Function and Add a Dynamic DNS Account

To begin configuring Dynamic DNS, from the main menu, navigate to **Applications**, and select **Dynamic DNS**. The Dynamic DNS main configuration screen appears:

Applications >> Dynamic DNS Setup

Available settings are explained as follows:

Item	Description
Enable Dynamic DNS Setup	Check this box to enable DDNS function.
Set to Factory Default	Clear all profiles and recover to factory settings.
View Log	Display DDNS log status.
Force Update	Force the router updates its information to DDNS server.
Auto-Update interval	Set the time for the router to perform auto update for DDNS service.

Index	Click the number below Index to access into the setting page of DDNS setup to set account(s).
Enable	Check the box to enable such account.
WAN Interface	Show the WAN interface associated with the DDNS profile.
Domain Name	Display the domain name that you set on the setting page of DDNS setup.

After clicking on the index number, the detail configuration screen for the DDNS profile appears:

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

Index : 1

☒ Enable Dynamic DNS Account

WAN Interface: WAN1 First

Service Provider: dyn.com (www.dyn.com)

Service Type: Dynamic

Domain Name: Max: 54 characters || Max: 63 characters

Login Name: Max: 64 characters

Password: Max: 64 characters

☐ Use Backup MX

Mail Extender: Max: 63 characters

Determine WAN IP: WAN IP

Available settings are explained as follows:

Item	Description
Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
WAN Interface	WAN1/WAN2/WAN3 First - While connecting, the router will use WAN1/WAN2/WAN3 as the first channel for such account. If WAN1/WAN2/WAN3 fails, the router will use another WAN interface instead. WAN1/WAN2/WAN3 Only - While connecting, the router will use WAN1/WAN2/WAN3 as the only channel for such account.
Service Provider	Select the service provider for the DDNS account.
Service Type	Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field. Note that this option is not available when User-Defined 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 User-Defined is selected as Service Provider.
Login Name	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.

Wildcard and Backup MX	The Wildcard and Backup MX (Mail Exchange) features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.
Mail Extender	If the mail server is defined with another name, please type the name in this area. Such mail server will be used as backup mail exchange.
Determine Real WAN IP	If a Vigor router is installed behind any NAT router, you can enable such function to locate the real WAN IP. When the WAN IP used by Vigor router is private IP, this function can detect the public IP used by the NAT router and use the detected IP address for DDNS update. There are two methods offered for you to choose: ● WAN IP - If it is selected and the WAN IP of Vigor router is private, DDNS update will take place right away. ● Internet IP - If it is selected and the WAN IP of Vigor router is private, it will be converted to public IP before DDNS update takes place.

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

DrayDDNS Settings

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

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

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

Index : 1

☒ Enable Dynamic DNS Account

Service Provider	DrayDDNS (Global)	Wizard	View Log
Status	Inactivated		
Domain Name	Max: 50 characters	drayddns.com	Sync domain
Determine WAN IP	WAN IP	☒ IPv4 ☐ IPv6	
WAN Interfaces	☐ WAN 1 ☐ WAN 2 ☐ WAN 3	☐ Also IP in Service Status Setup	
Connection Type	Http		
Let's Encrypt certificate			
Status	Empty	Update	
Auto Renew	☐		

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).
Service Provider	Choose DrayTek Global as the service provider. Wizard - This button is available when DrayTek Global is selected as Service Provider. To activate the DrayTek's DDNS service, click it to enable license issued by DrayTek through Wizards>>Service Activation Wizard. Refer to section A-1 How to use DrayDDNS? for detailed information.

Status	Display if the license is activated or not.
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: ● WAN IP - If it is selected and the WAN IP of Vigor router is private, DDNS update will take place right away. ● Internet IP - If it is selected and the WAN IP of Vigor router is private, it will be converted to public IP before DDNS update takes place.
WAN Interfaces	WAN1/WAN2/WAN3 - While connecting, the router will use WAN1/WAN2/WAN3 as the channel for such account.
Connection Type	Select HTTP or HTTPS for DrayDDNS.
Let's Encrypt certificate	Create –Click it to generate a certificate issued by Let's Encrypt for applying to such DDNS account. Auto Update - Check the box to make the system update the certificate automatically.

Disable the Function and Clear all Dynamic DNS Accounts

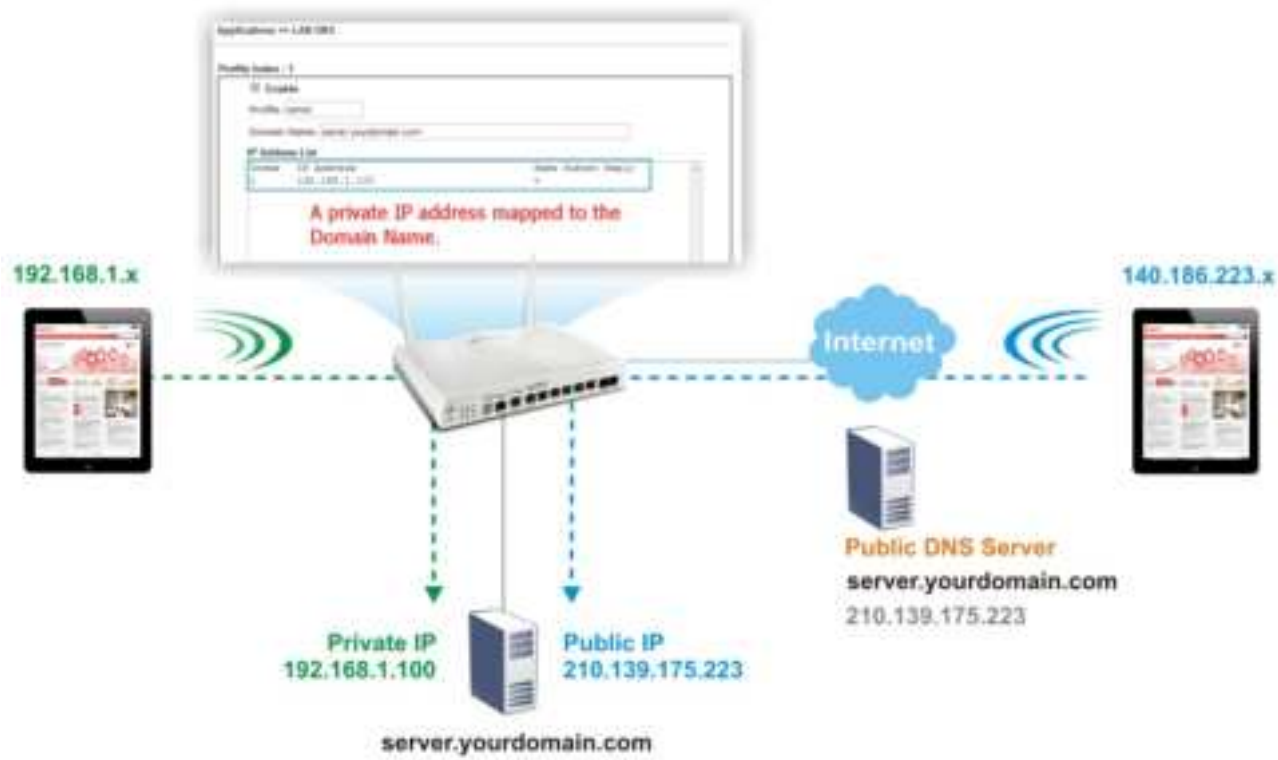
Uncheck **Enable Dynamic DNS Setup**, and click **Clear All** button to disable the function and clear all accounts from the router.

Delete a Dynamic DNS Account

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

II-4-2 LAN DNS / DNS Forwarding

The LAN DNS lets the network administrators host servers with privacy and security. When the network administrators of your office set up FTP, Mail or Web server inside LAN, you can specify specific private IP address (es) to correspondent servers. Thus, even the remote PC is adopting public DNS as the DNS server, the LAN DNS resolution on Vigor2765 Series will respond the specified private IP address.



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

Applications >> LAN DNS / DNS Forwarding ?

LAN DNS Resolution / Conditional DNS Forwarding Set to Factory Default

Index	Enable	Profile	Domain Name	Forwarding	DNS Server
1.	☐			-	
2.	☐			-	
3.	☐			-	
4.	☐			-	
5.	☐			-	
6.	☐			-	
7.	☐			-	
8.	☐			-	
9.	☐			-	
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.

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

To configure a LAN DNS profile, click on its index to bring up the configuration page.

Applications >> LAN DNS / DNS Forwarding

Profile Index : 1

☐ Enable

Profile:

Type: LAN DNS

Domain Name:

Note:

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

CNAME/Alias Domain Name:

IP Address List (Max. 40 entries)

Index	IP Address	Same Subnet Reply

Or,

Applications >> LAN DNS / DNS Forwarding

Profile Index : 1

☐ Enable

Profile:

Type: DNS Forwarding

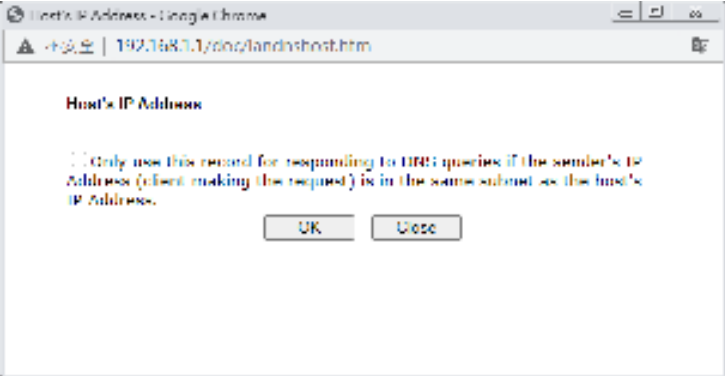
Domain Name:

Note:

1. Support wildcard subdomain, ex: *example.com
2. Support full wildcard, ex: *
3. Full wildcard will not serve to DNS cache table, and DNS server field only support IP

DNS Server IP/Host Name:

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable such profile.
Profile	Enter 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.
Type	Select LAN DNS or DNS Forwarding
If LAN DNS is selected	Domain Name - Enter the domain name for the router to look for in DNS queries to intercept and reply to. Wildcards in the form of asterisks (*) can be used to match a domain level. For example, *.draytek.com will match domain names such as www.draytek.com and ftp.draytek.com, whereas www.draytek.* will match domain names such as www.draytek.com and www.draytek.co.uk. CNAME - Click Add to add an domain name alias for the domain name. Click Delete next to an alias entry to delete it. 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 Add to bring up the Add IP Address dialog box:  ● Host's IP Address –Enter the IP address to be returned in response to a DNS query for the configured domain names and aliases. ● Only responds to the DNS... - Select to use this IP address only if the IP address of the source of the DNS query belongs to the same subnet as the host IP address entered above. After changes have been made, click OK to save and dismiss the dialog box, or Close to discard the changes and dismiss the dialog box. Delete -To delete an IP address, click on it and then click Delete.
If DNS Forwarding is selected	Domain Name - Enter the domain name for the router to look for in DNS queries to intercept and reply to. Wildcards in the form of asterisks (*) can be used to match a domain level. For example, *.draytek.com will match domain names such as www.draytek.com and ftp.draytek.com, whereas www.draytek.* will match domain names such as www.draytek.com and www.draytek.co.uk.

	DNS Server IP Address - Enter the IP address of the DNS server you want to use for DNS forwarding.

To save changes made to the LAN DNS profile, click **OK**. To clear the profile and restore the factory default blank values, click **Clear**.

II-4-3 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-4-3-1 General Setup

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

Application >> DNS Security ?

DNS Security

General Setup		Domain Diagnosis		Refresh	
Interface	Enable	Primary DNS	Secondary DNS	Bogus DNS Reply	
WAN1	☐	---	---	Drop ▼	
WAN2	☐	---	---	Pass ▼	
WAN3	☐	---	---	Drop ▼	

Notice:

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

Available settings are explained as follows:

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

II-4-3-2 Domain Diagnose

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

Application >> DNS Security

General Setup
Domain Diagnosis
DNS Cache

Domain: 00 IPv4 00 IPv6
Interface: WAN1
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-4-4 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: 2006 Jan 1 Sat 0:16:27 | System time set | Set to Factory Default

Index	Enable	Comment	Time	Frequency
1	☐			Hour
2	☐			Hour
3	☐			Hour
4	☐			Hour
5	☐			Hour
6	☐			Hour
7	☐			Hour
8	☐			Hour
9	☐			Hour
10	☐			Hour
11	☐			Hour
12	☐			Hour
13	☐			Hour
14	☐			Hour
15	☐			Hour

Legend: ☒ Force on ☐ Force down

OK

Available settings are explained as follows:

Item	Description
Current System Time	Shows the current time of the router.
System time set	Click to navigate to System Maintenance >> Time and Date to set the system time and date.
Set to Factory Default	Reset all schedules to factory default values.
Index	Shows the index number of the schedule entry.
Enable	Select to enable the schedule; clear to disable it.

Comment	Shows the name given to the schedule.
Time	Shows the start and end times of the schedule. The time interval of the schedule is indicated in dark grey.
Frequency	Shows the days of the week configured for the schedule. Selected days are shown in dark grey. ● - If it lights in green, it means such schedule is active.

To configure a schedule, click on its index to bring up the settings page.

Applications > Schedule

Index No. 1 Current System Time: 2000 Jan 1 Sat 0:19:00 | System time set

☒ Enable Schedule Setup

Comment: Ready for RD

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

Start Time (hh:mm): 1:00

Duration Time (hh:mm): 22:00

End Time (hh:mm): 23:00

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	Select to enable the schedule; clear to disable it.
Comment	Name to identify this schedule entry.
Start Date (yyyy-mm-dd)	The date when the entry comes into effect.
Start Time (hh:mm)	The time when the schedule is triggered. See the How Often setting below for details.
Duration Time (hh:mm)	How long the action lasts when the scheduled is triggered.
End Time (hh:mm)	It will be calculated automatically when Start Time and Duration Time are configured well.
Action	Action to take when the schedule is triggered. Force On - The feature with which this schedule is associated will be turned on. Force Down - The feature with which this schedule is associated will be turned off.
How Often	How frequently the schedule is triggered. ● Once - The schedule is triggered once, on the Start Date at the Start Time, for the Duration Time. ● Weekdays - The schedule will be triggered repeatedly, starting on the Start Date at the Start Time, on the

	selected days of the week, at the Start Time, for the Duration Time. ● 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.

To save changes made to the Schedule, click **OK**. To clear the schedule and restore the factory default blank values, click **Clear**. To cancel the changes and return to the main Schedule page, click **Cancel**.

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-4-5 RADIUS

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

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

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

RADIUS Setup

☒ **Enable**

☒ **Enable Accounting**

Comments (Max: 25 characters)

RADIUS Request Interval sec (2~30)

Primary Server

Primary Server		Max: 63 characters
Secret		Max: 63 characters
Authentication Port	1812	
Accounting Port	1813	
Disconnect Message Port	3768	
Interim Update Interval	10	min(x)(10~1440)
Retry	2	times(1~3)

Secondary Server

Secondary Server		Max: 63 characters
Secret		Max: 63 characters
Authentication Port	1812	
Accounting Port	1813	
Disconnect Message Port	3768	
Interim Update Interval	10	min(x)(10~1440)
Retry	2	times(1~3)

Note:

If RADIUS server has specified Interim Update Interval value(Acct-Interim-Interval), Vigor Router will follow the interval that the RADIUS server provides and ignore the Interim Update Interval setting here.

OK

Clear

Cancel

RADIUS Server Status Log

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

Available settings are explained as follows:

Item	Description
Enable	Check to enable the RADIUS server settings for RADIUS client authentication.
Enable Accounting	RADIUS Accounting is a network customer billing mechanism for RADIUS server. If enabled, Vigor router will deliver accounting request (e.g., IP address, traffic from the client) to the specified RADIUS server periodically.
Comments	Enter a brief description for the RADIUS server.
RADIUS Request Interval	Set a time interval for the router sending authentication request to the RADIUS server.

Primary Server / Secondary Server --- When the Primary server is down, Vigor system will try to connect the secondary server.

Primary Server	Primary Server - Enter the IP address of RADIUS server. 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. Authentication Port - The UDP port number that the RADIUS server uses for client authentication. The default value is 1812, based on RFC 2138. Accounting Port - The UDP port number that the RADIUS server uses to receive the accounting information from Vigor router. The default value is 1813. Disconnect Message Port - The UDP port number that the Vigor router uses to receive the disconnection information from the RADIUS server. The default value is 3799. Interim Update Interval - Set the time interval that Vigor router transmits the accounting information to RADIUS server. Retry - Set the number of attempts to perform reconnection with RADIUS server. If the connection (with the Primary Server) still fails, stop the connection attempt and begin to make connection with the secondary server.
Secondary Server	Secondary Server - Enter the IP address of RADIUS server. 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. Authentication Port - The UDP port number that the RADIUS server uses for client authentication. The default value is 1812, based on RFC 2138. Accounting Port - The UDP port number that the RADIUS server uses to receive the accounting information from Vigor router. The default value is 1813. Disconnect Message Port - The UDP port number that the Vigor router uses to receive the disconnection information from the RADIUS server. The default value is 3799. Interim Update Interval - Set the time interval that Vigor router transmits the accounting information to RADIUS server. Retry - Set the number of attempts to perform reconnection. If the connection (with the Secondary Server) still fails, stop the connection attempt. The client authentication would be determined as "failed".
RADIUS Server Status Log	Display the record of current status of RADIUS server.

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

II-4-6 UPnP

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



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

☒ Enable UPnP Service	Default WAN
☐ Enable Connection Control Service	Default WAN
☐ Enable Connection Status Service	WAN1
	WAN2
	WAN3

Notes:

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-4-7 IGMP

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

II-4-7-1 General Setting

Applications >> IGMP

General setting **Working status**

☐ **IGMP Proxy**
IGMP Proxy acts as a multicast proxy for hosts on the LAN side. Forbid 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)

Enable IGMP syslog: ☐

IGMP Snooping
Enable: Forward multicast traffic only to ports that are members of that group.
Disable: Treats multicast traffic the same as broadcast traffic.

☐ **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.

IGMP Accept List: Any
Only allow the IP of the LAN device to be included in the specified object/group to use IGMP

OK Cancel

Available settings are explained as follows:

Item	Description
IGMP Proxy	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. Interface - Specify an interface for packets passing through. 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. 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. 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. Enable IGMP syslog - Check the box to send the record of IGMP server to Syslog.

IGMP Snooping	Check this box to enable this function. Multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.
IGMP Fast Leave	Check this box to make the router stop forwarding multicast traffic to a LAN port as soon as it receives a leave message from that port. Each LAN port should have one IGMP host connected.
IGMP Accept List	When IGMP Snooping is enabled, use the drop down list to select an IP object or IP group. The IGMP will apply to the devices within the selected IP object/group only.

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

II-4-7-2 Working status

Applications >> IGMP

General setting Working status

| Refresh |

Multicast Group Table

Index	Group ID	P1	P2	P3	P4

IGMP Device Table

Index	MAC Address	IP Address	Interface	IGMP Version

Available settings are explained as follows:

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

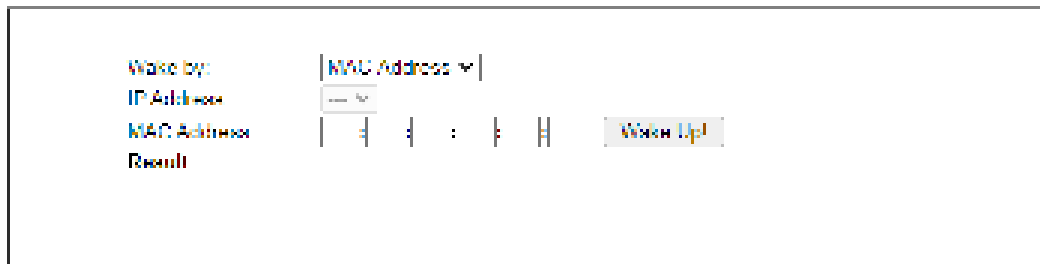
II-4-8 Wake on LAN

A PC client on LAN can be woken up by the router it connects. When a user wants to wake up a specified PC through the router, he/she must type correct MAC address of the specified PC on this web page of **Wake on LAN** (WOL) of this router.

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

Applications >> Wake on LAN

Wake on LAN



Note:

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

Available settings are explained as follows:

Item	Description
Wake by	If you choose to be woken by MAC Address , you have to type the correct MAC address of the host in MAC Address boxes.
IP Address	The IP addresses that have been configured in Firewall>>Bind IP to MAC will be shown in this drop down list. Choose the IP address from the drop down list that you want to wake up.
MAC Address	Type any one of the MAC address of the bound PCs.
Wake Up	Click this button to wake up the selected IP. See the following figure. The result will be shown on the box.

II-4-9 SMS / Mail Alert Service

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

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

II-4-9-1 SMS Alert

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

Applications >> SMS / Mail Alert Service

SMS Alert		Mail Alert		[Set to Factory Default]	
Index	Enable	SMS Provider	Recipient Number	Notify Profile	Schedule(1-15)
1	☐	1-999		1-999	Name
2	☐	1-999		1-999	None
3	☐	1-999		1-999	Name
4	☐	1-999		1-999	None
5	☐	1-999		1-999	Name
6	☐	1-999		1-999	None
7	☐	1-999		1-999	Name
8	☐	1-999		1-999	None
9	☐	1-999		1-999	Name
10	☐	1-999		1-999	None

Note:

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

OK Cancel

Available settings are explained as follows:

Item	Description
Index	Check the box to enable such profile.
Enable	Click the box to enable such profile.
SMS Provider	Use the drop down list to choose SMS service provider. You can click SMS Provider link to define the SMS server.
Recipient Number	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-4-9-2 Mail Alert

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

Application >> SMS / Mail Alert Service

SMS Alert		Mail Alert		Set to Factory Default			
Index	Enable	Mail Service	Mail Address	Notify Profile	Schedule(1-15)		
1	☒	1-???		1-???	North	▼	North
2	☐	1-???		1-???	None	▼	None
3	☒	1-???		1-???	North	▼	North
4	☐	1-???		1-???	None	▼	None
5	☒	1-???		1-???	North	▼	North
6	☐	1-???		1-???	None	▼	None
7	☒	1-???		1-???	North	▼	North
8	☐	1-???		1-???	None	▼	None
9	☒	1-???		1-???	North	▼	North
10	☐	1-???		1-???	None	▼	None

Note:

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

OK

Cancel

Available settings are explained as follows:

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

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

II-4-10 Bonjour

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

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

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

Applications >> Bonjour



Bonjour Setup

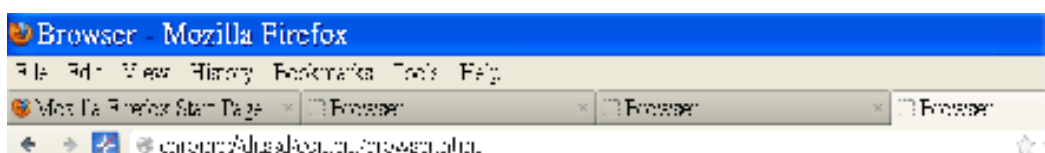
☐ Enable Bonjour Service
☐ HTTP Server
☐ FTP Server
☐ FTT Server
☐ SSH Server
☐ L2TP Printer Server

OK

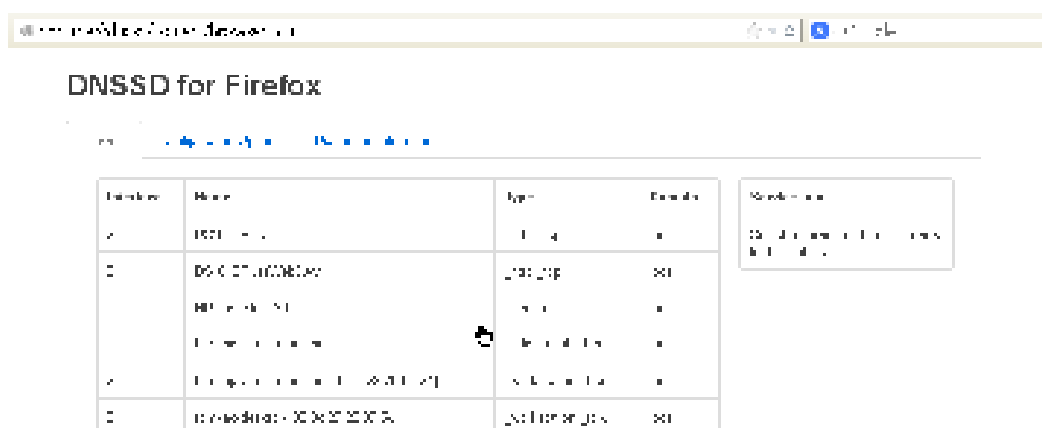
Cancel

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

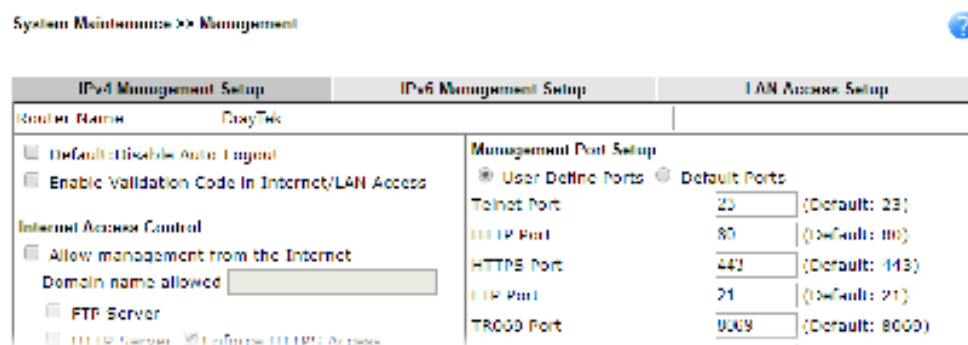
1. Here, we use Firefox and DNSSD to discover the service in such case. Therefore, just ensure the Bonjour client program and DNSSD for Firefox have been installed on the computer.



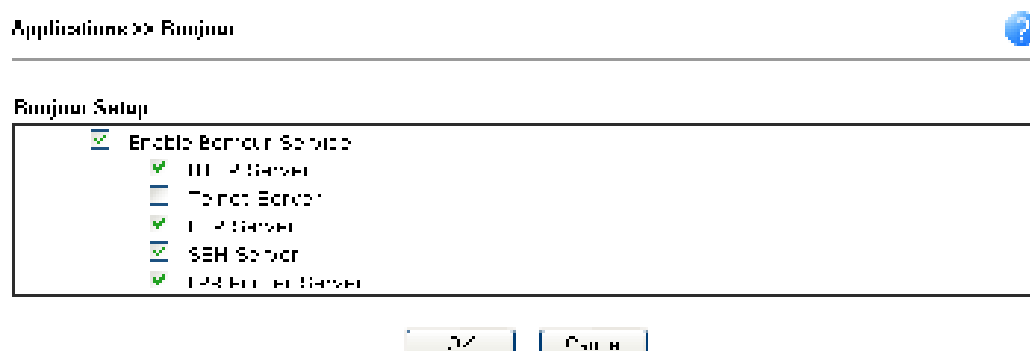
2. Open the web browser, Firefox. If Bonjour and DNSSD have been installed, you can open the web page (DNSSD) and see the following results.



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



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



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

Application Notes

A-1 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 2:26:50	
IPv4		IPv6			
LAN Status		Primary DNS: 191.25.152.1		Secondary DNS: 151.52.1.1	
IP Address	Tx Packets	Rx Packets			
10.1.2.1	2154	1115			
WAN 1 Status				:: Drop PPPoE	
Enable	Link	Name	Mode	Up Time	
Yes	Disconnected	j-i	PPPoE	2:26:50	
IP	GW IP	Tx Packets	Tx Data(Bps)	Rx Packets	Rx Data(Bps)
1.169.185.242	151.52.212.24	1400	5.11K	11211	212

Note that,

Username: jo***

Password: jo*****

Host name: j****.changeip.org

WAN IP address: 1.169.185.242

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



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

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 : WAN1

Service Provider : Customized

Provider Host : changeip.org

Service API : /dynamic/dns/update.asp?u=jo***&p=jo*****&hostname=j***.changeip.org&ip=###IP###&cmd=update&offline=0

Auth Type : basic

Connection Type : HTTP

Proxy Response :

Login Name : jo***

Password : jo*****

☐ Will Save

☐ Backup M8

Mail :

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*****

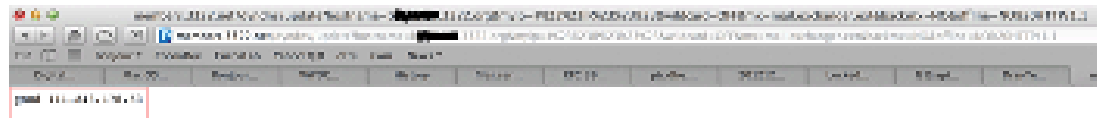
Host name: bi*****.3322.org

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

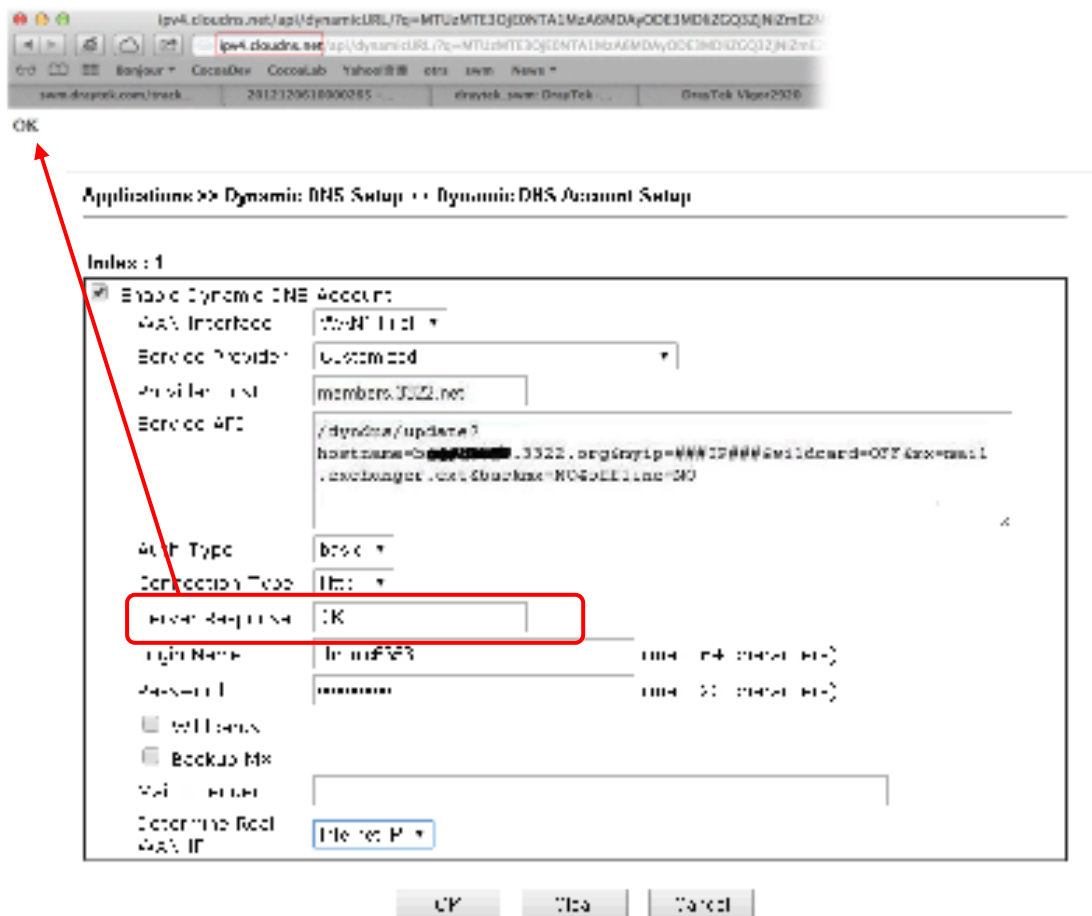
Service System	ON	Account
Account Interface	WAN IP v4	
Service Provider	Customized	
Provider Host	member.3322.net	
Service API	/dyndns/update? hostname=yourhost.3322.org&myip=###IP###&wildcard=OFF&mx=mail .exchanger.ext&backmx=NO&offline=NO	
Auth Type	Basic	
Current Interface	H1	
Server Response		
User Name	chcn0200	(max= 64 characters)
Password	*****	(max= 25 characters)
☐ Wildcards		
☐ Backmx		
Mail Exchanger		
Dynamic Host	Dynamic 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 CloudDNS.net.



II-5 Routing

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

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

Load Balance

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

Specify Interface

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

Address Mapping

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

Priority

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

Failover to/Failback

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

Other routing

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



Info

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

Web User Interface



II-5-1 Static Route

Go to **Routing** >> **Static Route**. You can create static routes so that traffic to specific IP addresses go through a particular LAN or WAN.

The Static Route Setup screen has separate tabs for IPv4 and IPv6. Select the appropriate tab to begin.

II-5-1-1 Static Route for IPv4

Routing >> Static Route Setup

IPv4		IPv6		Set to Factory Default View Routing Table	
Index	Enable	Destination Address	Mask	Gateway	Interface
1.	☐				
2.	☐				
3.	☐				
4.	☐				
5.	☐				
6.	☐				
7.	☐				
8.	☐				
9.	☐				
10.	☐				
11.	☐				
12.	☐				
13.	☐				
14.	☐				
15.	☐				
16.	☐				
17.	☐				
18.	☐				
19.	☐				
20.	☐				

OK Cancel

Backup settings Backup	Upload from file: Restore

Available settings are explained as follows:

Item	Description

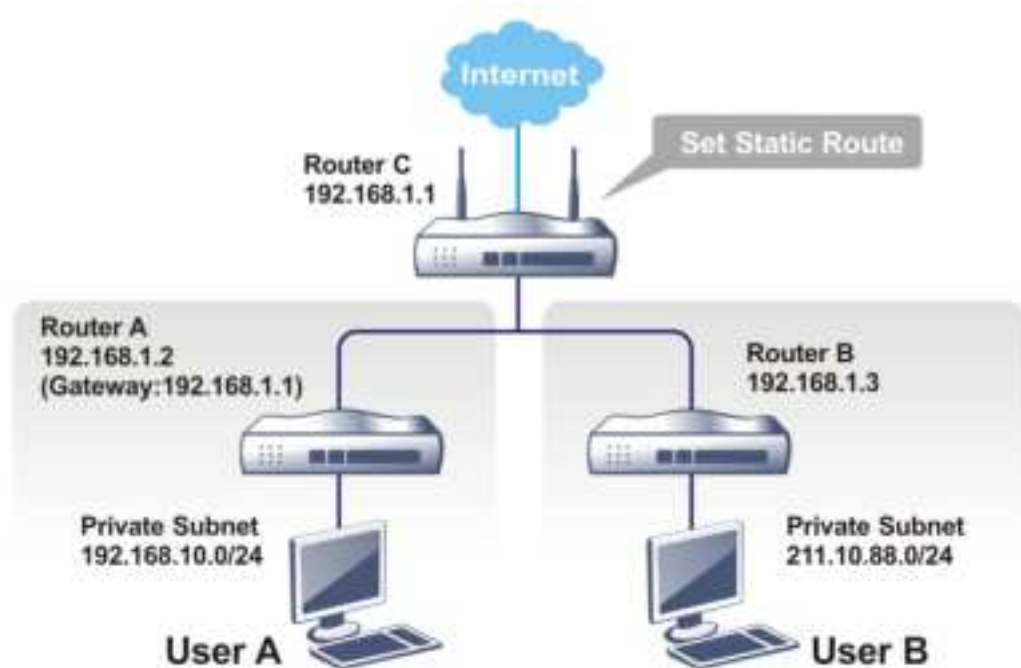
Set to Factory Default	Clear all of the settings and return to factory default settings.
Viewing Routing Table	Displays the routing table for your reference. 
Index	The number (1 to 40) under Index allows you to open next page to set up static route.
Enable	Enables or disables the static route.
Destination Address	Beginning destination address.
Mask	Subnet mask of the destination address.
Gateway	IP address of the gateway, which is the host that the traffic needs to go through to reach the destination.
Interface	The LAN or WAN that should be used to contact the gateway.
Backup	Click it to backup the configuration of static route settings.
Restore	Click it to restore the configuration of static route settings. Before clicking, make sure upload the configuration file onto Vigor router.

Add Static Routes to Private and Public Networks

Here is an example (based on IPv4) of setting Static Route in Main Router so that user A and B locating in different subnet can talk to each other via the router. Assuming the Internet access has been configured and the router works properly:

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

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



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



Info

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

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

Routing >> Static Route Setup

Index No. 1

☒ Enable	
Destination IP Address	192.168.10.0
Subnet Mask	255.255.255.252
Gateway IP Address	192.168.1.2
Network Interface	LAN1

Note:

WAN4, WAN5, WAN6 are PVGs or VLANs that can be configured on the [Multi-PVC/VLAN](#) page.

OK

Cancel

Delete

Available settings are explained as follows:

Item	Description
Enable	Enables or disables the static route.
Destination IP Address	Beginning destination address. Enter an IP address as the destination of the static route.
Subnet Mask	Subnet mask of the destination address. Enter the subnet mask for the static route.
Gateway IP Address	Enter the IP address of the gateway, which is the host that the traffic needs to go through to reach the destination.
Network Interface	Use the drop down list to specify an interface for such static route. The LAN or WAN that should be used to contact the gateway.

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

Routing >> Static Route Setup

Index No. 2

☒ Enable	
Destination IP Address	211.100.88.0
Subnet Mask	255.255.255.252
Gateway IP Address	192.168.1.3
Network Interface	LAN1

Note:

WAN4, WAN5, WAN6 are PVGs or VLANs that can be configured on the [Multi-PVC/VLAN](#) page.

OK

Cancel

Delete

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

Diagnostics >> View Routing Table

IPv4 Routing Table						Refresh
Key	Destination	Gateway	Interface			
C	192.168.18.0/255.255.255.255	vsw 192.168.1.2	LAN1			
C	192.168.1.0/255.255.255.0	directly connected	LAN1			
C	192.168.80.0/255.255.255.255	vsw 192.168.1.2	LAN1			

Key
C Connected S Static R RIP * default + private

II-5-1-2 Static Route for IPv6

You can set up to 40 profiles for IPv6 static route. Click on a route index on the IPv6 tab to configure an IPv6 static route.

Routing >> Static Route Setup

IPv4		IPv6		Set to Factory Default	View IPv6 Routing Table
Index	Enable	Destination Address	Gateway	Interface	
1	☐				
2	☐				
3	☐				
4	☐				
5	☐				
6	☐				
7	☐				
8	☐				
9	☐				
10	☐				
11	☐				
12	☐				
13	☐				
14	☐				
15	☐				
16	☐				
17	☐				
18	☐				
19	☐				
20	☐				
21	☐				
22	☐				
23	☐				
24	☐				
25	☐				
26	☐				
27	☐				
28	☐				
29	☐				
30	☐				
31	☐				
32	☐				
33	☐				
34	☐				
35	☐				
36	☐				
37	☐				
38	☐				
39	☐				
40	☐				

Available settings are explained as follows:

Item	Description
Index	The number (1 to 40) under Index allows you to open next page to set up static route.
Enable	Enables or disables the static route.
Destination Address	Beginning destination address.
Gateway	IP address of the gateway, which is the host that the traffic needs to go through to reach the destination.
Interface	The LAN or WAN that should be used to contact the gateway.
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.
Backup	Click it to backup the configuration of static route settings.
Restore	Click it to restore the configuration of static route settings. Before clicking, make sure upload the configuration file onto Vigor router.

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

[Routing >> 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	Enables or disables the static route.
Destination IPv6 Address / Prefix Len	Beginning destination address and the number of bits in the subnet mask of the destination IPv6 address. Enter the IP address with the prefix length for this entry.
Gateway IPv6 Address	IP address of the gateway, which is the host that the traffic needs to go through to reach the destination.
Network Interface	The LAN or WAN that should be used to contact the gateway.

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

II-5-2 Route Policy

The Route Policy feature gives you control over how different types of outbound traffic are routed, through any of the LANs, WANs or VPNs. To add, delete or modify load balance or route policies, select **Routing >> Route Policy** from the menu bar.

Routing >> Route Policy ?

Route Policy 10 rules per page | Set to Factory Default | Diagnose

Index	Enable	Comment	Protocol	Interface	Priority	Source	Destination	Dest Port	Move Up	Move Down
1	☐		Any	WAN1	200	Any	Any	Any		
2	☐		Any	WAN1	200	Any	Any	Any	UP	Down
3	☐		Any	WAN1	200	Any	Any	Any	UP	Down
4	☐		Any	WAN1	200	Any	Any	Any	UP	Down
5	☐		Any	WAN1	200	Any	Any	Any	UP	Down
6	☐		Any	WAN1	200	Any	Any	Any	UP	Down
7	☐		Any	WAN1	200	Any	Any	Any	UP	Down
8	☐		Any	WAN1	200	Any	Any	Any	UP	Down
9	☐		Any	WAN1	200	Any	Any	Any	UP	Down
10	☐		Any	WAN1	200	Any	Any	Any	UP	Down

<< 1-10 | 11-20 | 21-30 >> 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
Rules per page	The number of rules to display on a single page.
Set to Factory Default	Clear the settings of all Load-Balance and Route Policy rules.
Index	Rule index. Click to bring up the configuration page of the rule.
Enable	Select to enable this rule.
Protocol	Protocol(s) to which this rule applies.
Interface	LAN, IP Routed Subnet, WAN or VPN interface that the traffic described by this rule is to be directed.
Priority	The priority of this rule.
Source	The source IP address.
Destination	The destination IP address.
Move UP/Move Down	Click to shift priority of rule up/down by one.
Wizard Mode	The setup wizard will present the most-commonly used rule settings in three steps.
Advance Mode	All the rule settings will be shown on one configuration page.

If Wizard Mode is selected, you will be guided through the configuration process in three steps. Only the most commonly used settings will be shown.

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

Routing >> Route Policy

Index: 1 Criteria

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

Source IP ☒ Any
☐ Src IP Start - Src IP End

Destination IP ☒ Any
☐ Dest IP Start - Dest IP End
☐ Country Object

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
Source IP	Source IP addresses to which this rule is to be applied. Any - This rule applies to all source IP addresses. Src IP Start, Src IP End - This rule applies to the specified range of source IP addresses. If there is only one source IP address, enter the address in both the Start and End fields.
Destination IP	Destination IP addresses to which this rule is to be applied. Any - This rule applies to all destination IP addresses. Dest IP Start, Dest IP End - This rule applies to the specified range of destination IP addresses. If there is only one destination IP address, enter the address in both the Start and End fields. 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.

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

Routing >> Route Policy

Index: 1 Interface

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

Interface

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
Interface	You can select an interface from one of the following: WAN, LAN, VPN, IP Routed Subnet, and DMZ Subnet. Packets match with the above criteria will be transferred to the interface chosen here. Select an interface from the list.

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

Routing >> Route Policy

Index: 1 NAT or Routing

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

The current setting is:

☒ Force NAT
☐ Force Routing

< Back Next > Finish Cancel

Available settings are explained as follows:

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

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

Routing >> Route Policy

Index: 1 Configuration Summary

Criteria

Source IP: Any

Destination IP: Any

Interface

WAN1

More options

Force NAT

< Back Next > Finish Cancel

- If there is no error, click **Finish** to complete wizard setting. To make changes, click **Back** to return to the previous pages. To discard all changes, click **Cancel**.

Routing >> Route Policy

Route Policy

10 rules per page Set to Factory Default Diagnose

Index	Enable	Comment	Protocol	Interface	Priority	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End	Move Up	Move Down
1	☒		Any	WAN1	200	Any	Any	Any	Any	Any	Any		Down
2	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	Up	Down
3	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	Up	Down
4	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	Up	Down
5	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	Up	Down
6	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	Up	Down
7	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	Up	Down
8	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	Up	Down
9	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	Up	Down
10	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	Up	Down

<< 1 10 11 20 21 30 >>

Next >>

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

OK

If **Advance Mode** is selected, you will be presented with a single page with all the configurable settings for the rule.

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

Routing >> Route Policy

Index: 1

☒ Enable

Comment: Delete

Criteria

Protocol:

Source:

Destination:

Destination Port:

Send via If Criteria Matched

Interface:

☒ WAN/LAN
☐ VPN

Gateway:

☒ Default Gateway
 ☐ Specific Gateway

Packet Forwarding to WAN/LAN via:

☒ Force NAT
 ☐ Fine Routing

Forward to:

☒ WAN/LAN
☐ VPN
☐ Route Policy

Gateway:

☒ Default Gateway
 ☐ Specific Gateway

☐ Priority

OK Clear Cancel Diagnose

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	Select to enable rule and unlock all fields for configuration.
Comment	Type a brief explanation for such profile.
Criteria	Router examines outgoing LAN traffic to find the first rule whose criteria are satisfied. Protocol - Use the drop-down menu to choose a proper protocol for the WAN interface. Source - Source IP addresses to which this rule is to be applied. • Any - This rule applies to all source IP addresses. • IP Range - This rule applies to the specified range of source IP addresses. - Start - Enter an address as the starting IP for such profile. - End - Enter an address as the ending IP for such profile. • IP Subnet - This rule applies to source IP addresses

	defined by the specified network IP address and subnet mask. - Network - Enter an IP address here. - Mask - Use the drop down list to choose a suitable mask for the network. ● IP Object / IP Group - Use the drop down list to choose a preconfigured IP object/group. Destination - Destination IP addresses to which this rule is to be applied. ● Any - This rule applies to all source IP addresses. ● IP Range - This rule applies to the specified range of destination IP addresses. - Start - Enter an address as the starting IP for such profile. - End - Enter an address as the ending IP for such profile. ● IP Subnet - This rule applies to destination IP addresses defined by the specified network IP address and subnet mask. - Network - Enter an IP address here. - Mask - Use the drop down list to choose a suitable mask for the network. ● Domain Name - Specify a domain name as the destination. - 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. ● IP Object / IP Group - Use the drop down list to choose a preconfigured IP object/group. ● 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. Destination Port - Destination port numbers to which this rule is to be applied. As only TCP and UDP protocols use port numbers, this setting does not apply to the ICMP protocol. ● Any - This rule applies to all destination ports. ● Dest Port Range - This rule applies to the specified range of destination ports. - Start - Enter the destination port start for the destination IP. - End - Enter the destination port end for the destination IP. If this field is blank, it means that all the destination ports will be passed through the WAN interface.
Send to if criteria matched	If criteria are matched, the traffic will be sent to the designated interface and gateway. Interface - Packets match with the above criteria will be transferred to the interface chosen here. Select an interface from the list (WAN/LAN: A WAN or LAN interface; VPN: A Virtual Private Network). Gateway IP - Select a gateway. ● Default Gateway - Traffic will be sent to the default

	gateway address of the specified interface. ● Specific Gateway - Traffic will be sent to the specified gateway address instead of the default gateway address. Packet Forwarding to WAN/LAN via - When you choose LAN/WAN (e.g., WAN1) as the Interface for packet transmission, you have to specify the way the packet forwarded to. ● Force NAT - The source IP address will not be used to connect to the remote destination. Network Address Translation (NAT) will be used, where a common IP address will be used. ● Force Routing - The source IP address will be preserved when connecting to the remote destination. Failover to - If the interface specified above loses connection, traffic can be forwarded to an alternate interface or be scrutinized by an alternate route policy. ● 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 - The failed-over traffic can be sent to the Default Gateway of the alternate interface/route policy, or a Specific Gateway at the specified IP address.
Priority	Specifies the priority of the rule in relation to other rules. Lowering the priority value increases the priority of the rule, and vice versa. Routes in the routing table have a priority value of 150, whereas the default routes have a priority value of 250. The default priority value of Load Balance/Route Policy rules is 200. To change the priority, move the slider or enter a value.

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

Diagnose for Route Policy

The Diagnose function allows you to determine how a specific type of traffic from a host to a destination will be routed, and which routes, route policies and load balance rules match the criteria of the traffic.

Click **Diagnose**.

Analyze a single packet

Select this mode to make Vigor router analyze how a single packet will be sent by a route policy.

Diagnosics >> 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	Any	▼
Src IP	Specify an IP	▼
		192.168.1.2
Dst IP	Specify an IP	▼
		8.8.8.8
Dst Port	Any Port	▼

Analyze

Analysis

Available settings are explained as follows:

Item	Description
Packet Information	Specify the nature of the packets to be analyzed by Vigor router. Protocol - Specify a protocol for diagnosis. Src IP - IP address of host where the traffic originates. ● Specify an IP - One source IP address. ● Any IP - Source IP address is not specified. Any IP from LAN 1/LAN 2/LAN 3/LAN 4/LAN 5/LAN 6/DMZ. ● Subnet/IP Routed Subnet - Any source IP address on the specified subnet. Dst IP - IP address of the destination host. ● Specify an IP - One destination IP address. ● Any IP - Destination IP address is not specified. Dst Port - Number of port to which the traffic is sent. This setting is only applicable to UDP and TCP protocols. Use the drop down list to specify the destination port. Analyze - Click to analyze and display routes, route policies and load balance rules with matching criteria. If required, click export analysis to export the result as a file.

The following shows an analysis example. The packet matched the criteria of one route policy.

Test how the packets will be routed

Mode ☒ Analyze a single packet
☐ Analyze multiple packets by uploading an input file

Packet Information

Protocol: Any
 Src IP: Specify an IP: 192.168.1.2
 Dst IP: Specify an IP: 0.0.0.0
 Dst Port: Any Port

Analyze

Analysis



The packet was dropped because the send to interface of the matched policy "policy 1" was inactive and there was no follow setting.

Matched Route

Matched	Priority
N/A	N/A

Matched Policy

Matched	Priority	Followed
Route Policy 1	500	No

Analyze multiple packets by uploading an input file

Diagnostic >> Route Policy Diagnostic



Test how the packets will be routed

Mode ☐ Analyze a single packet
☒ Analyze multiple packets by uploading an input file

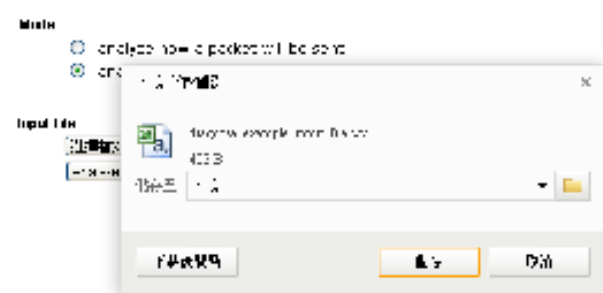
Input File

Upload file

(download an example input file)

Analyze

Available settings are explained as follows:

Item	Description
Input File	Browse - Click to browse folder structure and select an input file. Download and example input file - Click to download a sample input file (blank ".csv" file). Then, click the Browse button to select that blank ".csv" file for saving the result of analysis.  Analyze - After selecting input file, click to start the analysis process. Click the export button to export the

result as a file.

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.

The following shows the analysis of the sample input file. The matched routes and policies are highlighted in green. The Final Result column shows the outcome.

Diagnose >> 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:    (download an example input file) 

Analysis 

Input Packet Information				Matched Route		Matched Policy			Final Result		
Priority	Proto	Src IP	Dst IP	Dst Port	Route	Priority	Policy	Priority	Forwarded	Interface	Reason
LA	ICMP	192.168.1.10	10.10.10.10	Any	No Match	N/A	Route Policy 1	200	No	(null)	The packet was dropped because the source interface of the matched policy "policy 1" was inactive and there was no fallback setting.
NY	ICP	192.168.1.20	20.20.20.20	5000	No Match	N/A	Route Policy 1	200	No	(null)	The packet was dropped because the source interface of the matched policy "policy 1" was inactive and there was no fallback setting.
NZ	UDP	192.168.1.20	30.30.30.30	5000	No Match	N/A	Route Policy 1	200	No	(null)	The packet was dropped because the source interface of the matched policy "policy 1" was inactive and there was no fallback setting.
AU	ICMP	192.168.2.1	2.2.2.2	Any	No Match	N/A	Route Policy 1	200	No	(null)	The packet was dropped because the source interface of the matched policy "policy 1" was inactive and there was no fallback setting.
in-200 input											

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

Application Notes

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

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

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

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

Index	Enable	Alias WAN IP
1.	☐	...
2.	☒	172.17.1.1
3.	☐	172.17.1.2
4.	☐	0000
5.	☐	0000
6.	☐	0000
7.	☐	0000
8.	☐	0000

OK Cancel Close

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

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

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

Routing == 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/LAN via: ☒ Force NAT ☐ Force Routing

Failover to: ☒ WAN/LAN ☐ VPN ☐ Route Policy ☐ Gateway

Default WAN: VPN 1.777: Index 1: ☒ Default Gateway ☐ Specific Gateway

☐ Priority

- 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: 192.168.1.20

Destination: Domain Name

percsd.cheyek.com [Select] [Delete]

Add

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

Objects Setting >> String Object

Index	String
1	Floor_1
12	Floor_2
33	sdh3300
34	percsd.cheyek.com
35	Floor_3
36	cheyek.intel.com
37	percsd.cheyek.com
114	Floor_1

percsd.cheyek.com [Select] [Delete]

Add

Destination Port: Any

Serial via IP Criteria: Marshall

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

Criteria

Protocol: Any

Source: IP Range

Start: 192.168.1.20 End: 192.168.1.20

Destination: Domain Name

percsd.cheyek.com [Select] [Add]

percsd.cheyek.com [Select] [Add]

percsd.cheyek.com [Select] [Add]

percsd.cheyek.com [Select] [Add]

percsd.cheyek.com [Select] [Add]

Add to List

Destination Port: Any

Serial via IP Criteria: Marshall

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.

Destination

Domain Name

Set-ID	Name
101	server3.example.com
102	server2.example.com
103	server1.example.com
104	server4.example.com

Destination Port: Any

Send via IP 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

101 102 103 104 105

server3.example.com server2.example.com server1.example.com server4.example.com

Add

This page is left blank.

Part III Wireless LAN



Wireless

Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access.

III-1 Wireless LAN

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

Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The Vigor2765 wireless series router (with “n” in model name) is designed for maximum flexibility and efficiency of a small office/home. Any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access.

Vigor2765 wireless router is a highly integrated wireless local area network (WLAN) for 2.4 GHz 802.11n WLAN applications. Vigor2765 “n / ac” series router supports 802.11n up to 300 Mbps for 40 MHz channel operations.



Info

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

In an Infrastructure Mode of wireless network, Vigor wireless router plays a role as an Access Point (AP) connecting to lots of wireless clients or Stations (STA). All the STAs will share the same Internet connection via Vigor wireless router. The wireless network settings, such as SSID, channels, encryption protocol, can be configured in General Settings.



Multiple SSIDs

Vigor wireless routers support up to four SSIDs (Service Set Identifiers) per band for wireless connections. A service set is a group of wireless network clients that have the same networking parameters. Each service set can be configured to have a unique name (SSID) and specific download and upload rates, and can be used by different categories of users.

Real-time Hardware Encryption

Vigor wireless routers are equipped with a hardware AES encryption engine to provide the most effective and efficient protection of wireless traffic, without sacrificing 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 (PSK) is used to encrypt traffic during data transmission. WPA uses the Temporal Key Integrity Protocol (TKIP) for data encryption whereas WPA2 applies AES (Advanced Encryption Standard). A major advantage of WPA-Enterprise is that it supports not only encryption but also authentication.

You should select the appropriate security mechanism according to your needs. Because WEP has proven to be vulnerable to attacks, you should consider using WPA instead for the most secure connection. 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 default password (PSK) is listed on a label attached to the bottom of the router. Since anyone who has physical access to the router can discover the default password, you are strongly advised to change it.



Separate the Wireless and the Wired LAN- WLAN Isolation

WLAN Isolation allows you to separate wireless LAN clients from wired ones, either for the purpose of quarantining certain users, or restricting their access to LAN resources. When WLAN isolation is enabled on an SSID, its users will only be able to connect to the WAN (i.e., internet). This is ideal for providing visitors Internet access while keeping the wired network secure.

For the highest degree of security, you may consider adding firewall rules to filter access by MAC address.

Manage Wireless Stations - Station List

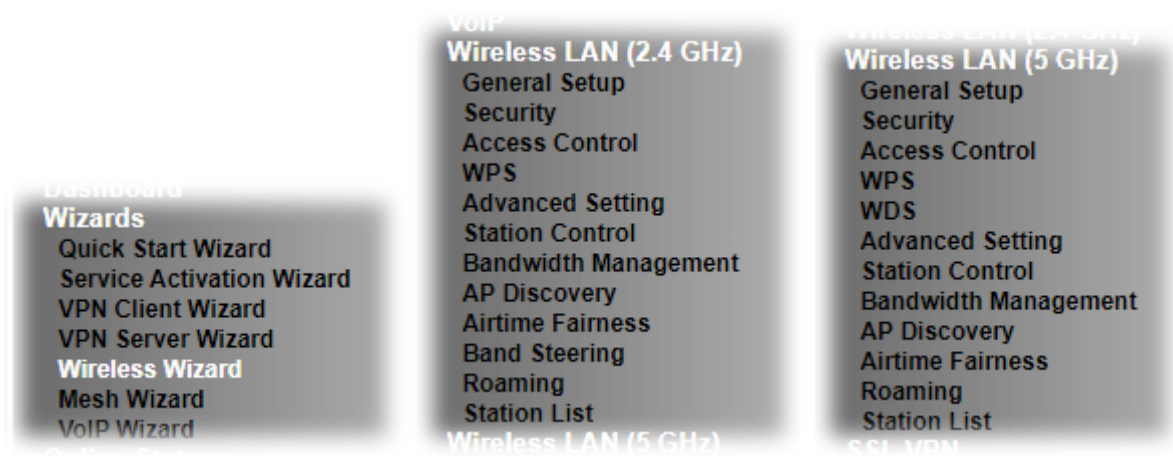
All stations on the wireless network and their connection status is shown here.

WPS

WPS (Wi-Fi Protected Setup) makes connecting wireless clients to wireless access points and routers a simple process.



Web User Interface



III-1-1 Wireless Wizard

On Wi-Fi-equipped models, you can configure the wireless access point (AP) using the Wireless Wizard. The Host AP Configuration sets up SSID 1 for use by internal users, who are allowed to access both the LAN and the WAN (Internet), whereas the Guest AP Configuration sets up SSID 2 for use by visitors, who are allowed only WAN access and whose access speeds can optionally be throttled.

The Wireless Wizard allows you to quickly configure a host SSID (for internal use, such as in a home or business environment), and optionally a guest SSID (for wireless clients that are restricted to Internet access only, typically used by visitors).

1. On the menu bar, click on **Wizards**, and then **Wireless Wizard**.
2. The Host AP Configuration page appears. This page sets up SSID 1 for use by internal users. SSID 1 configured using the wizard will have no access speed throttling (by means of the Rate Control feature), and both the LAN and the WAN will be accessible.

Wireless Wizard

Host AP Configuration

Wireless 2.4GHz Settings	
Name	DrayTek
Mode	Mixed (11b+11g+11n) ▼
Channel	Channel 6, 2437MHz ▼
Security Key	
Wireless 5GHz Settings	
☐ Use the same SSID and Security Key as above	
Name	DrayTek_5G
Mode	Mixed (11a+11n+11ac) ▼
Channel	Channel 36, 5180MHz ▼
Security Key	
Note: The host AP configured here will be used for home or internal company use	

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
Wireless 2.4GHz Settings	
Name	Service Set Identification (SSID), which shows up as the AP identifier. Maximum length is 32 characters.
Mode	Allowed Wi-Fi modes. 802.11b is the original Wi-Fi mode on the 2.4 GHz band and supports raw data rates up to 11 Mbit/s. 802.11g allows for enhanced throughput up to 54 Mbit/s. 802.11n provides throughput up to 300 MHz. Available selections are • 11b Only • 11g Only • 11n Only (2.4 GHz) • Mixed(11b+11g) • Mixed(11g+11n) • Mixed(11b+11g+11n) The selections labeled “Mixed” enable multiple simultaneously-active modes.
Channel	Wi-Fi channel used for this SSID. If set to Auto, the router uses the best available channel.
Security Key	The Pre-shared Key (PSK) used by WPA2/PSK (Wireless Protected Access 2/Pre-shared Key) to encrypt wireless traffic. The key is composed of 8 to 63 ASCII characters. You may also specify the key using 64 hexadecimal digits, prefixed with the sequence 0x (“0x321253abcde...”).
Wireless 5GHz Settings	
Use the same SSID and Security Key as above	If selected, the SSID Name and Security Key from the 2.4 GHz section will be used.
Name	Service Set Identification (SSID), which shows up as the AP identifier. Maximum length is 32 characters.
Mode	Allowed Wi-Fi modes. 802.11a is the original Wi-Fi mode on the 5 GHz band and supports raw data rates up to 11 Mbit/s. 802.11n enhances the throughput and provides up to 300 MHz. The newest standard, 802.11ac, can achieve 1.3 Gbit/s of data throughput on the 5 GHz band. Available selections are • 11a Only • 11n Only (5GHz) • Mixed(11a+11n) • Mixed(11a+11n+11ac) The selections labeled “Mixed” enable multiple simultaneously-active modes.
Channel	Wi-Fi channel used for this SSID. If set to Auto, the router uses the best available channel.
Security Key	The Pre-shared Key (PSK) used by WPA2/PSK (Wireless

	Protected Access 2/Pre-shared Key) to encrypt wireless traffic. The key is composed of 8 to 63 ASCII characters. You may also specify the key using 64 hexadecimal digits, prefixed with the sequence 0x ("0x321253abcde...").
Next	Click it to get into the next setting page.
Cancel	Exit the wireless wizard without saving any changes.

3. Click **Next** to proceed to the Guest AP Configuration page. The Guest AP Configuration page appears. This page sets up SSID 2 for use by guest users. SSID 2 configured using the wizard can optionally be set up with access speed throttling (by means of the Rate Control feature), and only the WAN (the Internet) will be accessible.

SSID 2 shares the same Mode and Channel settings as SSID 1 configured on the previous page.

Wireless Wizard

Guest AP Configuration

Available settings are explained as follows:

Item	Description
Wireless 2.4GHz Settings	
Enable/Disable	Enable or disable the SSID for guest use.
SSID	Service Set Identification (SSID), which shows up as the AP identifier. Maximum length is 32 characters.
Security Key	The Pre-shared Key (PSK) used by WPA2/PSK (Wireless Protected Access 2/Pre-shared Key) to encrypt wireless traffic. The key is composed of 8 to 63 ASCII characters. You may also specify the key using 64 hexadecimal digits, prefixed with the sequence 0x ("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 Enter the transmitting rate for data upload. Default value is 30,000 kbps. Total Download - Enter the transmitting rate for data download. Default value is 30,000 kbps.
Wireless 5GHz Settings	

III-1-2 General Setup

The **Wireless LAN>>General Setup** section lets you configure the most basic settings of your wireless network, including the SSIDs, WLAN channels and bandwidth control.

Wireless LAN(2.4GHz) >> General Setup

General Setting (IEEE 802.11)

☒ **Enable Wireless LAN**

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

Index	Enable	Active	SSID	Hide SSID	Isolate Member	Isolate VPN
1	☒	☒	ProxyTel	☐	☐	☐
2	☐	☐	ProxyTel_Guest	☐	☐	☐
3	☐	☐	Max: 31 characters	☐	☐	☐
4	☐	☐	Max: 31 characters	☐	☐	☐

Schedule

Schedule	Schedule Profile	Apply To
Schedule 1	None	☐ SSID1(A) ☐ SSID2 ☐ SSID3 ☐ SSID4
Schedule 2	None	☐ SSID1(A) ☐ SSID2 ☐ SSID3 ☐ SSID4
Schedule 3	None	☐ SSID1(A) ☐ SSID2 ☐ SSID3 ☐ SSID4
Schedule 4	None	☐ SSID1(A) ☐ SSID2 ☐ SSID3 ☐ SSID4

Note:

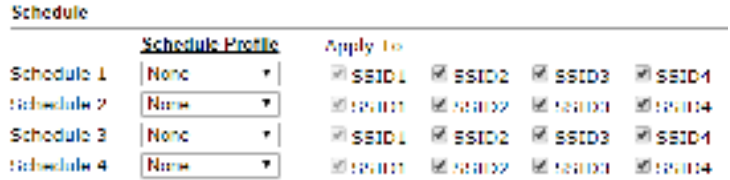
1. Isolate Member: Prevent the clients associated with this SSID from accessing each other.
2. Isolate VPN: Block the wireless clients from accessing the VPN network and prevent wireless traffic being sent to VPN connections.
3. Only the action "Force Down" in the Schedule Profile will be applied to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

OK

Cancel

Available settings are explained as follows:

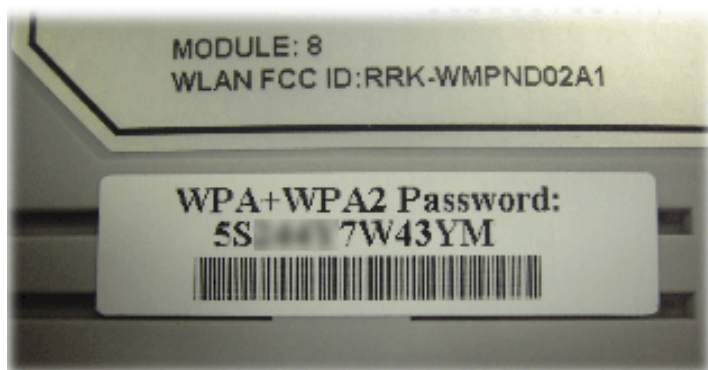
Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Mode	Select the 802.11 mode allowed on the band. On the 2.4 GHz band, the following wireless mode options are available: • 11b Only • 11g Only • 11n Only (2.4 GHz) • Mixed (11b+11g) • Mixed (11g+11n) • Mixed (11b+11g+11n) On the 5 GHz band on ac models (2765ac and 2765Vac), the following options are available: • 11a Only • 11n Only (5 GHz) • Mixed (11a+11n)

	• 11n Only (5 GHz) • Mixed (11a+11n) • Mixed (11a+11n+11ac)
Channel	Allows you to specify a particular wireless channel to use, or let the system determine the optimal channel by selecting “Auto”. The list of available channels varies depending on the locale for which the router is intended.
SSID	Service Set Identification (SSID), which shows up as the AP identifier. Maximum length is 32 characters.
Hide SSID	Select to keep SSIDs from showing up when scans are performed by wireless clients, which makes it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless client and software used, the user may see only an AP listed without the SSID, or the AP might not even show up.
Isolate	Member - Check this box to disallow communication between wireless clients (stations) on the same SSID. VPN - Check this box to block wireless clients (stations) from accessing VPN clients.
Schedule Profile	Set the wireless LAN to be disabled at certain time intervals. You may choose up to 4 schedules out of the 15 schedules defined in Applications >> Schedule . Only “Force Down” schedule profiles take effect, and the wireless function will be turned off for the duration of the profile. The default setting is blank for all schedules, meaning wireless function will always work.
Apply To	Selected SSID (2 /3 /4) will be forced up /down based on the schedule profile used. 

To save changes on the General Settings page, select **OK**; to discard changes, select **Cancel**.

III-1-3 Security

Every router has a default wireless password (PSK) which is provided on a label attached to 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.



For extra security you can set your own wireless password by clicking the **Wireless LAN>>Security** on the Web User Interface. Each of the 4 SSIDs can be configured independently using their own tab page.

Wireless LAN(2.4G Hz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID Mode WPA Encryption Mode Pre-Shared Key(PSK) Password Strength: Note: For strong passwords: WEP Key 1: Key 2: Key 3: Key 4: Note: Drop list WPA2/PSK TKIP for WPA/WEP for WPA2 Weak Medium Strong Type 0-63 ASCII characters, for example: "chgs01a2...". 1. Use at least 12 characters. 2. Include at least 3 of the following 4 types of character: digits, uppercase letters, lowercase letters, and non-alphanumeric characters (such as \$ % ^). 64 Bit Key 1: Key 2: Key 3: Key 4: Please configure the RADIUS Server if WDS is used. For 64 bit WEP key configurations, please insert 5 ASCII characters, for example: "AB312". For 128 bit WEP key configurations, please insert 13 ASCII characters.			
OK Cancel			

Available settings are explained as follows:

Item	Description
Mode	This dialog box lists all available security modes.
	Info
	You should also set RADIUS Server

	simultaneously if 802.1x mode is selected. Disable - Encryption mechanism is disabled. WEP - Allow only connections from WEP clients. Encryption key should be entered in the WEP Key section. WEP/802.1x Only - Accepts only WEP clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol. Allow only connections from WEP clients. Encryption key is obtained from a RADIUS server using the 802.1X protocol. WPA/802.1x Only - Allow only connections from WPA clients. Encryption key is obtained from a RADIUS server using the 802.1X protocol. WPA2/802.1x Only - Allow only connections from WPA2 clients. Encryption key is obtained from a RADIUS server using the 802.1X protocol. Mixed (WPA+WPA2/802.1x only) - Allow connections from both WPA and WPA2 clients. Encryption key is obtained from a RADIUS server using the 802.1X protocol. WPA/PSK - Allow connections only from WPA clients. Encryption key should be entered in the PSK field. WPA2/PSK - Allow connections only from WPA2 clients. Encryption key should be entered in the PSK field. Mixed (WPA+ WPA2)/PSK - Allow connections from both WPA and WPA2 clients. Encryption key should be entered in the PSK field.
WPA	WPA encrypts each frame transmitted from the radio using the key, which is either entered in the PSK (Pre-Shared Key) field, or or automatically negotiated via 802.1x authentication from a RADIUS server. Pre-Shared Key (PSK) - Enter 8-63 ASCII characters, for example, "012345678.." , or 64 hexadecimal digits with a leading "0x", for example, "0x321253abcde...". Password Strength - The system will display the strength of the password, indicated by the words "weak", "medium" or "strong".
WEP	WEP keys can either be 64-bit or 128-bit. 64-Bit - Either 5 ASCII characters, for example "12345", or 10 hexadecimal digitals with a leading "0x", such as "0x4142434445". 128-Bit - Either 13 ASCII characters, for example "ABCDEFGHJKLM", or 26 hexadecimal digits with a leading "0x", for example "0x4142434445464748494A4B4C4D". Up to four keys can be entered here, but only one key can be selected at any time. The keys can be entered in ASCII or Hexadecimal. All wireless devices intending to connect to the same SSID must support the same WEP encryption bit size and have the same key.

To save changes on this page, select **OK**; to discard changes, select **Cancel**.

Comment	Enter a brief description for the specified client's MAC address.
Add	Add a new filter entry to the MAC Address filter list using the information entered above.
Delete	Delete the selected MAC address from the list.
Edit	Update the selected MAC address in the list using the information entered above.
Cancel	Clear the contents of all the above fields. This will discard all changes without saving to the MAC Address Filter list.
OK	Click to save the MAC Address Filter list.
Clear All	Remove all entries from the MAC Address Filter 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.

To save changes on this page, select **OK**.

III-1-5 WPS

WPS (Wi-Fi Protected Setup) provides an easy way to connect wireless to wireless access points and routers with WPA or WPA2 encryption.



Info

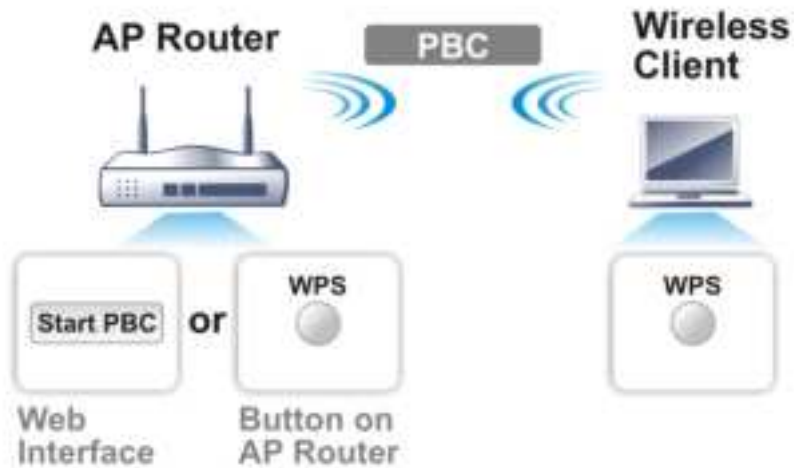
WPS works with wireless stations with WPS or WPS2 support. It does not work with WEP.

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**.

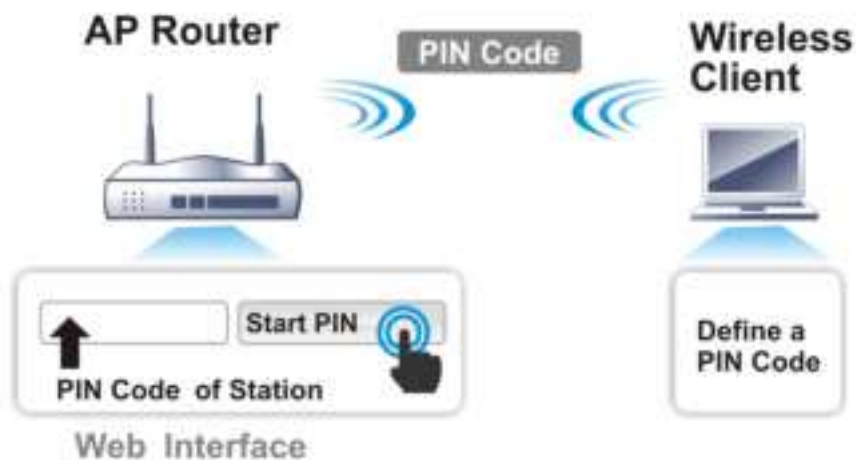
Using the PBC button

On the Vigor router, press and hold the WPS button on the front panel for 2 seconds, or click the **Start PBC** button on the **Wireless LAN>>WPS** page in the Web User Interface. On the wireless station (for example, a laptop computer), press the **WPS Start PBC** button on the network card.

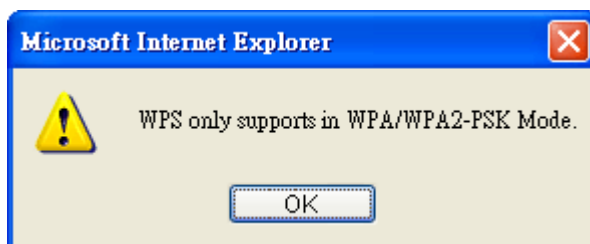


Using a PIN code

You may establish a wireless connection by entering a PIN code generated by a wireless client that supports WPS.



WPS is only supported when the encryption protocol is set to WPA-PSK or WPA2-PSK. If other protocols (such as WEP) have been selected in **Wireless LAN>>Security**, you will see the following message box:



Please click **OK** to dismiss dialog box, return to **Wireless LAN>>Security** and select WPA-PSK or WPA2-PSK mode before attempting to enable 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	BrayTek
Authentication Mode	WPA2WPAK

Device Configure

Configure via Push Button	Start PBC
Configure via Client PinCode	Start PIN

Status: Ready

Notes:

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	Displays system information related to WPS. The message “Configured” means that the wireless security (encryption) function of the router is properly configured and functioning properly.
SSID	Displays the SSID1. WPS is supported on SSID1 only.
Authentication Mode	Displays the current authentication mode of the router.
Configure via Push Button	Click Start PBC to invoke Push-Button style WPS setup procedure. The router will wait for about 2 minutes for WPS connection requests from wireless clients. The WPS LED on the router will blink fast when WPS is in progress, and will return to normal condition after two minutes.
Configure via Client PinCode	Enter a PIN code, and click the Start PIN button. The WPS LED on the router will blink rapidly when WPS is in progress, for up to 2 minutes or until a successful WPS connection from a wireless client has been established.

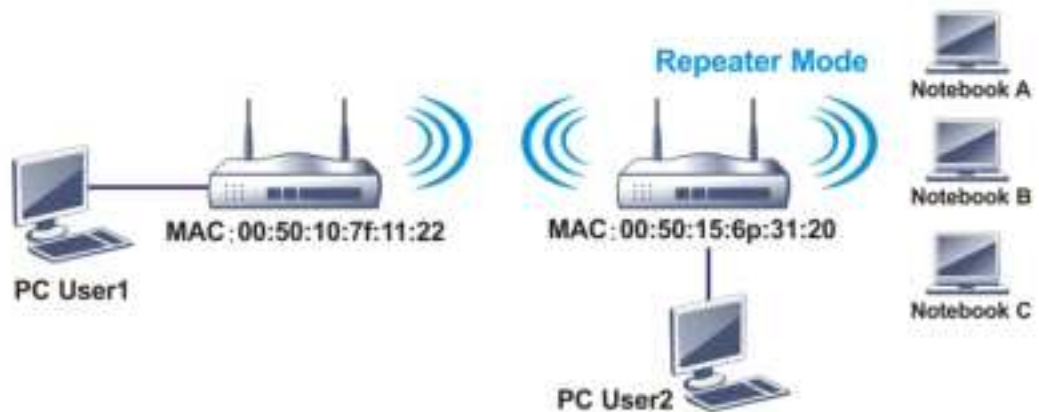
III-1-6 WDS (for WLAN 5 GHz)

Wireless Distribution System (WDS) is a protocol for linking access points (AP) wirelessly. WDS supports two modes:

- **Bridge mode**, which bridges traffic between two LANs wirelessly.



- **Repeater mode**, which extends the coverage range of a WLAN.



The main difference between these two modes is that, in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links, whereas 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 example, 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.

WDS Settings
| [Set to Factory Default](#) |

Mode: Disable ▾ Security ☒ Disable ☐ WEP ☐ Pre-shared Key WEP: Use the same WEP key set in Security Settings. Pre-shared Key: Type: ☐ WPA ☒ WPA2 Key: Max 63 characters Note: WPA and WPA2 are not compatible with EasyTek WPA. Type 8~63 ASCII characters, for example: 1qaz!@x2	Repeater Enable Peer MAC Address ☐ : : : : : : ☐ : : : : : : ☐ : : : : : : ☐ : : : : : : Access Point Function: ☒ Enable ☐ Disable Status: ☐ Send "Hello" message to peers Link Status Note: The status is valid only when the peer also supports this function.

OK
Cancel

Available settings are explained as follows:

Item	Description
Mode	Choose the WDS mode. Disable - WDS is disabled. Repeater - WDS is enabled in Repeater mode.
Security	Choose one of the types for the router. The setting you choose here will make the following WEP or Pre-shared key field valid or not. Disable - Security is disabled. WEP - Security is enabled. Pre-shared key - Security is enabled.
Pre-shared Key	Type - Select either WPA or WPA2 as the encryption protocol. Key - Enter 8 ~ 63 ASCII characters or 64 hexadecimal digits with a leading "0x".
Repeater	If Repeater was selected as the WDS mode, enter the peer MAC addresses in these fields. Up to four peer MAC addresses may be entered in this page. Select the checkbox in front of a MAC address to enable it.
Access Point Function	Select Enable to make this router serve as an access point; select Disable to disable access point function.
Status	Click to send a "hello" message to peers. This only works if the peer also supports this function.

To save changes on this page, select **OK**; to discard changes, select **Cancel**.

III-1-7 Advanced Setting

On this page you can configure advanced settings such as operation mode, channel bandwidth, guard interval, and aggregation MSDU for wireless data transmission.

If the Vigor router supports dual-band WLAN, you will see separate Advanced Setting sections for 2.4GHz and 5GHz.

2.4 GHz Advanced Setting page

Wireless LAN(2.4GHz) >> Advanced Setting

HT Physical Mode

Operation Mode	☒ Mixed Mode ☐ Green Field
Channel Bandwidth	☐ 20 ☒ 20MHz ☐ 40
Guard Interval	☐ long ☒ auto
Aggregation MSDU(A-MSDU)	☒ Enable ☐ Disable
Long Preamble	☐ Enable ☒ Disable
Packets-OverDrive™ TX Boost	☐ Enable ☒ Disable
Antenna	☒ 212R ☐ 111R
Tx Power	☒ 100% ☐ 80% ☐ 60% ☐ 30% ☐ 20% ☐ 10%
WMM Capable	☒ Enable ☐ Disable
APSD Capable	☐ Enable ☒ Disable
Rate Adaptation Algorithm	☒ New ☐ Old
Fragment Length (256 ~ 2346)	2346 bytes
RTS Threshold (1 ~ 2347)	2347 bytes
Country Code	(Reference)
Isolate 2.4GHz and 5GHz bands	☒ Enable ☐ Disable

OK

5 GHz Advanced Setting page

Wireless LAN(5GHz) >> Advanced Setting

Physical Mode

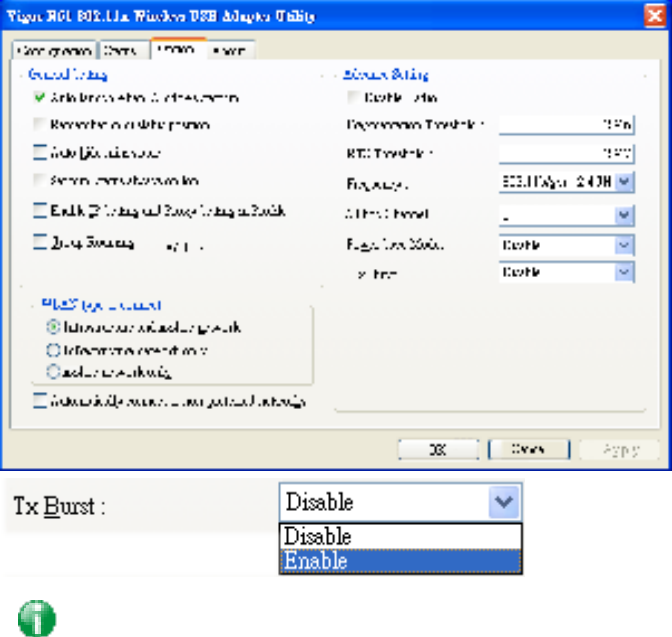
Operation Mode	☒ Mixed Mode ☐ Green Field
Channel Bandwidth	☐ 20 ☐ 20MHz ☒ 20/40/80
Guard Interval	☐ long ☒ auto
Aggregation MSDU(A-MSDU)	☒ Enable ☐ Disable
Tx Power	☒ 100% ☐ 80% ☐ 60% ☐ 30% ☐ 20% ☐ 10%
WMM Capable	☒ Enable ☐ Disable
APSD Capable	☐ Enable ☒ Disable
RTS Threshold (1 ~ 2347)	2347 bytes
Country Code	(Reference)
Isolate 2.4GHz and 5GHz bands	☒ Enable ☐ Disable

OK

Available settings are explained as follows:

Item	Description
Operation Mode	Mixed Mode - The router can transmit data using all protocols supported by 802.11a/b/g and 802.11n standards.

	However, all wireless transmissions will be slowed down when any 802.11g or 802.11b wireless client is connected. Green Field - Select this mode to achieve the highest throughput. This mode supports data transmission between 802.11n systems only. In addition, it does not have protection mechanism to prevent conflicts with neighboring 802.11a/b/g devices.
Channel Bandwidth	20 -Vigor Router will utilize 20 MHz channels for data transmission and reception between the AP and wireless stations. 40 -Vigor Router will utilize 40 MHz for data transmission and reception between the AP and wireless stations. 20/40 - Vigor Router will utilize either 20 MHz or 40 MHz for data transmission and reception depending on the number of nearby wireless APs. 20MHz will be used when there are more than 10 wireless APs; otherwise 40MHz will be used. Selecting this setting ensures the best performance for data transit on networks with both 20 MHz and 40 MHz clients.
Guard Interval	Enabling this setting ensures the integrity of wireless traffic by inserting guard intervals between symbols to reduce the adverse effects of propagation delays, and signal multipath or reflections. If you choose auto as guard interval, the router will choose short guard interval (which increases wireless performance) or long guard interval for data transmit depending on the station capability.
Aggregation MSDU (A-MSDU)	Aggregation MSDU can combine frames of different sizes to improve performance at the MAC layer for clients from certain manufacturers. The default setting is Enable.
Long Preamble	This option determines the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync fields which yield better transmission speeds. However, some older 802.11b wireless devices only support long preamble which uses 128-bit sync fields. Click Enable to use Long Preamble to maintain compatibility with these devices.
Packet-OVERDRIVE	This feature can enhance the performance in data transmission about 40%* (by checking Tx Burst). It is active only when both the Access Point and Station (in wireless client) support and invoke this function at the same time. Note: Vigor N61 wireless adapter supports this function. Therefore, you can install it on your PC to take advantage of Packet-OVERDRIVE (Refer to the following picture of Vigor N61 wireless utility window: choose Enable for TxBURST on the Option tab).

	 Info * the real transmission rate depends on the environment of the network.
Antenna	Vigor router can be attached with two antennas to have good data transmission via wireless connection. However, if you have only one antenna attached, please choose 1T1R.
TX Power	Sets the power percentage of the access point's transmission signal. The greater the TX Power value, the higher intensity of the signal will be.
WMM Capable	WMM stands for Wi-Fi Multimedia. It provides basic Quality of Service (QoS) by prioritizing traffic based on four access categories defined in the IEEE 802.11e standard. The access categories are AC_VO, AC_VI, AC_BE and AC_BK, which corresponds to traffic types of voice, video, best effort and low priority (background) data, respectively. To apply WMM parameters to wireless data transmission, click the Enable radio button.
APSD Capable	APSD (Automatic Power-Save Delivery) is an enhancement over the power-saving mechanisms supported by Wi-Fi networks. It allows access points to buffer traffic before transmitting it to wireless devices, thus allowing wireless devices to enter into power saving mode which reduces power consumption. Not all wireless clients support APSD properly, and the only way to find out if APSD is appropriate for your network is to experiment. The default setting is Disable.
Rate Adaptation Algorithm	Wireless transmission rate is adapted dynamically. Usually, performance of "new" algorithm is better than "old". Sets the way the Wireless transmission rate is adjusted dynamically. In most cases, selecting "New" will result in better performance than "Old".
Fragment Length (256 – 2346)	Set the Fragment threshold. You are advised to leave the default value, 2346, untouched.

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. Adjusts the 802.11 maximum transmit frame size, which might reduce chances of collision with hidden stations. You are advised to leave the default value, 2347, untouched.
Country Code	Vigor router broadcasts country codes according to the 802.11d standard. However, some wireless stations will detect/scan access points looking for country codes to determine which country it is in, and utilize channels appropriate to the country. The wireless client might get confused if there are multiple access points in the vicinity broadcasting different country codes. In such cases, it might be necessary to change the country code of the access point to ensure these clients can successfully establish a wireless connection.
Isolate 2.4GHz and 5GHz bands	The default setting is "Enable". It means that the wireless client using 2.4GHz band is unable to connect to the wireless client with 5GHz band, and vice versa. For WLAN 2.4GHz and 5GHz set with the same SSID name: ● No matter such function is enabled or disabled, clients using WLAN 2.4GHz and 5GHz can communicate for each other if Isolate Member (in Wireless LAN>>General Setup) is NOT enabled for such SSID. ● Yet, if the function of Isolate Member (in Wireless LAN>>General Setup) is enabled for such SSID, clients using WLAN 2.4GHz and 5GHz will be unable to communicate with each other.

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 that the wireless client can connect to the Vigor router. If this function is disabled, wireless clients can connect to the router as long as the router is powered on and the wireless feature is enabled.

This feature is especially useful for free WiFi service. For example, a coffee shop may offer free Wi-Fi service to its guests for one hour every day. In this scenario, the connection time can be set to “1 hour” and reconnection time set to “1 day”. In this way, every guest can surf the net for at most one hour, thus freeing up resources for other guests.

Wireless LAN(2.4GHz) > Station Control

SSID 1	SSID 2	SSID 3	SSID 4
SSID			
Enable ☐			
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).

Available settings are explained as follows:

Item	Description
SSID	Display the selected SSID.
Enable	Select to enable station control function for this SSID.
Connection Time / Reconnection Time	In the Connection Time dropdown box, select the maximum amount of time that a wireless client is allowed to connect within the period of time selected in the Reconnection Time dropdown box. Select User defined to manually enter the time in days, hours and minutes.
Display All Station Control List	Click to display all wireless clients that are under Station Control.
Hotspot Web Portal	Click to jump to the Hotspot Web Portal page.

To save changes on this page, select **OK**; to discard changes, select **Cancel**.

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(2.4G Hz) >> Bandwidth Management

SSID 1	SSID 2	SSID 3	SSID 4
SSID:		Dragonick	
Enable		☒	
Bandwidth Limit Type		Auto Adjustment v	
Total Upload Limit(Kbps)		10000	
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 Vigor2765.
Total Download Limit	It is available when Auto Adjustment is selected. Type a value to define the maximum data clientstations connecting to Vigor2765.
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 Vigor2765.
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 Vigor2765.

To save changes on this page, select **OK**; to discard changes, select **Cancel**.

III-1-10 AP Discovery

Vigor router can scan all regulatory channels to find working APs in the neighborhood. The scanning result can be used to determine the most desirable channel to use, or to locate an AP for establishing a WDS link. Note that during the scanning process (about 5 seconds), no client is allowed to connect to the Vigor. Only APs operating on the same band as the Vigor can be discovered.

Click the **Scan** button to start the AP discovery process.

Wireless LAN(2.4GHz) >> Access Point Discovery

Access Point List

Index	BSSID	Channel	RSSI	SSID	Authentication
See Statistics. Scan					

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	Click to start the AP discovery process. The results will be shown on the box above this button.
Statistics	Shows channel usage by the neighboring APs. Wireless LAN(2.4GHz) >> Statistics Channel usage by neighboring APs AP Number, Channel Channel Cancel

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.

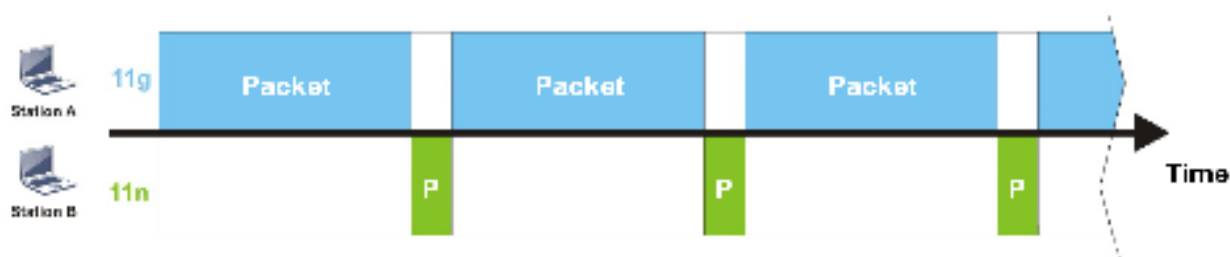
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

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, there are 2 wireless stations on the wireless network, Station A (11g) and Station B (11n), both of which transmit data packets to the Vigor router. Even though they have equal opportunity to access the wireless channel, Station B (11n) gets only a little airtime and waits too much because Station A (11g) takes longer to send one packet. In other words, transmission from Station B (fast rate) is effectively being throttled by Station A (slow rate).



To alleviate this problem, Airtime Fairness tries to assign *similar airtime* to each station (A and B) by controlling TX traffic. In the following figure, Station B (11n) has higher opportunities to send data packets than Station A (11g). In this way, Station B (fast rate) gets its fair share of airtime and its speed is not limited by Station A (slow rate).



This is similar to automatic Bandwidth Limit, where the dynamic bandwidth limit of each station depends on instant active station number and airtime assignment. Please note that Airtime Fairness of 2.4 GHz and 5 GHz bands are independent, but stations connected to different SSIDs on the same band are prioritized as a group, because they all use the same wireless channel. Under certain environments, this function can reduce the adverse effects of slow wireless devices and improve the overall wireless performance.

Environments that can benefit by applying airtime fairness:

- (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

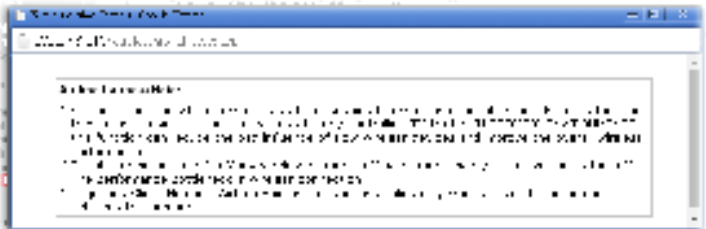
Triggering Client Number (2 ~ 64) (Default: 2)

Note:

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

OK Cancel

Available settings are explained as follows:

Item	Description
Enable Airtime Fairness	Try to assign similar airtime to each wireless station by controlling TX traffic. Airtime Fairness - Click the link to display the following explanation of airtime fairness note.  Triggering Client Number – Airtime Fairness function is applied only when there are at least this many active wireless stations.

To save changes on this page, select **OK**; to discard changes, select **Cancel**.



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 keep the 2.4 GHz band clear for legacy clients, and improves users' experience by reducing 2.4 GHz channel utilization.



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



Info

For Band Steering to work properly, the same SSID and security settings must be configured on both 2.4 GHz and 5 GHz bands.

To configure Band Steering, go to the **Wireless LAN (2.4GHz)>>Band Steering** page:

Wireless LAN(2.4GHz)>>Band Steering

☐ Enable Band Steering
Check Time for WLAN Client 5G Capability: 15 seconds (1 ~ 60) (Default: 15)

Note:

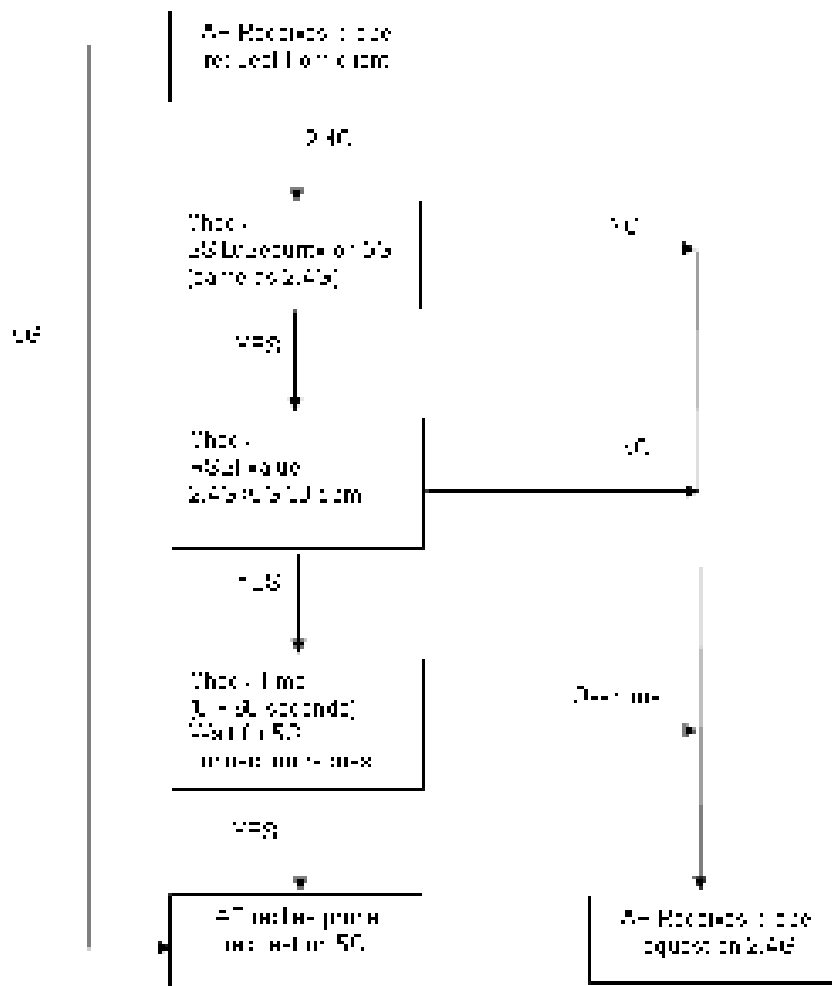
Please setup at least one pair of 2.4GHz and 5GHz Wireless LAN with the same SSID and security.

Available settings are explained as follows:

Item	Description
Enable Band Steering	When enabled, the router will detect if wireless clients are capable of dual-band or not within the time limit. Check Time... - When a wireless client attempts to connect, the router will block attempts to connect to the 2.4 GHz band for the specified period of time (default is 30 seconds), which hopefully will entice the client to connect to the 5 GHz band. If the client fails to connect to the 5 GHz band within the specified interval, it will then be able to connect to the 2.4 GHz band.

To save changes on this page, select **OK**; to discard changes, select **Cancel**.

Below shows how Band Steering works.



Example: 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	15 seconds(s) (1 ~ 60) (Default: 15)

Notes:

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

OK

Cancel

3. Click **OK** to save the settings.
4. Open **Wireless LAN (2.4GHz)>>General Setup** and **Wireless LAN (5GHz)>> General Setup**. Configure SSID as *DrayTek2765_BandSteering* for both pages. Click **OK** to save the settings.

Wireless LAN(2.4GHz)>>General Setup

General Setting (11LL 802.11)

☒ Enable Wireless LAN

Radio

Mode: Mixed(11b+11g+11n) v

Channel: Channel 6, 2437MHz v

SSID

Index	Enable	Active	SSID	Hide SSID	Isolate Member	Isolate VPN
1	☒	☒	DryTel2765_BandSteering	☒	☐	☐
2	☐	☐	DryTel2765_Guest	☐	☐	☐
3	☐	☐	Max: 31 characters	☐	☐	☐
4	☐	☐	Max: 31 characters	☐	☐	☐

Wireless LAN(5GHz)>>General Setup

General Setting (11FF 802.11)

☒ Enable Wireless LAN

Radio

Mode: Mixed(11a+11n+11ac) v

Channel: Channel 36, 5180MHz v

SSID

Index	Enable	Active	SSID	Hide SSID	Isolate Member	Isolate VPN
1	☒	☒	DryTel2765_BandSteering	☒	☐	☐
2	☐	☐	DryTel2765_Guest	☐	☐	☐
3	☐	☐	Max: 31 characters	☐	☐	☐
4	☐	☐	Max: 31 characters	☐	☐	☐

Same value
for 2.4GHz
and 5GHz

5. 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
SSID	DryTel2765_BandSteering		
Mode	WPA2/PSK v		
WPA	Encryption Mode Pre-Shared Key(PSK): TKIP for WPA/AES for WPA2 ----- Weak Medium Strong		
Note: Type U-63 ASCII characters, for example: Telg01a2... 1. For strong passwords: 1. Use at least 12 characters. 2. Include at least 3 of the following 4 types of characters: digits, uppercase letters, lowercase letters, and non-alphanumeric characters (such as !@#\$%^&*).			

Same value
for 2.4GHz
and 5GHz

Wireless LAN(5GHz)>>Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID	DryTel2765_BandSteering		
Mode	WPA2/PSK v		
WPA	Encryption Mode Pre-Shared Key(PSK): TKIP for WPA/AES for WPA2 ----- Weak Medium Strong		
Note: Type U-63 ASCII characters, for example: Telg01a2... 1. For strong passwords: 1. Use at least 12 characters. 2. Include at least 3 of the following 4 types of characters: digits, uppercase letters, lowercase letters, and non-alphanumeric characters (such as !@#\$%^&*).			

6. The Vigor will now steer wireless clients to the less congested wireless band, such as 5GHz to reduce network congestion.

III-1-13 Roaming

WiFi roaming allows wireless stations to switch connections between access points within an area to achieve better coverage and signal quality. It usually is up to the wireless station to switch to another access point with stronger signal strength while it is already connected, but Vigor wireless routers have an AP-assisted client roaming feature that could facilitate roaming on wireless stations. Depending on the roaming configuration, the Vigor monitors the Received Signal Strength Indicator (RSSI) of wireless stations and disconnect stations whose RSSI falls below a certain (configurable) threshold, thus forcing stations to seek out other WiFi hosts to connect to.

To configure wireless roaming settings, go to Wireless LAN >> Roaming.

Wireless LAN(2.4GHz) >> Roaming

Router-assisted Client Roaming Parameters

☒ Disable RSSI Requirement			
☐ Strictly Minimum RSSI	-73	dBm (42 % (Default -73))	
☐ Minimum RSSI	60	dBm (60 % (Default 60))	
With Adjacent AP RSSI over	5	dB (Default 5)	

Available settings are explained as follows:

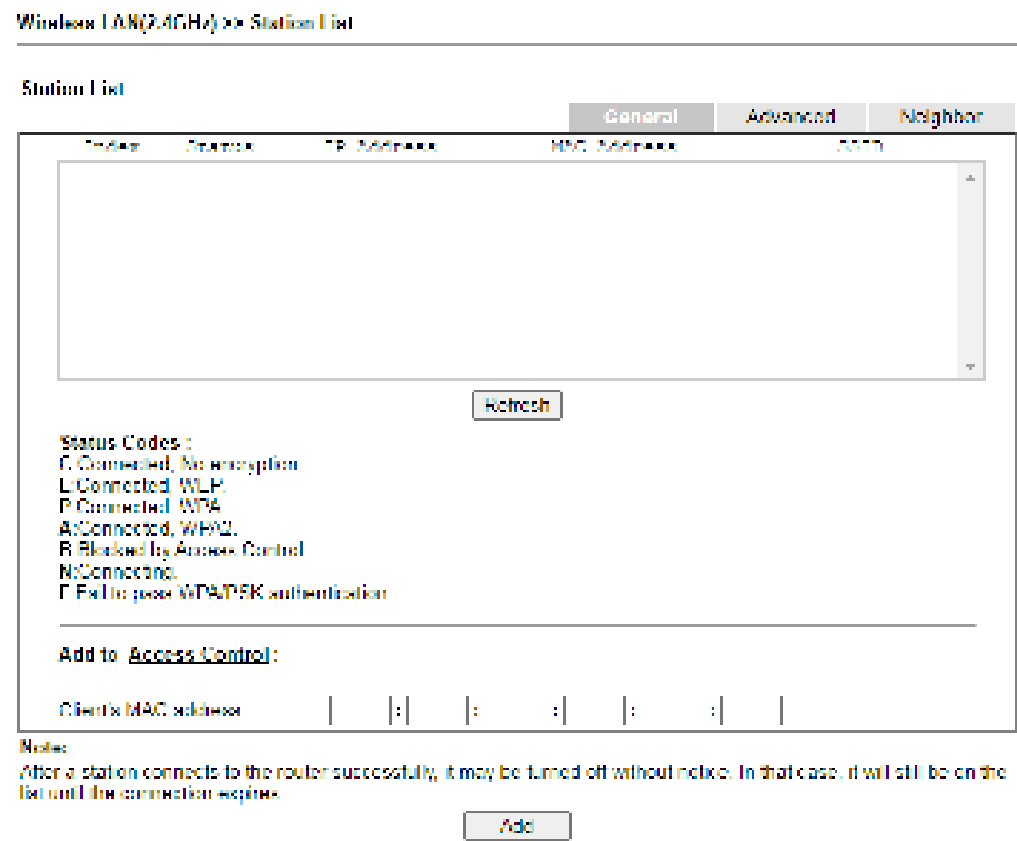
Item	Description
Disable RSSI Requirement	The Vigor router does not pay attention to the RSSI level of wireless stations. Selecting this option means the Vigor router will not interfere with the roaming behavior of wireless stations.
Strictly Minimum RSSI	The Vigor router will immediately disconnect the wireless station if its RSSI falls below the configured value.
Minimum RSSI	Minimum RSSI - The Vigor router will disconnect wireless clients whose RSSI falls below the minimum threshold only if there is also a neighboring wireless host (router or AP) that has an RSSI value (defined in the field of With Adjacent AP RSSI over) higher than a certain threshold. In order for this option to work, other wireless hosts connected to the same LAN subnet need to support the exchange of RSSI information with peer wireless hosts via Ethernet. With Adjacent AP RSSI over –Specify a value as a threshold.

To save changes on this page, select **OK**; to discard changes, select **Cancel**.

III-1-14 Station List

Station List provides an overview of all currently connected wireless clients and their status. As an added convenience, you may choose to add a particular wireless client to the Access Control by double clicking its entry in the list to populate the MAC address field, followed by clicking the Add button.

There are 3 tabs on the Station List screen: General, Advanced and Neighbor. Both General and Advanced show wireless stations connected to the Vigor router, whereas Neighbor shows nearby wireless stations connected to other access points that are detected by the Vigor router.



Available settings are explained as follows:

Item	Description
Refresh	Click to refresh the station list.
Add	Click to add the address in the Client's MAC address field to Access Control.

Below shows the Advanced tab, which lists the same clients as the General tab, but with more detailed information.

Wireless LAN(2.4GHz) >> Station List

Station List

General										Advanced		Neighbor	
Index	MAC Address	SSID	RSSI	Rate	TX	RX	MTX	PMF	WPS				
Refresh													
Add to Access Control :													
Client's MAC address : : : : :													

Notes:

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

Below shows the Neighbor tab, which lists wireless clients seen by the router but are not connected to the router's built-in access point.

Wireless LAN(2.4GHz) >> Station List

Station List

General										Advanced		Neighbor	
Index	MAC Address	Vendor	SSID	Approx. Distance	SSID	Vendor	Class						
1	88:8E:8A:00:00:00:15	Apple	WiFi (802.11n)	0.00 ~ 0.0m	SSID	Vendor	Class						
2	00:0F:33:00:00:00:01	TP-Link	WiFi (802.11n)	0.00 ~ 0.0m	SSID	Vendor	Class						
3	20:00:00:00:00:00:00	WiFi	802.11n	0.00 ~ 0.0m	SSID	Vendor	Class						
4	00:00:00:00:00:00:00	WiFi	802.11n	0.00 ~ 0.0m	SSID	Vendor	Class						
5	2A:1B:00:00:00:00:00	WiFi	802.11n	0.00 ~ 0.0m	SSID	Vendor	Class						
6	00:00:00:00:00:00:00	Realtek	WiFi (802.11n)	0.00 ~ 0.0m	SSID	Vendor	Class						
7	20:00:00:00:00:00:00	WiFi	802.11n	0.00 ~ 0.0m	SSID	Vendor	Class						
8	00:00:00:00:00:00:00	WiFi	802.11n	0.00 ~ 0.0m	SSID	Vendor	Class						
Refresh													
Add to Access Control :													
Client's MAC address : : : : :													

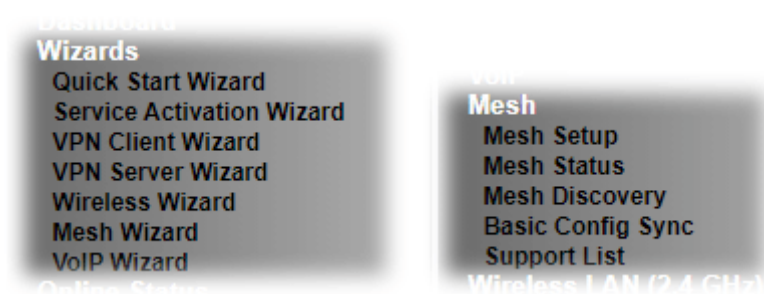
Notes:

1. Approx. Distance is calculated by actual signal strength of device detected. Inaccuracy might occur based on barrier encountered.
2. Due to the differences in signal strength for different devices, the calculated value of approximate distance also might be different.
3. Trademarks and brand names are the properties of their respective owners.

Add

III-2 Mesh Network

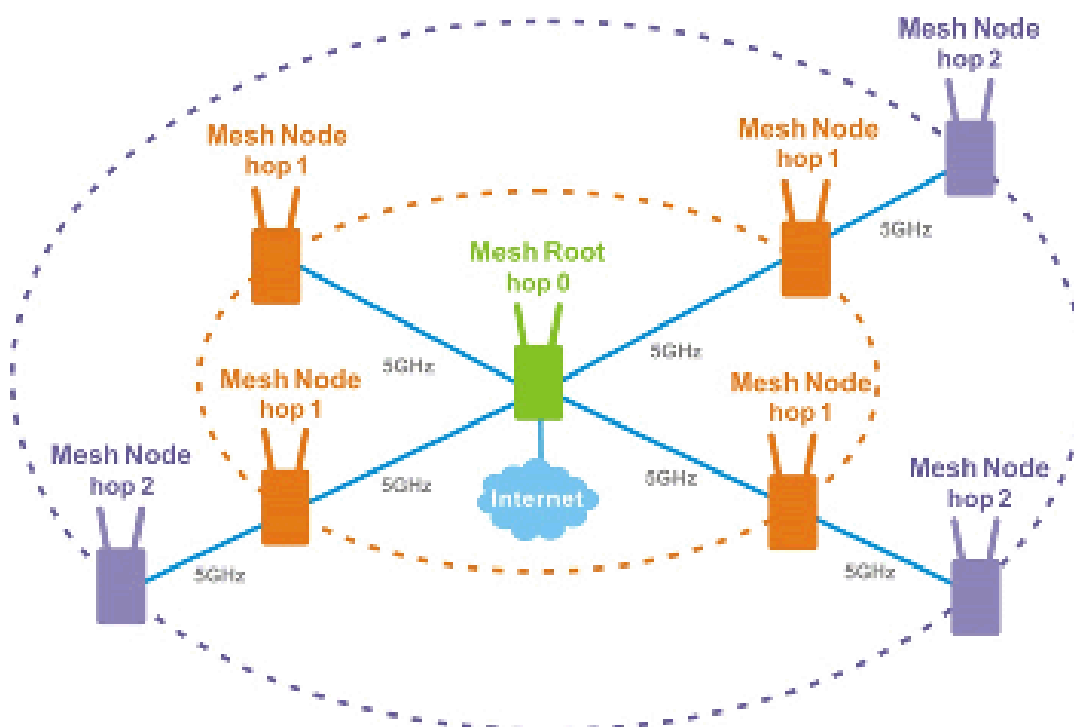
Vigor router plays a role of Mesh root in a VigorMesh network. To configure the mesh network, please use the Mesh Wizard or open the Mesh menu to configure detailed settings.



Please note that, within VigorMesh network,

- the total number allowed for mesh nodes is 8 (including the mesh root)
- the maximum number of hop is 3

Refer to the following figure:



For the mesh group set within VigorMesh network,

- It must be composed by “1” Mesh Root and “0~7” mesh nodes
- (Roaming) Normally members in a mesh group use the same Wireless SSID/security
- (Add) Only the mesh root can add a new mesh node into the mesh group
- (Recover) A disconnected mesh node will automatically try to connect to another connected mesh node of the same group

Mesh Root

Mesh Root indicates that Vigor router would be other AP's uplink connection. As a Mesh Root, Vigor router must connect to internet through WANs to have an internet connection.

The following figure shows how Vigor router runs as MESH ROOT:



III-2-1 Mesh Wizard

Mesh wizard offers a quick way to configure mesh network.

1. Go to **Wizards>Mesh Wizard**.

Mesh Wizard

Mesh Setup

The screenshot shows the 'Mesh Setup' wizard interface. It includes a checkbox for 'Enable Mesh' which is checked. Below this, there are two fields: 'Role' with a dropdown menu set to 'Mesh Root' and 'Group Name' with a text input field containing 'VigorMesh'. At the bottom, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

2. Check the **Enable Mesh** box. Click **Next** to get the following page.

Mesh Wizard

Wifi Setup

Wifi Settings

Wifi Name:

Wifi Password:

☐ Enable Guest Wifi

Guest Wifi Name:

Guest Wifi Password:

Notes:

The Wifi settings will apply to all Wireless bands.

3. Set the Wifi Name and password; click **Next** to get the following page.

Mesh Wizard

Enter login password

Please enter an alpha-numeric string as your Password

Old Password:

New Password:

Confirm Password:

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

4. Set the password, if required. Then, click **Finish** to get the following page.

Mesh Wizard

Mesh Node Setup

Setup additional VigorVPs to Mesh network?

Please power up and wait for us to find it

Search List

Select	Model	MAC	Device Name

- Click **Search** and wait for a few minutes. Later, APs around Vigor router will be shown below.

Mesh Wizard

Mesh Node Setup

Setup additional Vigor APs to Mesh network?

Please power up and wait for us to find it.

Search List

Select	Model	MAC	Device Name
☒	VigorAP903	00:50:7F:01:01:BC	AP903

Search

Apply

Cancel

- Select the one (e.g., VigorAP903 in this case) you want to group under Vigor router. Then, click **Apply**.

Mesh Wizard

Mesh Node Setup

Setup additional Vigor APs to Mesh network?

Please power up and wait for us to find it.

Search List

4%

Search

Applying

Cancel

- When the mesh node setup is finished, click **Finish**.

Mesh Wizard

Mesh Node Setup Finished

Setup Mesh Root and Mesh Node completed.

Cancel

Finish

8. After "Mesh Wizard Setup OK!" appears, go to **Mesh>>Mesh Status**. The mesh node (AP903) has been grouped under the Vigor router.

Mesh Wizard

Mesh Wizard Setup OK!

Mesh >> Mesh Status

Local Status

Refresh

Device Name	DrayTek								
MAC Address	00:1D-AA-15:B0:C3								
Model	Vigor2765								
Operation Mode	MeshRoot								
Wireless Downlink Band	Auto								
Group Name	VigorMesh								
Link Status	Connected								
Hop	0								
Downlink Number	1								
Downlink	00:50:7F:F1:7F:1D (VigorAP903) Wireless 5GHz (Ch36) (-58dBm / 81%)								

Devices

Total Number of Clients: 38

Index	Status	Device Name	IP Address	MAC Address (Model)	Hop	Uplink	Uptime	Clients	Action
1	Root	DrayTek	172.16.21.84	00:1D-AA:15:B0:C3 (Vigor2765)	0		3d 12:08:49	14	Reconnect
2	Online	MK_AP903	172.16.21.58	00:50:7F:F1:7F:1D (VigorAP903)	1	14:49:BC:17:70:08 Wireless 5GHz (Ch36) (-60dBm / 75%)	3d 12:00:44	8	Disconnect

Online(sync ready)

Online

Offline

III-2-2 Mesh Setup

This page can modify settings related to Mesh. You can search and specify mesh nodes as members under current mesh group.

Mesh >> Mesh Setup

General Setup

[Refresh](#)

☒ Enable Mesh

Role

Mesh Root

Wireless Downlink Band

Dedicate 5GHz

Group Name

VigorMesh

Auto Reselect

☒

Log Level

Basic

Mesh Group

Select	Index	Role	MAC Address	Model	CFG Sync	Device Name
☐	1	Root	00:1D:7A:01:54:00:00	Vigor2705		

[Reset](#)

[Delete](#)

☐ Undo WLAN to Mesh

[OK](#)

[Cancel](#)

Add Mesh Node

Please Search button below to find and select the new node into Mesh Group

[Search](#)

Search List

Select	MAC Address	Model	Operation Mode	Device Name

[Apply](#)

[Backup Mesh Config](#)

[Backup](#)

[Upload From File](#)

[PC](#)

[Android](#)

[iOS](#)

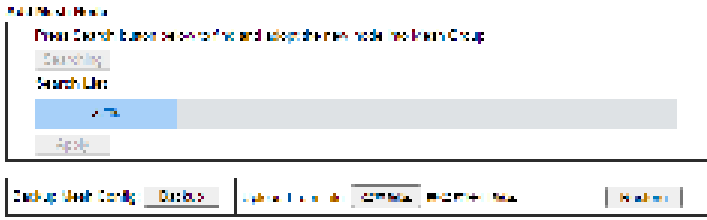
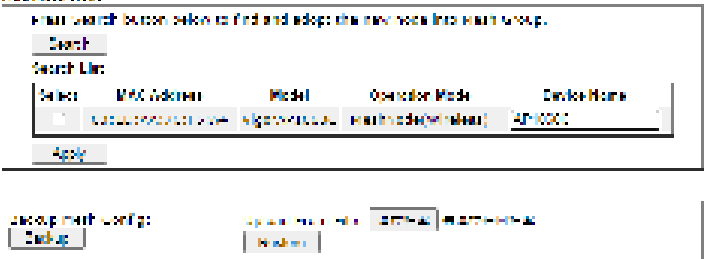
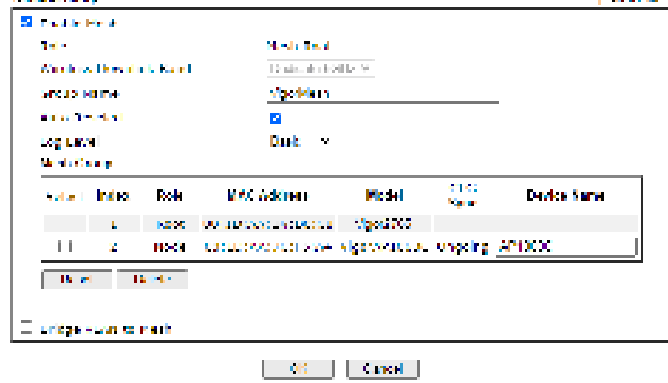
[Restore](#)

Note:

After enabling the Mesh function, all the settings on Wireless LAN (5 GHz) power will be invalid

Available settings are explained as follows:

Item	Description
General Setup	
Enable Mesh	Check to enable the mesh function.
Role	Displays the role of Vigor router. Vigor router is a mesh root to provide internet access for Mesh Network.
Wireless Downlink Band	At present, only 5GHz is dedicated as the downlink band for connecting with an uplinked mesh node.
Group Name	Displays the name of the current mesh group.
Auto Reselect	It is selected in default. To perform the auto reselect, make sure the process for CFG Sync and CFG Check for mesh nodes are successful. If enabled, after changing the environment of mesh network (e.g., offline, disconnection), the root device will perform auto reselect to reconstruct the mesh network.
Log Level	Choose Basic or Detailed . Related information will be shown

	on the Diagnostics>>System Log .
Mesh Group	The basic information including role, MAC address, and model name of the mesh root and node (up to 8 entries, one mesh root and seven mesh nodes) will be shown on this field. Reset - Click it to clear the Mesh Group information. Delete - Click it to remove the selected entry.
Bridge VLAN to Mesh	Select to enable the function.
Add Mesh Node - It is available only if the Mesh function is enabled.	
Search	Click to scan available APs around this Vigor router.  The detected APs will be shown on the Search List. 
Apply	Select the mesh node you want and click this button. The new mesh node will be shown on Mesh Group. 
Backup Mesh Config	Backup - Click the button to save the configuration as a file.
Upload/ Restore	Click the Upload button to specify a configuration file. Then click Restore to apply the configuration. When the MAC address of the Vigor router is not the mesh root of the mesh group, the restore operation will not succeed.

III-2-3 Mesh Status

This page shows the mesh network status.

One Mesh Group can contain up to 8 devices. In the following figure, the device with hop 0 is one special Ethernet Backhaul. It means this node will use Ethernet cable to join the mesh group while others use the wireless link.

Mesh >> Mesh Status

Local Status										Refresh
Device Name	DrayTek									
MAC Address	00:1D:AA:15:B0:C3									
Model	Vigor2765									
Operation Mode	MeshRoot									
Wireless Downlink Band	Auto									
Group Name	VigorMesh									
Link Status	Connected									
Hop	0									
Downlink Number	1									
Downlink	00:50:7F:F1:7F:1D (VigorAP903) Wireless 5GHz (Ch36) (-58dBm / 81%)									

Devices										Total Number of Clients: 38
Index	Status	Device Name	IP Address	MAC Address (Model)	Hop	Uplink	Uptime	Clients	Action	
1	Root	DrayTek	172.16.21.84	00:1D:AA:15:B0:C3 (Vigor2765)	0		3d 12:08:49	14	Reconnect	
2	Online	MY_AP903	172.16.21.58	00:50:7F:F1:7F:1D (VigorAP903)	1	14:48:BC:17:70:08 Wireless 5GHz (Ch36) (-60dBm / 76%)	3d 12:05:44	8	Disconnect	
3	Online	HR_AP903	172.16.21.62	00:50:7F:67:28:DC (VigorAP903)	2	00:50:7F:F1:7F:1D Wireless 5GHz (Ch36) (-84dBm / 65%)	3d 12:05:22	10	Disconnect	
4	Online	TS_AP1000	172.16.21.57	00:1D:AA:04:F0:DC (VigorAP1000C)	3	00:50:7F:57:29:0C Wireless 5GHz (Ch36) (-65dBm / 50%)	3d 12:05:00	8	Disconnect	

● Online(sync ready)
 ● Online
 ● Offline

Available settings are explained as follows:

Item	Description
Local Status	Display general information for this device.
Devices	Display detailed information for this device (as mesh root) and mesh node(s) in the group. Index - Display the number of the device within a mesh group. Status - Display the role and connect status of the device. Device Name - Display the name of the device (for identification). IP Address - Display the IP address of the device. MAC Address - Display the MAC address of the device. Hop - Display the level of the device in Mesh Network. "0" means the device is connected to Internet by using Ethernet cable (wired). "1" to "3" means how many wireless links the device has to go through to reach a Hop 0 device. Uplink - Display the MAC address of the device that the AP connects to.
Total number of Clients	Display the station list of all mesh devices.

Station List of All Stations						
Index	MAC Address	Manufacturer	Model	SSID	Channel (RSSI)	LinkStatus(RSSI)
1	00:50:7F:11:19:10:00	TP-LINK	TP-LINK	mesh_1P	6	60% (-60dBm)
2	00:50:7F:11:19:10:00	TP-LINK	TP-LINK	mesh_1P	6	41% (-73dBm)
3	00:50:7F:11:19:10:00	TP-LINK	TP-LINK	mesh_1P	6	20% (-85dBm)
4	00:50:7F:11:19:10:00	TP-LINK	TP-LINK	mesh_1P	6	20% (-85dBm)
5	00:50:7F:11:19:10:00	TP-LINK	TP-LINK	mesh_1P	6	20% (-85dBm)
6	00:50:7F:11:19:10:00	TP-LINK	TP-LINK	mesh_1P	6	20% (-85dBm)
7	00:50:7F:11:19:10:00	TP-LINK	TP-LINK	mesh_1P	6	20% (-85dBm)
8	00:50:7F:11:19:10:00	TP-LINK	TP-LINK	mesh_1P	6	20% (-85dBm)
9	00:50:7F:11:19:10:00	TP-LINK	TP-LINK	mesh_1P	6	20% (-85dBm)
10	00:50:7F:11:19:10:00	TP-LINK	TP-LINK	mesh_1P	6	20% (-85dBm)
11	00:50:7F:11:19:10:00	TP-LINK	TP-LINK	mesh_1P	6	20% (-85dBm)
12	00:50:7F:11:19:10:00	TP-LINK	TP-LINK	mesh_1P	6	20% (-85dBm)
13	00:50:7F:11:19:10:00	TP-LINK	TP-LINK	mesh_1P	6	20% (-85dBm)
14	00:50:7F:11:19:10:00	TP-LINK	TP-LINK	mesh_1P	6	20% (-85dBm)
15	00:50:7F:11:19:10:00	TP-LINK	TP-LINK	mesh_1P	6	20% (-85dBm)
16	00:50:7F:11:19:10:00	TP-LINK	TP-LINK	mesh_1P	6	20% (-85dBm)
17	00:50:7F:11:19:10:00	TP-LINK	TP-LINK	mesh_1P	6	20% (-85dBm)
18	00:50:7F:11:19:10:00	TP-LINK	TP-LINK	mesh_1P	6	20% (-85dBm)
19	00:50:7F:11:19:10:00	TP-LINK	TP-LINK	mesh_1P	6	20% (-85dBm)
20	00:50:7F:11:19:10:00	TP-LINK	TP-LINK	mesh_1P	6	20% (-85dBm)

III-2-4 Mesh Discovery

Before a Mesh Node is connected, it is unable to check the device status from Mesh Root. This page can help to discover all Mesh devices around and offer the Link Status and Operation Mode of each Mesh device.

For obtaining the list of devices around this Vigor router, click **Scan**. Later, surrounding Mesh device(s) will be displayed on this page.

Mesh >> Mesh Discovery

Device List

Index	MAC Address	Model	Operation Mode	Link Status
1	00:50:7F:11:19:10:00	VigorAP900	MeshNode(Wireless)	Disconnected
2	00:50:7F:11:19:10:00	VigorAP900	MeshNode(Wireless)	Connected
3	00:1D:6A:6A:2C:00	VigorAP10000	AP	Connected
4	00:1D:6A:6A:2C:00	VigorAP10000	AP	Connected
5	00:1D:6A:6A:2C:00	VigorAP10000	MeshNode(Wireless)	New

Scan

Note:

During the scanning process (about 10 seconds), no station is allowed to connect with the Router and Mesh Network may disconnect.

Only the device with the Link Status of "New" can be selected and grouped under this router.

III-2-5 Basic Config Sync

If you add one Mesh Node in a mesh group, the Mesh Root will send the basic configuration to the device. This page could help you to change the Mesh Root settings and deliver the new configuration of the Mesh Root to all "connected" Mesh Nodes.

Mesh => Basic Configuration Sync

System Maintenance

Index	Name	Value
1	X_00507F_System.Management.SkipQuickStart/Wizard	Enable
2	X_00507F_System.TROOSetting.CPEEnable	1
3	ManagementServer.URL	http://192.16.2.222:80/A...
4	ManagementServer.Username	Angela
5	ManagementServer.Password	*****
6	ManagementServer.ConnectionRequestUsername	vigor
7	ManagementServer.ConnectionRequestPassword	*****
8	X_00507F_System.AdminmodePassword.Admin	admin
9	X_00507F_System.AdminmodePassword.Password	*****
10	X_00507F_System.SyslogMail.SysLogAccess.SysLogEnable	0
11	X_00507F_System.SyslogMail.SysLogAccess.LogServerIP	
12	X_00507F_System.SyslogMail.SysLogAccess.LogServerPort	514
13	X_00507F_System.SyslogMail.MailAlert.MailAlertEnable	0
14	X_00507F_System.SyslogMail.MailAlert.SMTPServer	
15	X_00507F_System.SyslogMail.MailAlert.MailTo	
16	X_00507F_System.SyslogMail.MailAlert.Username	
17	X_00507F_System.SyslogMail.MailAlert.Password	*****
18	X_00507F_System.SyslogMail.MailAlert.UseTLS	0
19	X_00507F_System.SyslogMail.MailAlert.SMTPServerPort	25

Wireless LAN (2.4GHz)

Index	Name	Value
1	X_00507F_WirelessLAN_AP-General.EnableWLAN	1
2	X_00507F_WirelessLAN_AP-General.SSID.1.SSID	2020-mk-angela-1
3	X_00507F_WirelessLAN_AP-General.SSID.1.Enable	1
4	X_00507F_WirelessLAN_AP-General.SSID.1.Hide	0
5	X_00507F_WirelessLAN_AP-General.SSID.1.IsolateMember	0

Available settings are explained as follows:

Item	Description
System Maintenance / Wireless LAN (2.4Hz) / Wireless LAN (5GHz)	Check the item(s) you want to make configuration sync. Apply - Click it to apply the settings configured by this router to all connected mesh node.

Tips for Mesh Network Setup

- Set up TWO mesh devices with uplink RSSI larger than -65dBm.
- Upgrade the firmware version of Mesh devices through Mesh link, starting from the mesh device with less hop number. For example, upgrade the firmware from the root, hop1 Mesh Node then hop2 Mesh Node, and so on.
- VigorMesh network supports up to 3 hops of mesh devices. However, it is suggested to connect the mesh group with less than or equals to 2 hops.

For your reference, we make a real mesh environment test and get the following record. (Use VigorAP APP to do internet speed test with different hops mesh node.)

Internet Download Speed (for root and hop1 ~ hop3):

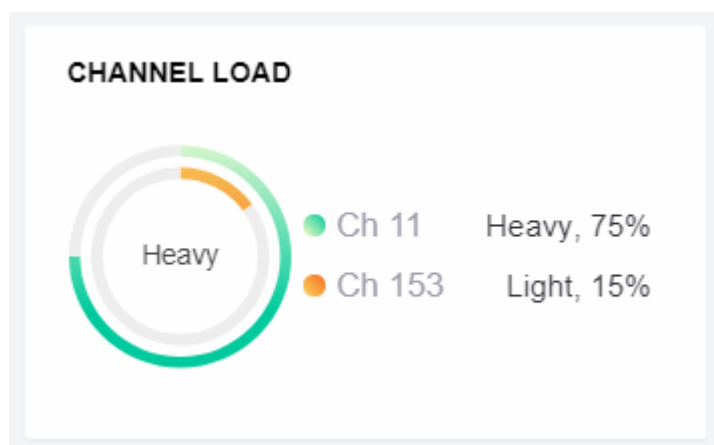
iPad connects to Root : 80Mbps

iPad connects to hop1 Node : 49Mbps (Uplink RSSI : -55dBm)

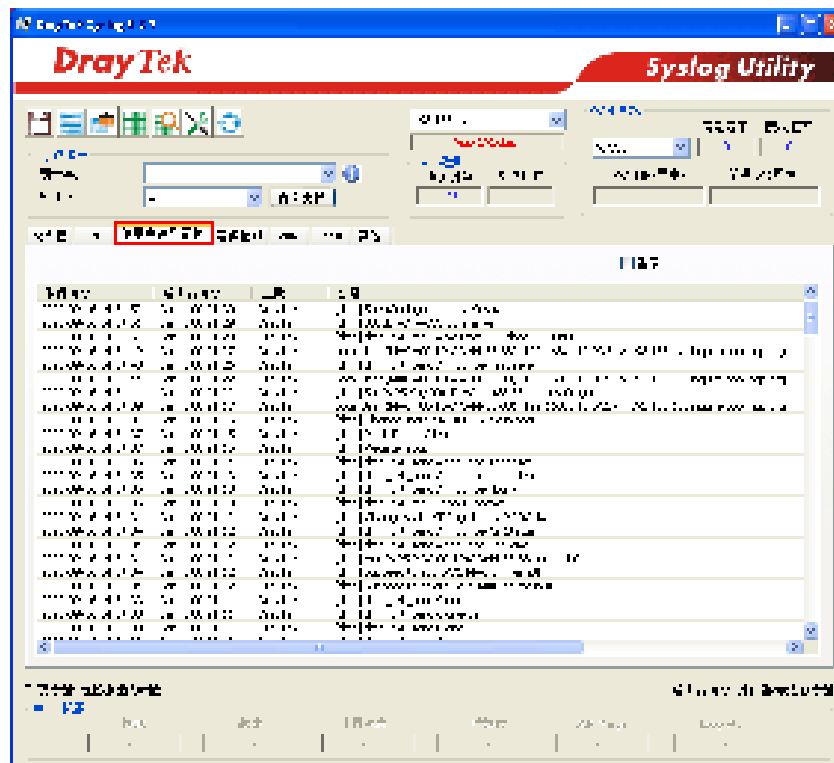
iPad connects to hop2 Node : 41Mbps (Uplink RSSI : hop2 -64dBm / hop1 -55dBm)

iPad connects to hop3 Node : 26Mbps (Uplink RSSI : hop3 -62dBm / hop2 -68dBm / hop1 -55dBm)

- It is not suggested to use a wireless Mesh Node with Ethernet cable connected to a Mesh Root.
- If resetting a Mesh Root,
 - All "connected" Mesh Nodes will be informed to reset.
 - Group List and Group Key will be reset, too.
 - For those Mesh Nodes unable to reset, reset them manually. Reset the Group List by web or factory default.
- If resetting a Mesh Node,
 - Group List and Group Key will be cleared.
 - Link Status will become "New".
- If Mesh Search / Apply / Discover is worked too fast or is done with empty result, your request may be rejected. Please try again.
- Troubleshooting:
 - Check the firmware version. Please make sure all APs within the mesh group are in the newest firmware version.
 - Check the OP (operation) Mode. Make sure new Mesh Node doesn't accidentally get DHCP IP and becomes AP mode.
 - Check the country code and channels. For example, it is impossible for connecting a VigorAP 912C Mesh Root with 5G channel 36 to VigorAP920R Wireless Mesh Node in EU country code.
 - Check the channel load. Make sure it is not over 70%.



- Collect some Mesh logs and send the result to DrayTek for analyzing.



III-2-6 Support List

Mech Support List

The following compatibility test lists DrayTek AP models supported by Vigor model Mech.

Model	Status	Firmware Version
ModAP 002	Y	1.1.0
VigorAP 003	Y	1.3.8
ModAP 9120	Y	1.1.0
VigorAP 1000C	Y	1.3.5

Y: tested and is supported.

N: Not supported.

Part IV VoIP



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

IV-1 VoIP

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



Info

This function is used for “V” models.

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

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

sip: user:password @host: port

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

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

Calling via SIP Servers

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

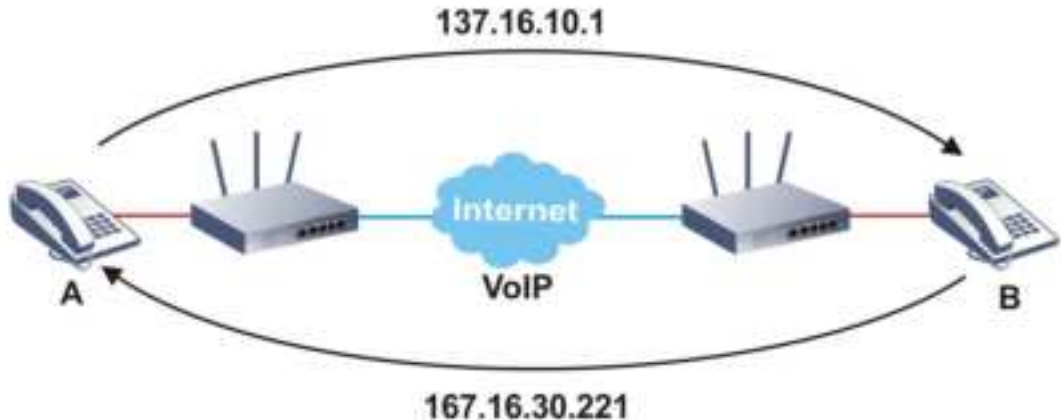
If you both register to the same SIP Registrar, then it will be illustrated as below:



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

Peer-to-Peer

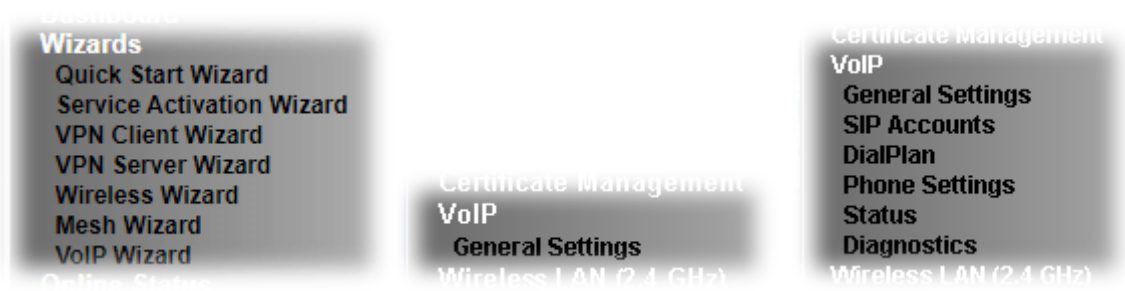
Before calling, you have to know your friend's IP Address. The Vigor VoIP Routers will build connection between each other.



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

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

Web User Interface



IV-1-1 VoIP Wizard

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



Info

This wizard is available for “V” model only.

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

VoIP Wizard

Set VoIP service provider domain

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

Set Account quickly

Phone 1 (default mapping to Account 1)		
Account Number/Name		(63 char max.)
Password		(127 char max.)
Phone 2 (default mapping to Account 2)		
☒ use the same Account as phone1		
Account Number/Name		(63 char max.)
Password		(127 char max.)

Available settings are explained as follows:

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

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

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

VoIP Wizard

Please confirm your settings:

VoIP Service Provider	draytel.org
SIP Port	5060
Phone 1 Account	56703
Phone 2 Account	56834

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

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

VoIP Wizard Setup OK!

IV-1-2 General Settings

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

VoIP>>General Settings

☒ **Enable VoIP**

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

OK

After checking the box and click **OK**, the router will reboot. Open **VoIP>>General Settings** again. The following page appears for you to configure secure phone, IP call; and set NAT Traversal Setting, RTP for the VoIP function.

VoIP>>General Settings

☒ **Enable VoIP**

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

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

NAT Traversal Setting
STUN Server _____
External IP _____
SIP PING Interval 150 sec

RTP
☒ **Symmetric RTP**
Dynamic RTP Port Start 10050
Dynamic RTP Port End 10060
RTP TOS IP precedence 5 10100000

IP Call
☒ **Enable IP Call**

OK

Available settings are explained as follows:

Item	Description
Secure Phone	Enable Secure Phone - It allows users to have encrypted RTP stream with the peer side using the same protocol (ZRTP+SRTP). Check this box to have secure call. Enable SAS Voice Prompt - If it is enabled, SAS prompt will be heard for both ends every time. If it is disabled, no SAS prompt will be heard any more.
NAT Traversal Setting	STUN Server - Type in the IP address or domain of the STUN

	server. External IP - Type in the gateway IP address. SIP PING interval - The default value is 150 (sec). It is useful for a Nortel server NAT Traversal Support.
RTP	Symmetric RTP - Check this box to invoke the function. To make the data transmission going through on both ends of local router and remote router not misleading due to IP lost (for example, sending data from the public IP of remote router to the private IP of local router), you can check this box to solve this problem. Dynamic RTP Port Start - Specifies the start port for RTP stream. The default value is 10050. Dynamic RTP Port End - Specifies the end port for RTP stream. The default value is 15000. RTP TOS - It decides the level of VoIP package. Use the drop down list to choose any one of them.
IP Call	Enable IP Call –It allows that a user could dial outgoing IP Calls; and Vigor router could receive the incoming IP Calls.

Application for Secure Phone

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

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

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

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



Info

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

IV-1-3 SIP Accounts

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

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



Info

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

VoIP > SIP Accounts



SIP Accounts List

Refresh

Index	Profile	Domain/Realm	Proxy	Account Name	Codec	Ring Port	Status
1					G.729MB	☐ Phone1 ☐ Phone2	
2				---	G.729MB	☐ Phone1 ☐ Phone2	-
3					G.729MB	☐ Phone1 ☐ Phone2	
4				---	G.729MB	☐ Phone1 ☐ Phone2	-
5					G.729MB	☐ Phone1 ☐ Phone2	
6				---	G.729MB	☐ Phone1 ☐ Phone2	-

R means registered on SIP server
- fail to register on SIP server

Alias List

OK

Available settings are explained as follows:

Item	Description
Index	Click this link to access into next page for setting SIP account.
Profile	Display the profile name of the SIP account.
Domain/ Realm	Display the domain name or IP address of the SIP registrar server.
Proxy	Display the domain name or IP address of the SIP proxy server.
Account Name	Display the account name of SIP address before @.
Codec	Display the codec type for the account.
Ring Port	Specify which port will ring when receiving a phone call.
Status	Show the status for the corresponding SIP account. R means such account is registered on SIP server successfully. - means the account is failed to register on SIP server.
Alias List	Allows you to set multiple SIP alias names.

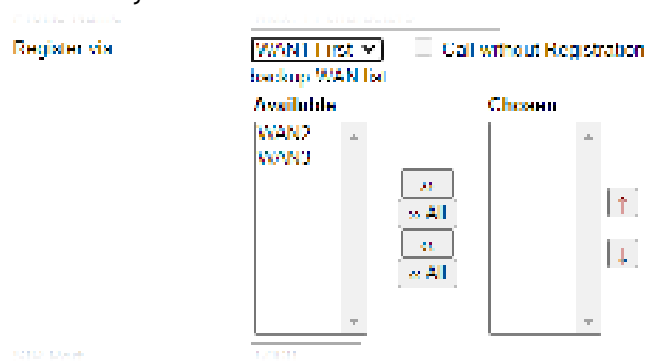
Click any index link to access into the following page for configuring SIP account.

SIP Account Index No. 1

Profile Name	iptel (11 char max.)	
Register via	Auto	☐ Call without Registration
SIP Port	5060	
Domain/Realm	iptel.org	
Proxy	iptel.org	
☐ Act as outbound proxy		
Display Name	diegobee15203	
Account Number/Name	diegobee415203	
☐ Authentication ID	diegobee15203	
Password	*****	
Expiry Time	1 hour	3600 sec
NAT Traversal Support	None	
Mapping to Alias List	None	
Call Forwarding	Disable	
SIP URI		
Time Out	30	sec
Ring Port	☒ Phone1 ☒ Phone2	
Ring Pattern	1	
Prefer Codec	G.711MU (64Kbps)	☐ Single Codec
Packet Size	30ms	
Voice Active Detector	Off	

OK Cancel Close

Available settings are explained as follows:

Item	Description
Profile Name	Assign a name for this profile for identifying. You can type similar name with the domain. For example, if the domain name is <i>draytel.org</i> , then you might set <i>draytel-1</i> in this field.
Register via	If you want to make VoIP call without register personal information, please choose None and check the box to achieve the goal. Some SIP server allows user to use VoIP function without registering. For such server, please check the box of Call without Registration. Choosing Auto is recommended. The system will select a proper way for your VoIP call. Note, when WAN# First is selected, you have to specify backup WAN for this SIP account. Once the interface (WAN# First) disconnects, the backup WAN will perform the job automatically. 
SIP Port	Set the port number for sending/receiving SIP message for building a session. The default value is 5060 . Your peer must

	set the same value in his/her Registrar.
Domain/Realm	Set the domain name or IP address of the SIP Registrar server.
Proxy	Set domain name or IP address of SIP proxy server. By the time you can type :port number after the domain name to specify that port as the destination of data transmission (e.g., nat.draytel.org:5065)
Act as Outbound Proxy	Check this box to make the proxy acting as outbound proxy.
Display Name	The caller-ID that you want to be displayed on your friend's screen.
Account Number/Name	Enter your account name of SIP Address, e.g. every text before @.
Authentication ID	Check the box to invoke this function and enter the name or number used for SIP Authorization with SIP Registrar. If this setting value is the same as Account Name, it is not necessary for you to check the box and set any value in this field.
Password	The password provided to you when you registered with a SIP service.
Expiry Time	The time duration that your SIP Registrar server keeps your registration record. Before the time expires, the router will send another register request to SIP Registrar again.
NAT Traversal Support	If the router (e.g., broadband router) you use connects to internet by other device, you have to set this function for your necessity. None –Disable this function. Stun - Choose this option if there is Stun server provided for your router. Manual - Choose this option if you want to specify an external IP address as the NAT transversal support. Nortel - If the soft-switch that you use supports Nortel solution, you can choose this option.
Mapping to Alias List	Select one of the alias profiles.
Call Forwarding	There are four options for you to choose. Disable is to close call forwarding function. Always means all the incoming calls will be forwarded into SIP URL without any reason. Busy means the incoming calls will be forwarded into SIP URL only when the local system is busy. No Answer means if the incoming calls do not receive any response, they will be forwarded to the SIP URL by the time out. SIP URL - Type in the SIP URL (e.g., aaa@draytel.org or abc@iptel.org) as the site for call forwarded. Time Out - Set the time out for the call forwarding. The default setting is 30 sec.
Ring Port	Set Phone 1 and/or Phone 2 as the default ring port(s) for this SIP account.
Ring Pattern	Choose a ring tone type for the VoIP phone call.
Prefer Codec	Select one of five codecs as the default for your VoIP calls. The codec used for each call will be negotiated with the peer party before each session, and so may not be your default choice. The default codec is G.729A/B; it occupies little

	bandwidth while maintaining good voice quality. If your upstream speed is only 64Kbps, do not use G.711 codec. It is better for you to have at least 256Kbps upstream if you would like to use G.711. Single Codec - If the box is checked, only the selected Codec will be applied.
Packet Size	The amount of data contained in a single packet. The default value is 20 ms, which means the data packet will contain 20 ms voice information.
Voice Active Detector	This function can detect if the voice on both sides is active or not. If not, the router will do something to save the bandwidth for other using. Click On to invoke this function; click Off to close the function.

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

VoIP >> SIP Accounts



SIP Accounts List

Return

Index	Profile	Domain/Realm	Proxy	Account Name	Codec	Ring Port		Status
1	ipitel	ipitel.org	ipitel.org	diegolee4152031	G.711MU	☒ Phone1	☒ Phone2	
2					G.720A/B	☐ Phone1	☐ Phone2	

IV-1-3-1 Alias List

This page lists all SIP alias profiles.

A SIP alias is just like an extension number in that people can dial it to reach a specific person directly. Normally, when you have a user account for one ITSP, the ITSP will provide you one SIP account. However, with this feature, you can own multiple SIP alias over one SIP account. When you register with a regular user account, the alias is registered as well as the main SIP account. Then, when somebody dials the alias, the SIP URI bound to the alias will ring.

Click the **Alias List** link to access the configuration page as shown below.

VoIP >> Alias

Alias List

Index	Profile Name	Number	Active	Account
1			No	
2			No	
3			No	
4			No	
5			No	
6			No	
7			No	
8			No	
9			No	
10			No	

<< 1-10 | 11-20 | 21-30 >>

Next >>

Available settings are explained as follows:

Item	Description
Index	Click the number link for each profile.
Profile Name	Display the alias name for such sub account.

Number	Display the phone number of such account.
Active	Display current activation status for such account, enabled (Yes) or disabled (No).
Account	Display the SIP account name / number for this sub account attached.

You can set 30 profiles as alias. Click the number under Index to set detailed configuration.

VoIP >> Alias

Alias 1.

Active	☒ Enable ☐ Disable
Alias Name	522293
Alias Number	522293
Alias of SIP account	1 diegohe415200 v

Available settings are explained as follows:

Item	Description
Active	Click Enable to activate this entry. Or, click Disable to inactive this entry.
Alias Name	Specify a name for an alias number.
Alias Number	Enter an alias number. The alias numbers are obtained from your ITSP.
Alias of SIP account	Specify one of the main SIP account profiles.

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

VoIP >> Alias

Alias List

Index	Profile Name	Number	Active	Account
1.	522293	522293	Yes	diegohe415200
2.			No	
3.			No	
4.			No	
5.			No	
6.			No	
7.			No	
8.			No	
9.			No	
10.			No	

<< 1-10 | 11-20 | 21-30 >>

Next >>

When an Alias profile is enabled, the main SIP Account page will be changed as follows:

IV-1-4 DialPlan

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

IV-1-4-1 Phone Book

In this section, you can set your VoIP contacts in the “phonebook”. It can help you to make calls quickly and easily by using “speed-dial” **Phone Number**. There are total 60 index entries in the phonebook for you to store all your friends and family members’ SIP addresses. **Loop through** and **Backup Phone Number** will be displayed if you are using Vigor2765 series for setting the phone book.

VoIP >> DialPlan Setup

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

<< 1 20 | 21 40 | 41 60 >>

Next >>

Status: x Active x Inactive

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

VoIP >> DialPlan Setup

Phone Book Index No. 1

☒ Enable	
Phone Number	0910204067
Display Name	Only
SIP URL	1112
	lwl-pulse.com
Dial Out Account	Default
Secure Phone	None
	None
	SRTP/LSRTP
OK	Cancel

Available settings are explained as follows:

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

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



Info

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

Example:

VoIP >> DialPlan Setup

Phone Book		Digit Map	Call Barring	Regional		
Index	Phone Number	Display Name	SIP URL	Dial Out Account	Secure Phone	Status
1.	0310234567	Party	1112@local.globe.com	Default	ZRTP+SRTP	✓
2.				Default	None	✗
3.				Default	None	✗
4.				Default	None	✗
5.				Default	None	✗

IV-1-4-2 Digit Map

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

VoIP >> DialPlan Setup

Phone Book			Digit Map	Call Barring		Regional			
#	Enable	Match Prefix	Mode	OP Number	Min Len	Max Len	Route	Move Up	Move Down
1	☒	03	Replace	8853	7	8	VolP1		Down
2	☒	885	Strip	885	9	10	VolP2	UP	Down
3	☐		None		0	0	None	UP	Down
4	☐		None		0	0	None	UP	Down
5	☐		None		0	0	None	UP	Down
6	☐		None		0	0	None	UP	Down
7	☐		None		0	0	None	UP	Down
8	☐		None		0	0	None	UP	Down
9	☐		None		0	0	None	UP	Down
10	☐		None		0	0	None	UP	Down
11	☐		None		0	0	None	UP	Down
12	☐		None		0	0	None	UP	Down
13	☐		None		0	0	None	UP	Down
14	☐		None		0	0	None	UP	Down
15	☐		None		0	0	None	UP	Down
16	☐		None		0	0	None	UP	Down
17	☐		None		0	0	None	UP	Down
18	☐		None		0	0	None	UP	Down
19	☐		None		0	0	None	UP	Down
20	☐		None		0	0	None	UP	

Note:

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

OK

Cancel

Available settings are explained as follows:

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

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

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

IV-1-4-3 Call Barring

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

VoIP >> DialPlan Setup



Phone Book		Digit Map	Call Barring	Regional		
Set to Factory Default						
Index	Call Direction	Barring Type	Barring Number/URI/URI	Route	Schedule	Status
1.						X
2.						o
3.						X
4.						o
5.						X
6.						o
7.						X
8.						o
9.						X
10.						o

Oct 1 10:11:20:00

[Next](#)

Block Anonymous
Route: ☐ Phone1 ☐ Phone2
Index(1-15) in Schedule Setup: ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐
Note:
Block the incoming calls which do not have the caller ID.

Block Unknown Domain
Route: ☐ Phone1 ☐ Phone2
Index(1-15) in Schedule Setup: ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐
Note:
If the domain of the incoming call is different from the domain found in SIP accounts, the call should be blocked.

Block IP Address
Route: ☐ Phone1 ☐ Phone2
Index(1-15) in Schedule Setup: ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐
Note:
The incoming calls by means of IP dialing (e.g. 192.168.1.10) should be blocked.

OK

Cancel

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

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

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

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

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

VoIP >> DialPlan Setup

Call Barring Index No. 1

☒ Enable	
Call Direction	IN
Barring Type	Specific URI/URL
Specific URI/URL	
Route	All
Index (1-15) in Schedule Setup	

Notes:

Wildcard '*' is supported.

OK Cancel

Available settings are explained as follows:

Item	Description
Enable	Check it to enable this entry.
Call Direction	Determine the direction for the phone call, IN - incoming call, OUT-outgoing call, IN & OUT - both incoming and outgoing calls.
Barring Type	Determine the type of the VoIP phone call, URI/URL or number.
Specific URI/URL or Specific Number	This field will be changed based on the type you selected for barring Type.
Route	All means all the phone calls will be blocked with such mechanism.
Index (1-15) in Schedule Setup	Enter the index of schedule profiles to control the call barring according to the preconfigured schedules. Refer to section Applications>>Schedule for detailed configuration.

IV-1-4-4 Regional

This page allows you to process incoming or outgoing phone calls by regional. Default values (common used in most areas) will be shown on this web page. You **can change** the number based on the region that the router is placed.

VaIP >> DialPlan Setup

Phone Book	Digit Map	Call Barring	Regional	
☒ Enable Regional		[Set to Factory Default]		
Last Call Return [Miss]	169			
Last Call Return [In]	112	Last Call Return [Out]:	*14	
Call Forward [All] [Act]	172	Number 14 Call Forward [Deact]	173 14	
Call Forward [Busy] [Act]	180	Number 14 Call Forward [No Ans] [Act]	*92 +number+*	
Do Not Disturb [Act]	170	+*	Do Not Disturb [Deact]	*78 +*
Hide caller ID [Act]	167	14	Hide caller ID [Deact]	168 14
Call Waiting [Act]	168	+*	Call Waiting [Deact]	*57 +*
Block Anonymous [Act]	177	14	Block Anonymous [Deact]	187 14
Block Unknown Domain [Act]	140	+*	Block Unknown Domain [Deact]	*94 +*
Block IP Calls [Act]	160	14	Block IP Calls [Deact]	165 14
Block Lost Calls [Act]	170	+*		

Available settings are explained as follows:

Item	Description
Enable Regional	Check this box to enable this function.
Last Call Return [Miss]	Sometimes, people might miss some phone calls. Please dial number typed in this field to know where the last phone call comes from and call back to that one.
Last Call Return [In]	You have finished an incoming phone call, however you want to call back again for some reason. Please dial number typed in this field to call back to that one.
Last Call Return [Out]	Dial the number typed in this field to call the previous outgoing phone call again.
Call Forward [All][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place.
Call Forward [Deact]	Dial the number typed in this field to release the call forward function.
Call Forward [Busy][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place while the phone is busy.
Call Forward [No Ans][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place while there is no answer of the connected phone.
Do Not Disturb [Act]	Dial the number typed in this field to invoke the function of DND.
Do Not Distrub [Deact]	Dial the number typed in this field to release the DND function.

Hide caller ID [Act]	Dial the number typed in this field to make your phone number (ID) not displayed on the display panel of remote end.
Hide caller ID [Deact]	Dial the number typed in this field to release this function.
Call Waiting [Act]	Dial the number typed in this field to make all the incoming calls waiting for your answer.
Call Waiting [Deact]	Dial the number typed in this field to release this function.
Block Anonymous[Act]	Dial the number typed in this field to block all the incoming calls with unknown ID.
Block Anonymous[Deact]	Dial the number typed in this field to release this function.
Block Unknown Domain [Act]	Dial the number typed in this field to block all the incoming calls from unknown domain.
Block Unknown Domain [Deact]	Dial the number typed in this field to release this function.
Block IP Calls [Act]	Dial the number typed in this field to block all the incoming calls from IP address.
Block IP Calls [Deact]	Dial the number typed in this field to release this function.
Block Last Calls [Act]	Dial the number typed in this field to block the last incoming phone call.

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

IV-1-5 Phone Settings

This page allows user to set phone settings for Phone 1 and Phone 2 respectively. However, it changes slightly according to different model you have.

VoIP >> Phone Settings

Index	Port	Call Feature	Tone	Gain (Mic/Speaker)	Default SIP Account	DTMF Relay
1	Phone1	Call : ,	Default	1.5		On Port
2	Phone2	Call : ,	Default	1.5		On Port

Available settings are explained as follows:

Item	Description
Phone Setting	Port – there are two phone ports provided here for you to configure. Phone1/Phone2 allows you to set general settings for PSTN phones. Call Feature - A brief description for call feature will be shown in this field for your reference. Tone - Display the tone settings that configured in the advanced settings page of Phone Index. Gain - Display the volume gain settings for Mic/Speaker that configured in the advanced settings page of Phone Index. Default SIP Account - “draytel_1” is the default SIP account. You can click the number below the Index field to change SIP account for each phone port. DTMF Relay - Display DTMF mode that configured in the advanced settings page of Phone Index.

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

Detailed Settings for Phone Port

Click the number link for Phone port, you can access into the following page for configuring Phone settings.

[VoIP >> Phone Settings](#)

Phone1

Call Feature Hotline Session Timer ☐ 30 sec T.38 Fax Function Error Correction Mode REDUNDANCY DND (Do Not Disturb) Mode Index (1-15) in Schedule Setup: ☐ ☐ ☐ ☐ Note: Active and Idle Timeout settings will be ignored Index (1-60) in Phone Book >> Exception List: ☐ ☐ ☐ ☐ ☐ ☐ CLIR (hide caller ID) ☒ Call Waiting ☒ Call Transfer	Default SIP Account Play dial tone only when account registered

OK Cancel Advanced

Available settings are explained as follows:

Item	Description
Hotline	Check the box to enable it. Type in the SIP URL in the field for dialing automatically when you pick up the phone set.
Session Timer	Check the box to enable the function. In the limited time that you set in this field, if there is no response, the connecting call will be closed automatically.
T.38 Fax Function	Check the box to enable T.38 fax function. Error Correction Mode –choose a mode for error correction.
DND (Do Not Disturb) mode	Set a period of peace time without disturbing by VoIP phone call. During the period, the one who dial in will listen busy tone, yet the local user will not listen any ring tone. Index (1-15) in Schedule - Enter the index of schedule profiles to control when the phone will ring and when will not according to the preconfigured schedules. Refer to section Application >>Schedule for detailed configuration. Index (1-60) in Phone Book - Enter the index of phone book profiles. Refer to section DialPlan –Phone Book for detailed configuration.
CLIR (hide caller ID)	Check this box to hide the caller ID on the display panel of the phone set.
Call Waiting	Check this box to invoke this function. A notice sound will appear to tell the user new phone call is waiting for your response. Click hook flash to pick up the waiting phone call.
Call Transfer	Check this box to invoke this function. Click hook flash to initiate another phone call. When the phone call connection succeeds, hang up the phone. The other two sides can communicate, then.

Default SIP Account	You can set SIP accounts (up to six groups) on SIP Account page. Use the drop down list to choose one of the profile names for the accounts as the default one for this phone setting. Play dial tone only when account registered - Check this box to invoke the function.

In addition, you can press the **Advanced** button to configure tone settings, volume gain, MISC and DTMF mode. **Advanced** setting is provided for fitting the telecommunication custom for the local area of the router installed. Wrong tone settings might cause inconvenience for users. To set the sound pattern of the phone set, simply choose a proper region to let the system find out the preset tone settings and caller ID type automatically. Or you can adjust tone settings manually if you choose User Defined. TOn1, TOff1, TOn2 and TOff2 mean the cadence of the tone pattern. TOn1 and TOn2 represent sound-on; TOff1 and TOff2 represent the sound-off.

VoIP >> Phone Settings

Advance Settings >> Phone1

Tone Settings										
Region	Caller ID Type		TOn1		TOff1		TOn2		TOff2	
	Low Freq(Hz)	High Freq(Hz)	Ton 1 (msec)	Ton 2 (msec)	Ton 1 (msec)	Ton 2 (msec)	Ton 1 (msec)	Ton 2 (msec)	Ton 1 (msec)	Ton 2 (msec)
Dial tone	350	440	0	0	0	0	0	0	0	0
Ringing tone	440	480	1000	2000	0	0	0	0	0	0
Busy tone	400	620	500	500	0	0	0	0	0	0
Congestion tone	480	620	250	250	0	0	0	0	0	0

Volume Gain		DTMF	
Mic Gain(1-10)	5	DTMF Mode	Outland (H.323/301)
Speaker Gain(1-10)	5	Playback Type (RFC2833)	101
MISC		☐ Replace + digit in caller ID to 00	
Dial Tone Power Level (1-50)	27		
Ring Frequency (10-50Hz)	25		
Call Waiting Tone Power Level (1-30)	13		
Interdigit Timeout (1-10 sec)	4		

Available settings are explained as follows:

Item	Description
Region	Select the proper region which you are located. The common settings of Caller ID Type, Dial tone, Ringing tone, Busy tone and Congestion tone will be shown automatically on the page. If you cannot find out a suitable one, please choose User Defined and fill out the corresponding values for dial tone, ringing tone, busy tone, congestion tone by yourself for VoIP phone. Also, you can specify each field for your necessity. It is recommended for you to use the default settings for VoIP communication.
Volume Gain	Mic Gain (1-10)/Speaker Gain (1-10) - Adjust the volume of microphone and speaker by entering number from 1- 10. The larger of the number, the louder the volume is.
MISC	Dial Tone Power Level - This setting is used to adjust the

	loudness of the dial tone. The smaller the number is, the louder the dial tone is. It is recommended for you to use the default setting. Call Waiting Tone Power Level - This setting is used to adjust the loudness of the call waiting tone. The smaller the number is, the louder the tone is. It is recommended for you to use the default setting. Interdigit Timeout -Type a value in this field to specify time limit for interdigit.
DTMF	DTMF Mode –There are four DTMF modes for you to choose. ● InBand - Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone. ● Out Band - Choose this one then the Vigor will capture the keypad number you pressed and transform it to digital form then send to the other side; the receiver will generate the tone according to the digital form it receive. This function is very useful when the network traffic congestion occurs and it still can remain the accuracy of DTMF tone. ● SIP INFO- Choose this one then the Vigor will capture the DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message. Payload Type (rfc2833) - Type a number from 96 to 127, the default value was 101. This setting is available for the OutBand (RFC2833) mode. Replace + digit in caller ID to - For international phone call, the phone number could add a '+' sign, for example, +8865972727. However, the caller ID (DTMF type especially) can not display '+' at all. Therefore, this function can be enabled to give another number to replace the plus sign, for example, "+" can be replaced by "00". Then the above phone number will become 008865972727. When the callee receives such number, he can use re-dial function to dial back to the caller.

IV-1-6 Status

From this page, you can find codec, connection and other important call status for each port.

VoIP => Status

Status													Refresh Seconds	Refresh
Port	Status	Codec	PeerID	Elapse(hh:mm:ss)	Tx Pkts	Rx Pkts	Rx Losses	Rx Jitter(ms)	In Calls	Out Calls	Miss Calls	Speaker Gain		
Phone1	IDLE			00:00:00	0	0	0	0	0	0	0	5		
Phone2	IDLE			00:00:00	0	0	0	0	0	0	0	5		

Log					
Date(hh:mm:ss:yyyy)	Time(hh:mm:ss)	Direction(hh:mm:ss)	InCallPkt(s)	Amount (P)	Peer (P)
00-00-0	00:00:00	00:00:00	-	-	
00:00-0	00:00:00	00:00:00	-	-	
00-00-0	00:00:00	00:00:00	-	-	
00:00-0	00:00:00	00:00:00	-	-	
00-00-0	00:00:00	00:00:00	-	-	
00:00-0	00:00:00	00:00:00	-	-	
00-00-0	00:00:00	00:00:00	-	-	
00:00-0	00:00:00	00:00:00	-	-	
00-00-0	00:00:00	00:00:00	-	-	
00:00-0	00:00:00	00:00:00	-	-	

xxxxxxxx: VoIP is encrypted.
xxxxxxxx: VoIP isn't encrypted

Available settings are explained as follows:

Item	Description
Refresh Seconds	Specify the interval of refresh time to obtain the latest VoIP calling information. The information will update immediately when the Refresh button is clicked.
Port	It shows current connection status for Phone(s) ports.
Status	It shows the VoIP connection status. IDLE - Indicates that the VoIP function is idle. HANG_UP - Indicates that the connection is not established (busy tone). CONNECTING - Indicates that the user is calling out. WAIT_ANS - Indicates that a connection is launched and waiting for remote user's answer. ALERTING - Indicates that a call is coming. ACTIVE-Indicates that the VoIP connection is launched.
Codec	Indicates the voice codec employed by present channel.
PeerID	The present in-call or out-call peer ID (the format may be IP or Domain).
Elapse(hh:mm:ss)	The format is represented as hours:minutes:seconds.
Tx Pkts	Total number of transmitted voice packets during this connection session.
Rx Pkts	Total number of received voice packets during this

	connection session.
Rx Losses	Total number of lost packets during this connection session.
Rx Jitter	The jitter of received voice packets.
In Calls	Accumulation for the times of in call.
Out Calls	Accumulation for the times of out call.
Miss Calls	Accumulation for the times of missing call.
Speaker Gain	The volume of present call.
Log	Display logs of VoIP calls.

IV-1-7 Diagnostics

VoIP Diagnostics is used for diagnosing if VoIP phone failure is caused by different tone or caller ID.

VoIP >> Diagnostics

VoIP Diagnostics

Caller ID Tone

IV-1-7-1 Caller ID

VoIP >> VoIP Diagnostics

Send Caller ID

FXS 1	FXS 2

Current type: FSK_LTSI

Caller ID used to send:

Item	Type	Status
☒	FSK_LTSI	Untest
☐	FSK_FTSI (UK)	Untest
☐	FSK_BELLGURL (US/NU)	Untest
☐	DTMF	Untest
☐	DTMF (UK)	Untest
☐	DTMF (SFIM) (FIN)	Untest

Set

Test

IV-1-7-2 Tone

VoIP => VoIP Diagnostics

Send Tone

FXS 1		FXS 2				
Region		User Defined ▼				
	Low Freq(Hz)	High Freq(Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)
Dial tone	350	440	0	0	0	0
Ringling tone	400	450	400	200	400	2000
Busy tone	400	0	0	0	0	0
Congestion tone	400	0	400	300	225	125

Item	Type	Status
☐	Dial tone	Untest
☐	Busy Tone	Untest
☐	Congestion tone	Untest

Part V VPN



VPN



SSL VPN



Certificate
Management

A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link.

It is a form of VPN that can be used with a standard Web browser.

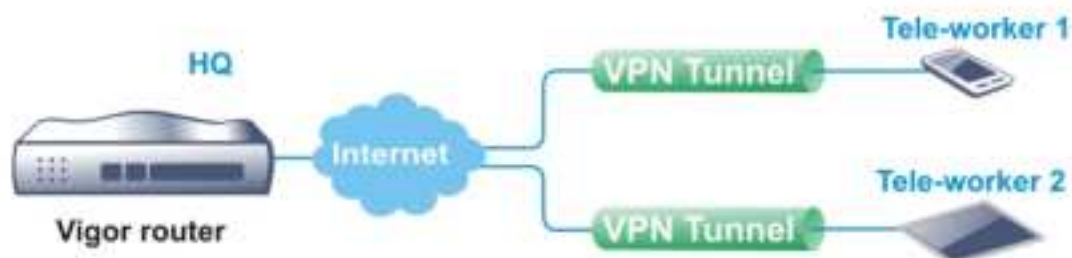
A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Here Vigor router support digital certificates conforming to standard X.509.

V-1 VPN and Remote Access

A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link.

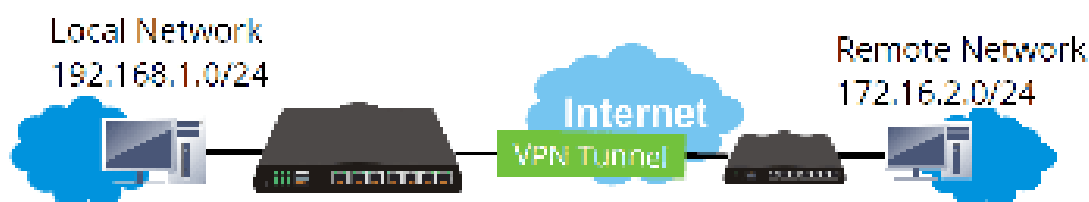
The VPN built is suitable for:

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



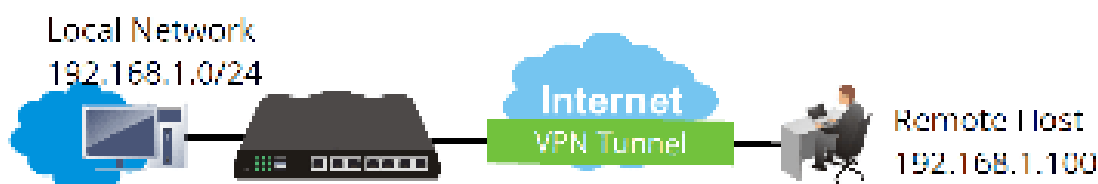
Site-to-Site (LAN-to-LAN)

- A connection between two router's LAN networks.
- Allows employees in branch offices and head office to share the same network resources.

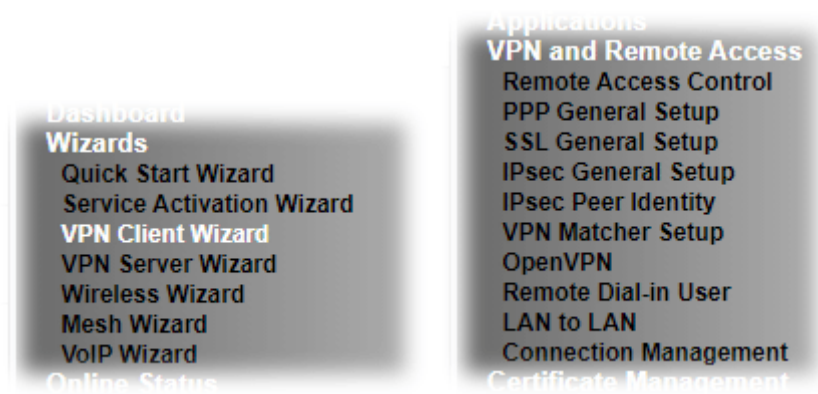


Remote Access (Remote Dial-in)

- A connection between the remote host and router's LAN network. The host will use an IP address in the local subnet.
- Allows employees to access the company's internal resources when they are traveling.



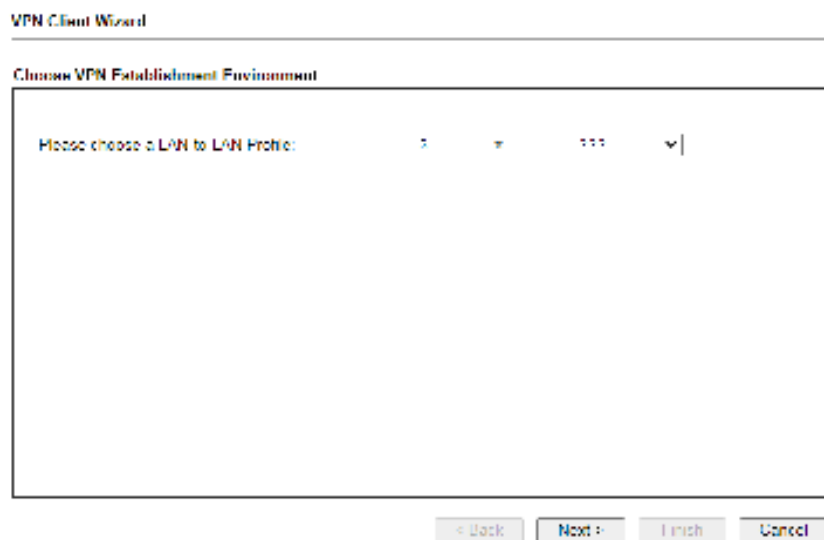
Web User Interface



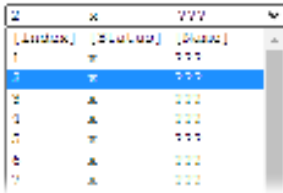
V-1-1 VPN Client Wizard

The VPN Client Wizard will configure the router as a **client** to connect to a remote VPN server using a LAN-to-LAN VPN tunnel. The wizard will guide you through the setup process.

1. On the menu bar, click on **Wizards**, and then **VPN Client Wizard**.



Available settings are explained as follows:

Item	Description
Please choose a LAN-to-LAN Profile	The profile used to store this tunnel configuration. Selecting an index that has already been setup previously will result in the existing setup getting overwritten by the wizard. 

- 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 IPsec XAuth IPsec IKEv2/FAP (only for NAT Mode) L2TP over IPsec OpenVPN (AES256) High IPsec IKEv1/IKEv2 SSL OpenVPN (ALG128) Medium PPTP (Encryption) Low L2TP/PPTP (None Encryption) OpenVPN (None Encryption)	Throughput Ranking: Very High L2TP/PPTP (None Encryption) High IPsec IKEv2/FAP/IKEv1/XAuth OpenVPN (UDP None Encryption) Medium L2TP over IPsec / PPTP (Encryption) OpenVPN (UDP) OpenVPN (TCP None Encryption) Low SSL/OpenVPN (TCP)

LAN-to-LAN VPN Client Mode Selection: Route Mode ▾

Select VPN Type: PPTP (Encryption) ▾

Note:

- Please use Route Mode for typical LAN-to-LAN tunnels.
- If the remote network is only expecting a single client or IP and is not configured to route the subnet then select NAT Mode.
- If you are unsure of your configuration select Route Mode.

Item	Description
LAN-to-LAN Client Mode Selection	Choose the client mode. Route Mode –All traffic between the local network and the remote network bear the originating IP addresses. Select this if the VPN server can establish routes to handle inter-LAN traffic routing. NAT Mode –The VPN client (local router) uses a single IP address assigned by the VPN server (remote router) and uses NAT to keep track of the connections. Select this if the VPN server expects only one IP address on the local network to communicate with the remote network.
Select VPN Type	Select a VPN protocol for the LAN-to-LAN tunnel. Different VPN protocols offer different levels of security and performance.

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.

If you have selected **PPTP (None Encryption)** or **PPTP (Encryption)**, the following configuration screen appears.

VPN Client Wizard

VPN Client PPTP Encryption Settings

Profile Name	777
VPN Dial Out Through	WAN1 First
☐ Always on	
Server IP/Host Name for VPN (e.g. dslayer.com or 128.45.67.89)	
Username	999
Password	Max: 120 characters
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0/24
Local Network IP	192.168.1.1
Local Network Mask	255.255.255.0/24

< Back Next > Finish Cancel

If you have selected **IPsec**, the following configuration screen appears.

VPN Client Wizard

VPN Client IPsec Settings

Profile Name	777
VPN Dial Out Through	WAN1 First
☐ Always on	
Server IP/Host Name for VPN (e.g. dslayer.com or 128.45.67.89)	
IKL Authentication Method	
☒ Pre-Shared Key	
Confirm Pre-Shared Key	
☐ Digital Signature (X.509)	
Peer ID	None
Local ID	
☒ Alternative Subject Name First	
☐ Subject Name First	
Local Certificate	None
IPsec Security Method	
☐ Medium (MD)	
☒ High (ESP)	AESE with Authentication
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0/24
Local Network IP	192.168.1.1
Local Network Mask	255.255.255.0/24

< Back Next > Finish Cancel

If you have selected **L2TP/SSL**, the following configuration screen appears.

VPN Client Wizard

VPN Client L2TP Settings

Profile Name	999
VPN Dial-Out Through	WAN1 First
☐ Always on	
Server IP/Host Name for VPN (e.g., draytek.com or 121.45.67.89)	
Username	777
Password	Max: 128 characters
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0 / 24
Local Network IP	192.168.1.1
Local Network Mask	255.255.255.0 / 24

< Back Next > Finish Cancel

If you have selected **L2TP over IPsec (Nice to Have)** or **L2TP over IPsec (Must)**, the following configuration screen appears.

VPN Client Wizard

VPN Client L2TP over IPsec (Nice to Have) Settings

Profile Name	777
VPN Dial-Out Through	WAN1 First
☐ Always on	
Server IP/Host Name for VPN (e.g., draytek.com or 123.45.67.89)	
IKL Authentication Method	
☒ Pre-Shared Key	
Confirm Pre-Shared Key	
☐ Digital Signature (X.509)	
Peer ID	None
Local ID	
☒ Alternative Subject Name First	
☐ Subject Name First	
Local Certificate	None
IPsec Security Method	
☐ Medium (MD)	
☒ High (ESP)	AESE with Authentication
Username	999
Password	Max: 128 characters
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0 / 24
Local Network IP	192.168.1.1
Local Network Mask	255.255.255.0 / 24

< Back Next > Finish Cancel

If you have selected **OpenVPN**, the following configuration screen appears.

VPN Client Wizard

VPN Client OpenVPN Encryption Settings

Profile Name	000
VPN Dial-Out Through	WAN1 First
Import OpenVPN config file	
☐ Always On	
Username	000
Password	Max: 120 characters
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0/24
Local Network IP	192.168.1.1
Local Network Mask	255.255.255.0/24

Available settings are explained as follows:

Item	Description
Profile Name	Name that identifies this profile. The maximum length of the Profile Name is 10 characters.
VPN Dial-Out Through	The WAN interface to be used for dialing out to establish the VPN tunnel. WANx First - The Router first attempts to establish the VPN tunnel using this WAN interface. When that is unsuccessful, it will attempt to use other WAN interfaces. WANx Only - The Router will establish the VPN tunnel using this WAN interface only. WANx Only: Only establish VPN if WANy down - The Router will establish the VPN tunnel using this WAN interface if the other WAN interface is offline.
Always On	If selected, the router will maintain the VPN connection.
Server IP/Host Name for VPN	Enter the IP address or hostname of the server of the remote VPN server.
Server Port (for SSL Tunnel)	Enter the port number for SSL tunnel.
IKE Authentication Method	IKE Authentication Method to be used. Choose between Pre-shared Key and Digital Signature (X.509). Pre-shared Key ● Pre-Shared Key- Specify a key for IKE authentication. ● Confirm Pre-Shared Key-Confirm the pre-shared key. Digital Signature (X.509) ● Peer ID - Select Peer ID from the dropdown list. Peer IDs are managed using VPN and Remote Access >> IPsec Peer Identity.

	● Local ID - Select Alternative Subject Name First or Subject Name First. ● Local Certificate - Select a certificate from the dropdown list. Local certificates are managed using Certificate Management >> Local Certificate.
IPsec Security Method	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.
Username	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 enter one LAN IP address (according to the real location of the remote host) for building VPN connection.
Remote Network Mask	Please enter the network mask (according to the real location of the remote host) for building VPN connection.
Local Network IP	Enter the local network IP for TCP / IP configuration.
Local Network Mask	Enter the local network mask for TCP / IP configuration.

- After you have entered all the required information, click **Next** to proceed to the confirmation page. The confirmation page shows a summary of all the settings. If you need to make adjustments to the settings, click **Back** to return to the previous page. Otherwise, select one of the following actions and click **Finish** to save the changes to the LAN-to-LAN VPN profile.

VPN Client Wizard

Please confirm your settings

LAN-to-LAN Index: 1
 Profile Name: VPN_Comp1
 VPN Connection Type: L2TP over IPsec (Must)
 VPN Dial-Out Through: WAN1 First
 Always on: Yes
 Server IP/Host Name: draytek.com
 IKE Authentication Method: Pre-Shared Key
 IPsec Security Method: AES with Authentication
 Remote Network IP: 172.16.3.89
 Remote Network Mask: 255.255.255.0
 Local Network IP: 192.168.1.1
 Local Network Mask: 255.255.255.0

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

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

Back

Next >

Finish

Cancel

Available settings are explained as follows:

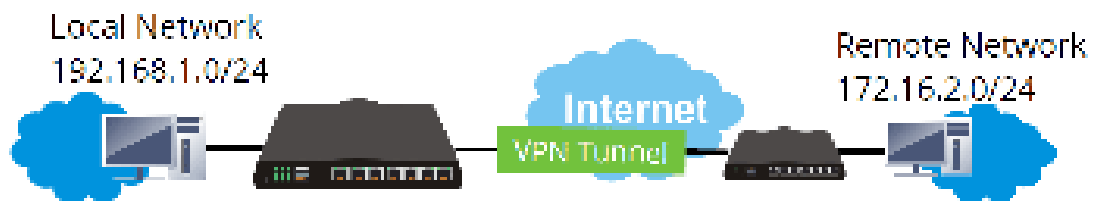
Item	Description
Go to the VPN Connection Management	Proceed to VPN and Remote Access>>Connection Management to manage VPN sessions.
Do another VPN Server Wizard Setup	Rerun the VPN Client Wizard to configure another LAN-to-LAN VPN profile.
View more detailed configuration	Open this profile in VPN and Remote Access>>LAN to LAN to make additional configuration changes.

V-1-2 VPN Server Wizard

The VPN Server Wizard can be used to set the router up as a **server** that accepts inbound VPN connections from a VPN server using a LAN-to-LAN VPN tunnel.

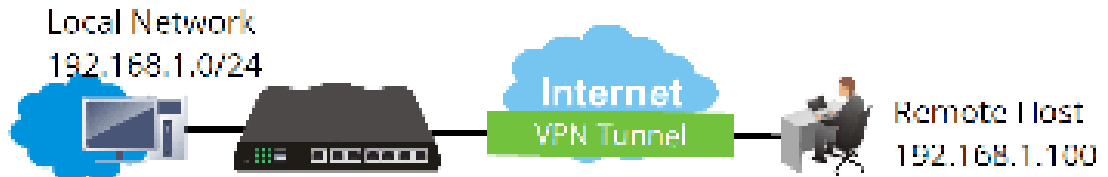
Site-to-Site (LAN-to-LAN)

- 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.



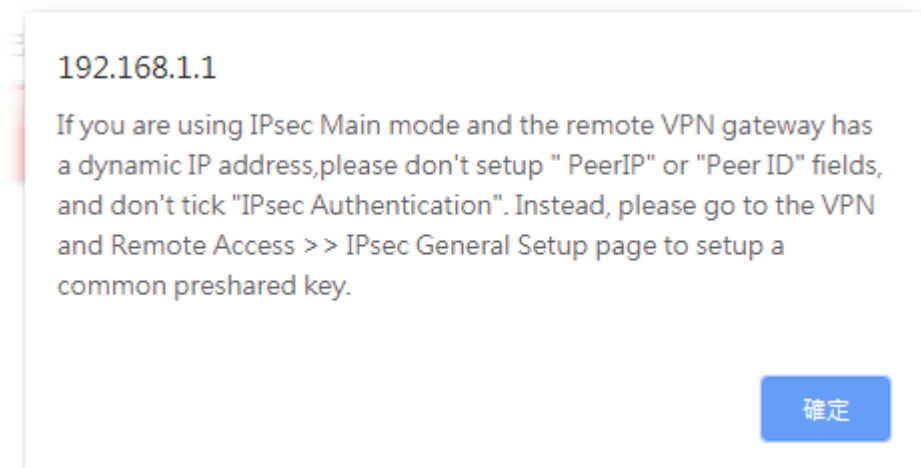
The wizard will guide you step by step through the setup process.

1. On the menu bar, click on **Wizards**, and then **VPN Server Wizard**.

Available settings are explained as follows:

Item	Description
VPN Server Mode Selection	Type of VPN Server to be configured. Site to Site VPN (LAN-to-LAN) - Configures the VPN server for inbound connections from other routers. Remote Dial-in User (Teleworker) - Configures VPN server for inbound connections from remote users.
Please choose a LAN-to-LAN Profile	If the VPN Server Mode selected was Site to Site VPN (LAN-to-LAN) , choose a LAN-to-LAN profile to store this configuration.
Please choose a Dial-in User Accounts	If the VPN Server Mode selected was Remote Dial-in User (Teleworker) , choose a Dial-in user profile to store this configuration.
Allowed Dial-in Type	Select all VPN protocols that are allowed for this LAN-to-LAN Profile or Dial-in User Account. 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.

2. After making the choices for the server profile, please click **Next**.
3. The following dialog box appears, reminding you to not configure IPsec fields if the remote location has a dynamic IP address.



Click **OK** to dismiss the dialog box and proceed to the next page.

If you have chosen to configure a LAN-to-LAN VPN profile, proceed to step 4.

If you have chosen to configure a Remote Dial-in User VPN profile, proceed to step 5.

4. The **Site to Site VPN (LAN-to-LAN)** configuration page appears as follows if you have selected **PPTP/SSL**.

VPN Server Wizard

VPN Authentication Setting

Profile Name	999
PPTP Authentication	
Username	999
Password	Max: 120 characters
Peer IP/VPN Client IP	
Site to Site Information	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0 / 24
Local Network IP	192.168.1.1
Local Network Mask	255.255.255.0 / 24

If you have selected **PPTP & IPsec & L2TP** (three types) or **PPTP & IPsec** (two types) or **L2TP with Policy (Nice to Have/Must)**, the following configuration screen appears.

VPN Server Wizard

VPN Authentication Setting

Profile Name	???
PP/IP / IPsec / L2/IP with IPsec Authentication	
Username	???
Password	Min: 128 characters
☒ Pre-Shared Key	
Confirm Pre-Shared Key	
☐ Digital Signature (X.509)	
Peer ID	None
Local ID	
Alternative Subject Name First	
Subject Name First	
Peer IP/VPN Client IP	
Peer ID	
Site-to-Site Information	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0 / 24
Local Network IP	192.168.1.1
Local Network Mask	255.255.255.0 / 24

If you have selected **IPsec**, the following configuration screen appears.

VPN Server Wizard

VPN Authentication Setting

Profile Name	???
IPsec Authentication	
☒ Pre-Shared Key	
Confirm Pre-Shared Key	
☐ Digital Signature (X.509)	
Peer ID	None
Local ID	
Alternative Subject Name First	
Subject Name First	
Peer IP/VPN Client IP	
Peer ID	
Site-to-Site Information	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0 / 24
Local Network IP	192.168.1.1
Local Network Mask	255.255.255.0 / 24

If you have selected **SSL Tunnel**, the following configuration screen appears.

VPN Server Wizard

VPN Authentication Setting

Profile Name	???
SSL Tunnel Authentication	
Username	???
Password	Max: 128 characters
Peer IP/VPN Client IP	
Site to Site Information	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0 / 24
Local Network IP	192.168.1.1
Local Network Mask	255.255.255.0 / 24

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
Profile Name	Name to identify this VPN profile.
User Name	Used by the remote LAN to establish a VPN connection. The length of the user name is limited to 11 characters.
Password	Used by the remote LAN to establish a VPN connection. The length of the password is limited to 11 characters.
IPsec / IPsec XAuth / L2TP with IPsec / SSL Tunnel Authentication	
Pre-Shared Key	For PPTP / IPsec / IPsec XAuth / L2TP with IPsec / SSL Tunnel authentication, you have to configure a pre-shared key and/or digital signature. Note that, if the remote client has a dynamic IP address, do not enable any of the settings (PSK / Digital Signature) in this section. Instead, configure the global IPsec settings by using VPN and Remote Access>>IPsec General Setup. Pre-Shared Key - Select to enter an IPsec Pre-shared Key specific to this profile. The length of the PSK is limited to 64 characters. Confirm Pre-Shared Key - Re-enter the Pre-shared Key again to confirm.
Digital Signature (X.509)	Digital Signature (X.509) - Select to enable X.509 digital signature. Peer ID - Select a predefined X.509 digital signature as the Peer ID. Peer IDs must be configured first using VPN and Remote Access>>IPsec Peer Identity. Local ID - Specifies whether the Subject Name or the Alternative Subject Name of the X.509 Peer ID is to be checked first. Select either Alternative Subject Name First or Subject Name First.
Peer IP/VPN Client IP	Enter the WAN IP address or VPN client IP address for the

	remote client. If values are specified, only connections coming from the specified IP address and/or having the specified Peer ID will be accepted.
Peer ID	Enter the ID name for the remote client. The maximum length of the peer ID is 47 characters. If the values are specified, only connections coming from the specified IP address and/or having the specified Peer ID will be accepted.
Site to Site Information	
Remote Network IP	Enter the IP address of the remote network.
Remote Network Mask	Enter the subnet mask of the remote network.
Local Network IP	Enter the local network IP for TCP / IP configuration.
Local Network Mask	Enter the local network mask for TCP / IP configuration.

5. The Remote Dial-in User (Teleworker) VPN configuration page appears as follows if you have selected **PPTP/SSL/IKEv2 EAP**.

VPN Server Wizard

VPN Authentication Setting

PPTP / IKEv2 / L2TP / SSL Tunnel Authentication	
Username	???
Password	Max: 128 characters
Peer IP/VPN Client IP	
Subnet	LAN 1 ▼

If you have selected **IKEv1/IKEv2**, the following configuration screen appears.

VPN Server Wizard

VPN Authentication Setting

IPsec/IKMP/L2 Authentication	
☒ Pre-Shared Key	
Confirm Pre-Shared Key	
☐ Digital Signature (X.509)	
Peer ID	None
Peer IP/VPN Client IP	
Peer ID	
Submit	LAN 1

< Back Next > Finish Cancel

If you have selected **IPsec XAuth/L2TP with IPsec Policy (None)**, the following configuration screen appears.

VPN Server Wizard

VPN Authentication Setting

IPsec XAuth Authentication	
Username	999
Password	Max: 120 characters
☒ Pre-Shared Key	
Confirm Pre-Shared Key	
Peer IP/VPN Client IP	
Peer ID	
Submit	LAN 1

< Back Next > Finish Cancel

If you have selected **IPsec XAuth/L2TP with IPsec Policy (Nice to Have)/L2TP with IPsec Policy (Must)**, the following configuration screen appears.

VPN Server Wizard

VPN Authentication Setting

IPsec Auth (L2TP with IPsec Authentication)	
Username	YYY
Password	Max: 128 characters
☒ Pre-Shared Key	
Confirm Pre-Shared Key	
☐ Digital Signature (X.509)	
Peer ID	None
Peer IP/VPN Client IP	
Peer ID	
Subject	LAN 1

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

If you have selected **OpenVPN**, the following configuration screen appears.

VPN Server Wizard

VPN Authentication Setting

OpenVPN Tunnel Authentication	
Username	YYY
Password	Max: 128 characters
Peer IP/VPN Client IP	
Subject	LAN 1

OpenVPN General Setup

Certificate Setup		
Generated certificate	Root Certificate:	None
	Server Certificate:	None
	Client Certificate:	None
	Trust Certificate:	None
Generate		
Note: OpenVPN authentication is based on certificate. You may either generate now (by clicking "Generate" button) or upload existing certificates to the following path: 1. Upload Server Certificate to Certificate Management > Local Certificate . 2. Upload Trusted Certificate to Certificate Management >> Trusted CA Certificate .		

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

Available settings are explained as follows:

Item	Description
User Name	Used by the remote LAN to establish a VPN connection. The length of the user name is limited to 11 characters.
Password	Used by the remote LAN to establish a VPN connection. The length of the password is limited to 11 characters.
IKEv1/IKEv2 / IPsec XAuth / L2TP with IPsec / SSL Tunnel Authentication	
Pre-Shared Key	For IKEv1/IKEv2 / IPsec / IPsec XAuth / L2TP with IPsec / SSL Tunnel authentication, you have to configure a pre-shared key and/or digital signature. Note that, if the remote client has a dynamic IP address, do not enable any of the settings (PSK / Digital Signature) in this section. Instead, configure the global IPsec settings by using VPN and Remote Access>>IPsec General Setup. Pre-Shared Key - Select to enter an IPsec Pre-shared Key specific to this profile. The length of the PSK is limited to 64 characters. Confirm Pre-Shared Key - Re-enter the Pre-shared Key again to confirm.
Digital Signature (X.509)	Digital Signature (X.509) - Select to enable X.509 digital signature. Peer ID - Select a predefined X.509 digital signature as the Peer ID. Peer IDs must be configured first using VPN and Remote Access>>IPsec Peer Identity.
Peer IP/VPN Client IP	Enter the WAN IP address or VPN client IP address for the remote client. If values are specified, only connections coming from the specified IP address and/or having the specified Peer ID will be accepted.
Peer ID	Enter the ID name for the remote client. The maximum length of the peer ID is 47 characters. If the values are specified, only connections coming from the specified IP address and/or having the specified Peer ID will be accepted.
Subnet	Select an interface.
OpenVPN General Setup	Generate - Click to generate certificate for OpenVPN authentication. Or upload existing certificates from Local Certificate or Trusted CA Certificate page.

- After finishing the configuration, click **Next** to proceed to the confirmation page.

VPN Server Wizard

Please Confirm Your Settings

VPN Environment:	Remote Access VPN (Host to LAN)
Index:	1
Username:	same
Authentication Type:	Local User Database
Allowed Service:	OpenVPN Tunnel
Peer IP/VPN Client IP:	192.168.1.55
Subnet:	LAN 1

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

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

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

Available settings are explained as follows:

Item	Description
Go to the VPN Connection Management	Proceed to VPN and Remote Access>>Connection Management to manage VPN sessions.
Do another VPN Server Wizard Setup	Rerun the VPN Server Wizard to configure another LAN-to-LAN VPN profile.
View more detailed configuration	Open this profile in VPN and Remote Access>>LAN to LAN to make additional configuration changes.

- Click **Finish** to save the profile, or **Back** to make changes, or **Cancel** to exit the wizard without saving.

V-1-3 Remote Access Control

The Vigor router supports several protocols for VPNs, all of which can be enabled or disabled independently of one another.

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

☒ Enable PPTP VPN Service
☒ Enable IPSec VPN Service
☒ Enable L2TP VPN Service
☒ Enable SSL VPN Service
☒ Enable OpenVPN Service

Note:

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

OK

Clear

Cancel

Item	Description
Enable PPTP VPN Service	This is the one of the earliest VPN protocols and is natively supported by all Microsoft Windows versions since Windows 95, all Android devices, iOS devices before version 10, and Mac OS X before version 10.12. It is easy to set up, has low overhead, and moderately secure.
Enable IPSec VPN Service	This is a network protocol that encrypts traffic between two network locations. Windows, by means of Windows Firewall, natively supports IPsec tunnels between endpoints with static IP addresses. For computers with dynamically-assigned IP addresses, DrayTek provides the SmartVPN client .
Enable L2TP VPN Service	This is a tunneling protocol used in VPNs. It does not encrypt network traffic unless used in conjunction with IPsec.
Enable SSL VPN Service	This type of VPN uses Secure Sockets Layer (SSL) and Transport Layer Security (TLS), which are also used to encrypt traffic to and from websites. Since SSL and TLS work on top of TCP and UDP, which are the most common internet protocols, they are less likely to be have issues with firewalls and gateways.
Enable OpenVPN Service	This type of VPN offers a convenient way for users to build VPN between local end and remote end.

To save changes on the page, select **OK**; to discard changes, select **Cancel**; to clear settings on this page and revert to default settings, select **Clear**.

V-1-4 PPP General Setup

This page allows configuration of Point-to-Point Protocol (PPP) used by PPTP and L2TP VPN connections. From the Main Menu select **VPN and Remote Access >> PPP General Setup** to bring up the following configuration page.

VPN and Remote Access >> PPP General Setup

PPP General Setup

PPP/MP Protocol Dial-In PPP Authentication PPTP/CHAP/MS-CHAP/MS-CHAPv2 Dial-In PPP Encryption(MPPE) Optional MPPE Mutual Authentication (PAP) Yes No Username Max: 128 characters Password Max: 120 characters IP Address Assignment for Dial-In Users when DHCP is disabled: <table border="1"><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></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	PPP Authentication Methods ☒ Remote Dial-In User ☒ RADIUS Notes: 1. Default priority is Remote Dial-In User > RADIUS. 2. Vigor router also supports Remote-IP-Address from RADIUS server to assign IP address to VPN client. While using RADIUS authentications: Assign IP from subnet: LAN1
	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														

OK

Available settings are explained as follows:

Item	Description
Dial-In PPP Authentication	PAP Only - Authenticate dial-in users using the PAP protocol only. PAP/CHAP/MS-CHAP/MS-CHAPv2 - Attempt to authenticate dial-in users using various CHAP protocols, and if the remote VPN client fails to authenticate, fall back to PAP.
Dial-In PPP Encryption (MPPE)	Specifies if PPP encryption (MPPE) is to be used for dial-in VPN connections. Optional MPPE - MPPE is optional. If the VPN client supports MPPE, PPP data will be encrypted. Require MPPE (40/128bits) - Require PPP encryption for dial-in VPN connections. Both 40- and 128-bit encryption schemes are allowed. The remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data. Maximum MPPE - Require 128-bit PPP encryption for all dial-in VPN connections.
Mutual Authentication (PAP)	Specifies if mutual authentication is to be used. Some VPN peers (e.g., certain Cisco routers) require bi-directional authentication used for providing stronger security. When mutual authentication is enabled, Username and Password fields should also be populated using values from the VPN peer. The maximum lengths of these fields are 23 and 19 characters, respectively. Yes - Enable mutual authentication.

	No - Disable mutual authentication.
IP Address Assignment for Dial-In Users when DHCP is disabled	LAN1 - When the router's DHCP server is disabled, the router will assign IP addresses to dial-in VPN users starting with the IP address specified in Start IP Address. The total number of dial-in VPN IP addresses to be given out is specified in IP Pool Counts. LAN2 ~ LANx and DMZ will be available if it is enabled. Refer to LAN>>General Setup for enabling the LAN interface.
PPP Authentication Methods	The credentials to be used for PPP authentication will be obtained from the selected sources, in the following order: Remote Dial-in User - The usernames and passwords in VPN and Remote Access >> Remote Dial-in User section will be used. RADIUS - An external RADIUS server is to be used for authentication. Please be sure to set up the RADIUS server in Applications >> RADIUS/TACACS+ section.
While using Radius or LDAP Authentication	When the dial-in VPN user is authenticated using credentials from the Remote Dial-in User section, an IP address from the LAN specified in the user profile will be assigned. When the user is authenticated using credentials from other sources (RADIUS, AD, TACACS+), the assigned IP address will be drawn from the address pool of the LAN specified here.

To save changes on the page, select **OK**.

V-1-5 SSL General Setup

SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that encrypts traffic using SSL, which is the same technology used on secured websites. Because of SSL's prominence as an encryption protocol on the Internet, most networks have few restrictions on SSL traffic, and as a result SSL VPN is more likely to work when other VPN technologies experience difficulties due to obstacles such as firewalls and Network Address Translation (NAT).

In short,

- 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.

This page determines the general configuration for SSL VPN Server and SSL Tunnel.

VPN and Remote Access >> SSL General Setup

SSL General Setup

Bind to WAN	☒ WAN1 ☒ WAN2 ☒ WAN3
Port	443 (Default: 443)
Server Certificate	self signed ▼

Available settings are explained as follows:

Item	Description

Bind to WAN	Select the WAN interfaces to accept inbound SSL VPN connections.
Port	The port to be used for SSL VPN server. This is separate from the management port (HTTPS Port) which is configured in System Maintenance>>Management . The default setting is 443.
Server Certificate	Specify the certificate to be used for SSL connections. Select a certificate from imported or generated certificates on the router, or choose Self-signed to use the router's built-in default certificate. The selected certificate can be used in SSL VPN server and HTTPS Web Proxy.

To save changes on this page, select **OK**; to discard changes, select **Cancel**.

V-1-6 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

(Click in settings for Remote Diskless users and LAN-to-LAN VPN Client with Dynamic IP)

IKE Authentication Method

Certificate: None

Preferred Local ID: Alternative Subject Name

General Pre-Shared Key: Max: 128 characters

Confirm General Pre-Shared Key:

XAuth User Pre-Shared Key: Max: 63 characters

Confirm XAuth User Pre-Shared Key:

IPsec Security Method

☒ Basic ☐ Medium ☐ High

Encryption: AES256/DES
HMAC: SHA256/SHA1/MD5
DH Group: G21828/192/160/140/120/110
AH: ☒ Enable

OK Cancel

Available settings are explained as follows:

Item	Description
IKE Authentication Method	This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPsec-related VPN connections such as L2TP over IPsec and IPsec tunnel. There are two methods offered by Vigor router for you to authenticate the incoming data coming from remote dial-in user, XAuth and Pre-Shared Key. Certificate - X.509 certificates can be used for IKE authentication. To set up certificates on the router, go to the Certificate Management section. Preferred Local ID - Specify the preferred local ID information (Alternative Subject Name First or Subject Name First) for IPsec authentication while the client is using the general setting (without a specific Peer IP or ID in the VPN profile). General Pre-Shared Key - Define the PSK key for general authentication. Confirm General Pre-Shared Key- Re-enter the characters to confirm the pre-shared key. XAuth User Pre-Shared Key - Define the PSK key for IPsec XAuth authentication. Confirm XAuth User Pre-Shared Key- Re-enter the characters to confirm the pre-shared key for IPsec XAuth. Note: Any packets from the remote dial-in user which does not match the rule defined in VPN and Remote Access>>Remote Dial-In User will be applied with the method specified here.
IPsec Security Method	Available methods include Basic, Medium and High. Each method offers different encryption, HMAC and DH Group. Basic - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active. Medium - When this option is selected, the Authentication Header (AH) protocol can be used to provide authentication to IPsec traffic. High - When this option is selected, the Encapsulating Security Payload (ESP) protocol can be used to provide authentication and encryption to IPsec traffic. Three encryption standards are supported for ESP: DES, 3DES and AES, in ascending order of security.

To save changes on the page, select **OK**; to discard changes, select **Cancel**.

V-1-7 IPsec Peer Identity

This screen allows creating profiles of subject alternative names (SANs) and distinguished names/subject names that can be used for IPsec peer authentication in LAN-to-LAN or remote user dial-in VPN connections.

VPN and Remote Access >> IPsec Peer Identity

VPN Peer ID Accounts: Set to Factory Default

Index	Enable	Name	Index	Enable	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.	☐	???
			32.	☐	???

OK Cancel

Available settings are explained as follows:

Item	Description
Set to Factory Default	Click it to clear all indexes.
Index	Click the index number of the profile the view or edit its settings.
Enable	Check to enable the profile.
Name	User-entered name that identifies the profile.

The following setup screen is shown after a profile index has been clicked.

VPN and Remote Access => IPsec Peer Identity

Profile Index : 1

☐ Enable this account

Profile Name

☒ Accept Any Peer ID

☐ Accept Subject Alternative Name

Type

IP

☐ Accept Subject Name

Country (C)

State (ST)

Location (L)

Organization (O)

Organization Unit (OU)

Common Name (CN)

Email (E)

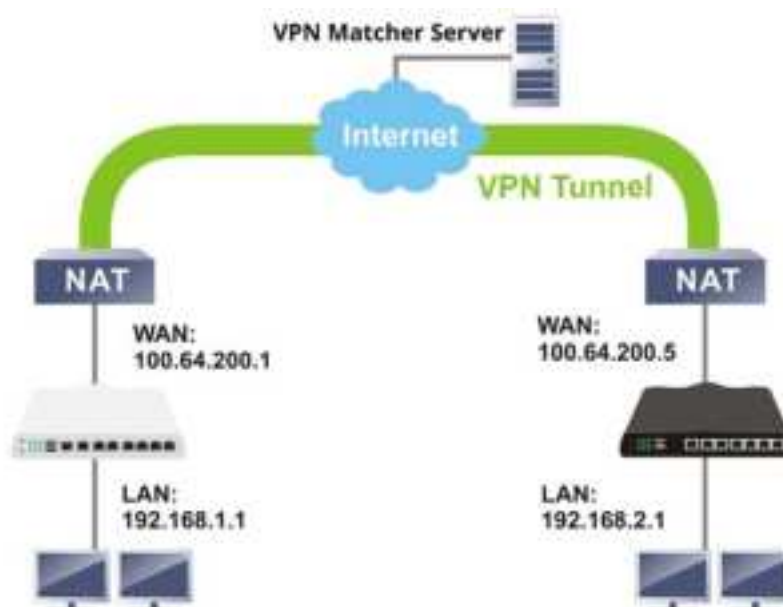
Available settings are explained as follows:

Item	Description
Enable this account	Check to enable such account profile.
Profile Name	A name that allows you to identify this profile. The maximum length of the name you can set is 32 characters.
Accept Any Peer ID	When this option is selected, the router accepts any subject alternative name or subject name as valid, regardless of the type and value.
Accept Subject Alternative Name	When this option is selected, the router accepts the type and value of the specified subject alternative name as valid authentication. Supported subject alternative types are IP Address , Domain Name and E-Mail .
Accept Subject Name	When this option is selected, the router performs peer authentication by matching the values of the different subject name fields. These fields include Country (C) , State (ST) , Location (L) , Organization (O) , Organization Unit (OU) , Common Name (CN) , and Email (E) .

To save changes on the page, select **OK**; to discard changes, select **Cancel**; to clear settings on this page and revert to default settings, select **Clear**.

V-1-8 VPN Matcher Setup

Normally, to establish VPN connection, at least one peer must have a public IP address. The VPN Matcher server can help two Draytek routers behind NAT establish a secure VPN tunnel for data transmission between each other. Refer to the following figure.



There is one limitation for the VPN connection. Both routers must be behind a cone NAT, but not symmetric NAT.

Go to **VPN and Remote Access >> VPN Matcher Setup** to open the following page.

VPN and Remote Access >> VPN Matcher Setup

☐ Enable ☒ Disable

VPN Matcher Server: :

Router List Key:

Note: You can get your Router List Key on VPN Matcher Dashboard

OK

NAT Detection

STUN Server:

Group Device List:

Available settings are explained as follows:

Item	Description
Enable / Disable	Click to enable / disable the function of VPN Matcher Setup.
VPN Matcher Server	The IP address of the DrayTek VPN Matcher server is defined as "vpn-matcher.draytek.com" with the port nubmer "31503".
Router List Key	Enter the authentication key for finding a Vigor router with the same group of this device from the VPN matcher server.

	Then set a VPN link between Vigor routers on both ends via VPN wizard.
OK	Click to save the settings.
STUN Server	Detect - Click to check if the NAT used by Vigor router is core NAT or not. If not, no VPN can be established.
Group Device List	Get List - After entering the Authkey above, click to get available Vigor router which is within the same group as this device.

V-1-9 OpenVPN

The OpenVPN protocol utilizes public keys, certificates, and usernames and passwords to authenticate the client. Traffic is carried over secure channels built upon industry-standard SSL/TLS encryption protocols.

With integrating of OpenVPN, Vigor router can help users to achieve more robust, reliable and secure private connections for business needs.

OpenVPN offers a convenient way for users to build a VPN between the local end and the remote end. There are two advantages of OpenVPN:

- It can be operated on different systems such as Windows, Linux, and MacOS.
- Based on the standard protocol of SSL encryption, OpenVPN can provide you with a scalable client/server mode, permitting multi-client to connect to a single OpenVPN Server process over a single TCP or UDP port.

In terms of credentials, the administrator can choose to let the router generate the certificates, or import certificates issued by third-party certificate authorities (CAs). When the router generates the certificates, it acts as the root CA to issue the trusted CA certificates (stored under Certificate Management >> Trusted CA Certificate), which are used to generate the server and client certificates used by OpenVPN (stored under Certificate Management >> Local Certificate). If, however, a certificate issued by a third-party CA is used, both the CA's certificate and the issued certificate need to be imported to the router in the Trusted CA Certificate and Local Certificate sections, respectively.

V-1-9-1 General Setup

OpenVPN requires the use of certificates. Before establishing OpenVPN connection, general settings for OpenVPN service shall be configured first.

VPN and Remote Access >> OpenVPN ?

OpenVPN Server Setup Client Config Import Certificate

General Setup

UDP	☒ Enable
UDP Port	1194
TCP	☒ Enable
TCP Port	1194
Cipher Algorithm	AEAD128
MAC Algorithm	SHA1
Certificate Authentication	

Certificate Setup

Certificate Source	☐ Router generated certificates
	☒ Uploading certificate to Router
Trust CA	default
Server Certificate	none

Note: OpenVPN on Vigor only support TUN device interface currently. So please setup corresponding configurations on the client side.

OK

Available settings are explained as follows:

Item	Description
General Setup	
UDP	Enable - Select checkbox to enable UDP protocol for OpenVPN connections. UDP Port - Enter the UDP port number.
TCP	Enable - Select checkbox to enable TCP protocol for OpenVPN connections. TCP Port - Enter the TCP port number.
Cipher Algorithm	Select the desired cipher algorithm. Two encryption algorithms are supported: AES128 and AES256. AES256 is more secure than AES128 but may result in lower performance because it incurs higher computational overhead.
HMAC Algorithm	HMAC stands for Hash-based Message Authentication Code. It is used to validate the data integrity and authenticity of the VPN data. Select the desired HMAC hash algorithm. Two hash algorithms, SHA1 and SHA256, are supported. SHA256 is preferred as it is more robust and reliable than SHA1.
Certificate Authentication	Select this checkbox if you would like to validate that the client certificate was issued by a trusted CA.
Certificate Setup	
Certificate Source	Select a source for the certificate to be used for OpenVPN. Router generated certificates - Router-generated certificates that will be used for OpenVPN. ● GENERATE - Click to generate a certificate. ● Delete all certificate - Click to remove all certificates generated by the router. Uploading certificates to Router - Third-party certificates will be used for OpenVPN. ● Trust CA - Use the dropdown list to select a trusted CA certificate that has already been uploaded to the router. To upload Trusted CA certificates to the router, click the Trust CA label and you will be taken to the Certificate Management >> Trusted CA Certificate page to perform the operation. ● Server Certificate - Use the dropdown list to select a server certificate that has already been uploaded to the router. To upload server certificates to the router, click the Server Certificate label and you will be taken to the Certificate Management >> Local Certificate page to perform the operation.

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

V-1-9-2 Client Config

On this page, you can create and export the configuration required for a remote OpenVPN client to connect to the router.

VPN and Remote Access via OpenVPN



OpenVPN Server Setup **Client Config** **Import Certificate**

Remote Server

☒ IP | ☐ Domain | ☐ VPN Matcher

Transport Protocol

UDP ☐ TCP ☒

Auto Dial Out

☒ Enable ☐ Disable

Set VPN as Default Gateway

☐ Enable ☒ Disable

UDP Ping

Seconds(s)

UDP Ping out

Seconds(s)

File Name

.ovpn

Client cert

.cert

Client key

.key

Mail Profile

1 ???

Mail Address

Send Email

Note

1. Please make sure the Client cert and the Client key are located in the same folder with .ovpn file.
2. Please make sure that WAN can be used as OpenVPN server.

Export

Available settings are explained as follows:

Item	Description
Remote Server	The OpenVPN client will use the IP address or domain name to connect to the router. Select either IP or Domain. IP - The OpenVPN configuration file will use the numeric IP address as the server address. Domain - The OpenVPN configuration file will use the domain as the server address. You need to ensure that the domain resolves to the IP address of a router WAN port. VPN matcher - The OpenVPN configuration file will use the VPN matcher server as the server address.
Transport Protocol	Select UDP or TCP for the protocol to be used by the OpenVPN client to connect to the router.
Auto Dial-Out	Enable - If selected, the remote client can auto-dial to this Vigor router to build an OpenVPN tunnel. Disable - Select to disable the function.
Set VPN as Default Gateway	Enable - If selected, the Vigor router will be treated as a "default" gateway for OpenVPN clients. The OpenVPN client will redirect all the traffic to the Vigor router via the OpenVPN tunnel.

	Disable - Select to disable the function.
UDP Ping	Ping remote device over the UDP control channel, if no packets have been sent for the number of seconds configured here.
UDP Ping exit	Let OpenVPN exit after the seconds set here if no reception of a ping or other packet from the remote device.
File Name	Enter the filename of the configuration file to be downloaded from the router.
CA cert	Enter the certificate authority (CA) file name obtained from 3rd party provider.
Client cert	Enter the filename of the client certificate obtained from 3rd party provider.
Client key	Enter the filename of the private key obtained from the 3rd party provider.
Mail Profile	The system administrator can send an email containing the OpenVPN client configuration to someone who needs it. Later, the recipient can use the configuration to connect to the company's Intranet. It is useful and convenient for Smart VPN Client user or employee on a business trip. Mail Address - Enter the IP address of the recipient. Send Email - After clicking this button, the recipient will receive an email with the content of OpenVPN client configuration.
Export	Click this button to download the settings on this page as a file, which can be imported into a VPN client to establish OpenVPN connections.

V-1-9-3 Import Certificate

On this page, you can import the certificate from other places for a remote OpenVPN client to connect to the router.

VPN and Remote Access >> OpenVPN



OpenVPN Server Setup **Client Config** **Import Certificate**

Import OpenVPN config file
Note:
1. TLS auth key won't be deleted even you load the first firmware.
2. Please clear the LAN-to-LAN Profile if you want to delete the TLS auth key.
Select an OpenVPN config file

Browse

Import

Click Import to upload the certificate

Import

Cancel

Import X509 Local / Trusted CA Certificate
Note:
1. Please setup the "System Maintenance >> Time and Date" correctly before signing the local/trusted CA certificate.
2. The Time Zone **MUST** be setup correctly!

Import Local Certificate

Import Trusted CA Certificate

Available settings are explained as follows:

Item	Description
Select an OpenVPN config file	Browse - Click to select a file. Import - Click to import a configuration file.
Import Local Certificate	Click to access into Local Certificate page for importing a certificate.
Import Trusted CA Certificate	Click to access into Trusted CA Certificate page for importing a certificate.

V-1-10 Remote Dial-in User

You can manage remote access by maintaining a table of remote user profiles, so that users can be authenticated via VPN connection.

Remote dial-in user profiles can be set up on this screen.

VPN and Remote Access >> Remote Dial-in User



Remote Access User Accounts:

[Set to Factory Default](#)

Index	Enable	User	Status	Index	Enable	User	Status
1	☐	???		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	☐	???	---

OK

Cancel

Restoring profile

[Restore](#)

Restore from file:

[Browse](#)

[Restore](#)

Available settings are explained as follows:

Item	Description
Set to Factory Default	Click to clear all remote-dial-in user profiles.
Index	Click the index number of the profile the view or edit its settings.
Enable	Check to enable the user profile.
User	Display the username for the specific dial-in user of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.
Status	Shows the LAN subnet and IP address assignment method. Example: LAN1-DHCP means that the IP address of the VPN connection will be drawn from the DHCP pool of the LAN1 subnet. The color of the status indicates the current state of the profile: Green - Profile is being used by a dial-in VPN connection.

	Red - Profile is not being used. Black - Profile is disabled.
Backup setting to file	Click Backup to save the configuration.
Restore From File	Click Select to choose a configuration file. Then click Restore to apply the file.

To save changes on the page, select **OK**; to discard changes, select **Cancel**.

The following setup screen is shown after a profile index has been clicked.

VPN and Remote Access == Remote Dial-In User

Index No. 1

User account and Authentication ☐ Enable this account ☒ Multiple Concurrent Connections Allowed Idle Timeout: 300 second(s) Allowed Dial-In Type ☐ PPTP ☒ IPsec Tunnel ☒ IKEv1/IKEv2 ☒ IKEv2 L2TP ☒ IPsec XAuth ☒ L2TP with IPsec Policy: Mixed ☒ SSL Tunnel ☒ OpenVPN Tunnel ☐ Specify Remote Node Remote Client IP: or Peer ID: Netlink Naming Packet: ☒ Pass ☐ Block Multicast via VPN: ☐ Pass ☒ Block (for some IGMP/IPv6/Comcast DHCP Relay, etc.) Subnet LAN 1 ☐ Assign Static IP Address 0.0.0.0	Username: 777 Password: ☐ Enable Mobile One-Time Password(mOTP) PIN Code: 4-7 digits Secret: 16-32 digits IKL Authentication Method ☒ Pre-Shared Key IKE Pre-Shared Key: ☐ Digital Signature(X.509) None IPsec Security Method ☒ Medium(AH) High(ESP) ☒ DES ☒ 3DES ☒ AES Local ID (optional): Schedule Profile None None None None

Note:

1. Username can not contain characters '*' and '@'
2. OpenVPN tunnel does not support mOTP.
3. When you are trying to use OpenVPN tunnel and the router is behind NAT, you may have to enable the VPN Match feature to bypass the NAT.
4. VPN-Match feature can only be used behind some NAT.

OK Clear Cancel

Available settings are explained as follows:

Item	Description
User account and Authentication	Enable this account - Select to enable this profile to be used by remote dial-in users. Multiple Concurrent Connections Allowed - If enabled, multiple VPN clients can connect the VPN server with the username/password set on this profile. Idle Timeout - Allowed idle time before the router disconnects the VPN connection. Default timeout value is 300 seconds.
Allowed Dial-In Type	Select all VPN protocols allowed for this profile.

	For L2TP, specify how IPsec should be applied. Options are: ● None - IPsec cannot be used with L2TP connections. ● Nice to Have - IPsec is preferred but not mandatory for L2TP connections. ● Must - IPsec is required when establish L2TP connections. Specify Remote Node - The IP address of the remote VPN client (Remote Client IP) or the Peer ID (used in IKE aggressive mode) can be optionally specified. The router will reject the connection if either of these values are entered in the profile but the remote client does not pass the value, or passes the wrong value. Netbios Naming Packet - Specifies whether to allow NetBIOS naming packets to traverse through the VPN tunnel. ● Pass - Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. ● Block - When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel. Multicast via VPN - Specifies whether to allow multicast packets to traverse through the VPN tunnel. ● 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	The VPN client will receive an IP address from the DHCP pool or IP address range specified in IP Address Assignment for Dial-In Users for the selected LAN subnet. Assign Static IP Address - Alternatively, a static IP address can be set by selecting the Assign Static IP Address checkbox. User Name - Used for PPTP, L2TP or SSL Tunnel dial-in type. Password - Used for PPTP, L2TP or SSL Tunnel dial-in type. Enable Mobile One-Time Passwords (mOTP) - Select to enable one-time passwords (Mobile-OTP). Enter the PIN Code and Secret. DrayTek's SmartVPN client has built-in support for mOTP. Third-party mOTP clients can be used to generate passwords when using other VPN clients. For more information on mOTP, visit Mobile-OTP's homepage. ● PIN Code - Enter the code for authentication (e.g., 1234). ● Secret - Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).
IKE Authentication Method	Pre-Shared Key - This checkbox is available when Remote Client IP or Peer ID is specified. Check the checkbox and click IKE Pre-shared Key to enter an IKE PSK (1-63 characters) that will be used only for this profile. Digital Signature (X.509) - To enable authentication using X.509 Peer IDs, check the checkbox then select an X.509 profile. X.509 profiles can be configured in VPN and Remote Access >> IPsec Peer Identity.
IPsec Security Method	Select all the IPsec protocols that are allowed to be used for

	this profile. Medium (AH) means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it. High (ESP) - High-Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES. Local ID (Optional)- Specify a local ID to be used when establishing a LAN-to-LAN VPN connection using IKE aggressive mode.
Schedule Profile	Set the VPN connection 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.

To save changes on the page, select **OK**; to discard changes, select **Cancel**; to clear settings on this page and revert to default settings, select **Clear**.

V-1-11 LAN to LAN

This section allows you to configure up to 32 LAN-to-LAN VPN connections. LAN-to-LAN connections can be configured to allow dial-in only, dial-out only, or both dial-in and dial-out.

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](#)

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

Change default route to: None 

☐ Pass packets from LAN in Routing mode to VPN

☒ Pass Packets to WAN when VPN disconnects

Backup/setting to file

Upload from file:  

Note

- Only 2 Lan-to-Lan profile can select "Always on".
- Only 1 Lan-to-Lan profile can select "Default Route".

Available settings are explained as follows:

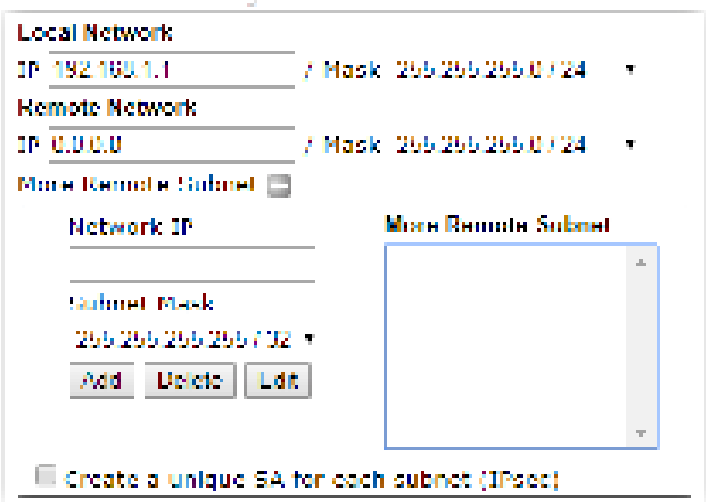
Item	Description
Set to Factory Default	Click to clear all indexes.
Index	Click the index number of the profile to view or edit its settings.
Enable	Check to enable the LAN-to-LAN VPN profile.
Name	Displays the name of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.

Available settings are explained as follows:

Item	Description
Common Settings	Enable this profile - Select to enable the profile. Profile Name –Specify a name that allows you to identify this profile. Call Direction - Specify the allowed call direction of this LAN-to-LAN profile. Four choices are available for connection mode: ● Both - Profile is to be used to initiate (dial out) or accept (dial in) connections. ● Dial-Out - Profile is to be used to initiate outgoing connections. ● Dial-In - Profile is to be used to accept incoming connections. ● GRE Tunnel - Connection is by means of a GRE tunnel. Dial-Out Through - Select the WAN connection for connections made using this profile. This setting is useful for dial-out only. ● WANx First - While connecting, the router will use WANx or LTE as the first channel for VPN connection. If WANx or LTE fails, the router will use another WAN interface instead. ● WANx Only or LTE Only - While connecting, the router will use WANx or LTE as the only channel for VPN connection. ● WAN1 Only: Only establish VPN if WAN2 down - If WAN2 failed, the router will use WAN1 for VPN connection. ● WAN2 Only: Only establish VPN if WAN1 down - If WAN1 failed, the router will use WAN2 for VPN connection. Always On - Select this option to maintain an always on dial-out connection. Idle Timeout - The router will close connection if no activity is observed in the VPN connection for this many seconds. Default value is 300 seconds. Netbios Naming Packet - Specifies whether to allow NetBIOS naming packets to traverse through the VPN tunnel. ● Pass - click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. ● Block - When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel. Multicast via VPN - Specifies whether to allow multicast packets to traverse through the VPN tunnel. ● 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.
Dial-Out Settings	VPN Server - Select the VPN protocol to be used. Server IP/Host Name - IP address or DNS host name of

	remote VPN host. Dial-Out Schedule Profile - Connect and disconnect according to schedule profiles. The default setting of this field is blank and the function will always work. User Name - Enter a username for establishing VPN connection. Password - Enter the password for establishing VPN connection. PPP Advanced Settings - Click it to expand the advanced settings for PPP. ● PPP Authentication - PAP Only - Authenticate dial-in users using the PAP protocol only. PAP/CHAP/MS-CHAP/MS-CHAPv2 - Attempt to authenticate dial-in users using various CHAP protocols, and if the remote VPN client fails to authenticate, fall back to PAP. ● VJ compression - Specifies whether to enable Van Jacobson (VJ) header compression, which improves throughput on slow connections. ● Request IP Address - Enter the IP address.
Dial-In Settings	Allowed VPN Type - Select permissible VPN protocols for dial-in connections. ● PPTP - Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below. ● IPsec Tunnel - Allow the remote dial-in user to trigger an IPsec VPN connection through Internet. ● L2TP with IPsec Policy - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below: - None - Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection. - Nice to Have - Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. - Must - Specify the IPsec policy to be definitely applied on the L2TP connection. ● SSL Tunnel - Allow the remote dial-in user to trigger an SSL VPN connection through Internet. ● Openvpn Tunnel - Allow the remote dial-in user to trigger an OpenVPN connection through Internet. Specify Remote VPN Gateway - You can specify the IP address of the remote dial-in user or peer ID (should be the same with the ID setting in dial-in type) by checking the box. Also, you should further specify the corresponding security methods on the right side. If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings. Username - This field is applicable when you select PPTP or

	L2TP with or without IPsec policy above. The length of the name is limited to 11 characters. Password - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 11 characters. PPP Advanced Settings - Click it to expand the advanced settings for PPP. ● VJ Compression - Specifies whether to enable Van Jacobson header compression, which improves throughput on slow connections. ● Assign Peer IP Address - Enter the IP address of the peer. Allowed IKE Authentication Method - This section is available when IPsec tunnel is selected as the dial-out protocol. Available options are IKE Pre-shared key and X.509 digital signature. ● Pre-Shared Key - To use a pre-shared key, select this radio-button and then click the IKE Pre-Shared Key button to enter the PSK. ● X.509 Digital Signature - To use an X.509 digital signature, select this radio button and then select an X.509 IPsec Peer Identity profile. To enable authentication using X.509 Peer IDs. X.509 profiles can be configured in VPN and Remote Access >> IPsec Peer Identity. Preferred Local ID - Select whether to first match Subject Alternative Name or Subject Name during authentication. ● Alternative Subject Name - The alternative subject name (configured in Certificate Management>>Local Certificate) will be inspected first. ● Subject Name - The subject name (configured in Certificate Management>>Local Certificate) will be inspected first. Allowed IPsec Security Method - This setting is available when IPsec Tunnel is selected as the dial-out protocol. ● AH- Authentication Header (AH) means data will be authenticated, but not be encrypted. Select to use Authentication Header protocol. By default, this option is active. ● ESP-DES/ESP-3DES/ESP-AES - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
TCP/IP Network Settings	This section configures the whether the local router applies NAT when linking the local network to the remote network, and whether IP address translation occurs when. The view changes depending on the setting of the field From first subnet to remote network, you have to do. Select NAT if the remote VPN server expects only one IP address on the local network; otherwise, select Route. TCP/IP Network Settings has different settings depending on whether NAT or Route mode is selected. Local Network – 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. ● IP / Mask - Display the local network IP and mask for TCP / IP configuration. You can modify the settings if required. Remote Network - 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. ● IP/ 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. More Remote Subnet - Click to bring up a dialog box to enter additional static routes for subnets destined for the remote network.  Mode - If the remote network only allows one IP address for the local network, select NAT; otherwise, select Route. RIP via VPN - Specifies the direction of Routing Information Protocol (RIP) packets. Available options are: ● TX/RX Both - can transmit or receive RIP packets ● TX Only - can only transmit but not receive RIP packets ● RX Only - can only receive but not transmit RIP packets ● Disable - RIP is disabled.
When the Mode is set to Routing	When Routing is selected, the available fields in the TCP/IP Network Settings section will be shown as:

	Translate Local Network - Check the box to enable the function. 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. ● Type - There are two types (Translate Whole Subnet, Translate Specific IP) for you to choose. When Translate Whole Subnet is selected as Type, available settings are listed as below: - Local Subnet - Select the LAN whose IP addresses are to be translated. - Translated IP - Specify an IP address. - More Local Subnet - Click it to add more subnets. When Translate Specific IP is selected as Type, available settings are listed as below: - Virtual IP Mapping –A pop up dialog will appear for you to specify the local IP address and the mapping virtual IP address.
When the Mode is set to NAT	When NAT is selected, the available fields in the TCP/IP Network Settings section will be shown as: RIP via VPN - Specifies the direction of Routing Information Protocol (RIP) packets. Available options are: ● TX/RX Both - can transmit or receive RIP packets ● TX Only - can only transmit but not receive RIP packets ● RX Only - can only receive but not transmit RIP packets

	● Disable - RIP is disabled. Change Default Route to this VPN tunnel - Select this option to direct all traffic that is not LAN-bound to this VPN tunnel. This option is functional when there is only one active WAN.

2. To save changes on the LAN to LAN profile page, select **OK**; to reset the entire page to blank, select **Clear**; to discard changes, select **Cancel**.

V-1-12 Connection Management

You can initiate outbound LAN-to-LAN VPN sessions, and view and disconnect all current LAN-to-LAN and dial-up VPN sessions.

You may disconnect any VPN connection by clicking **Drop** button. You may also aggressively Dial-out by using Dial-out Tool and clicking **Dial** button.

VPN and Remote Access >> Connection Management

Dial-out tool

Refresh

Dial

VPN Connection Status

All VPN StatusLAN-to-LAN VPN StatusRemote Dial-In User Status

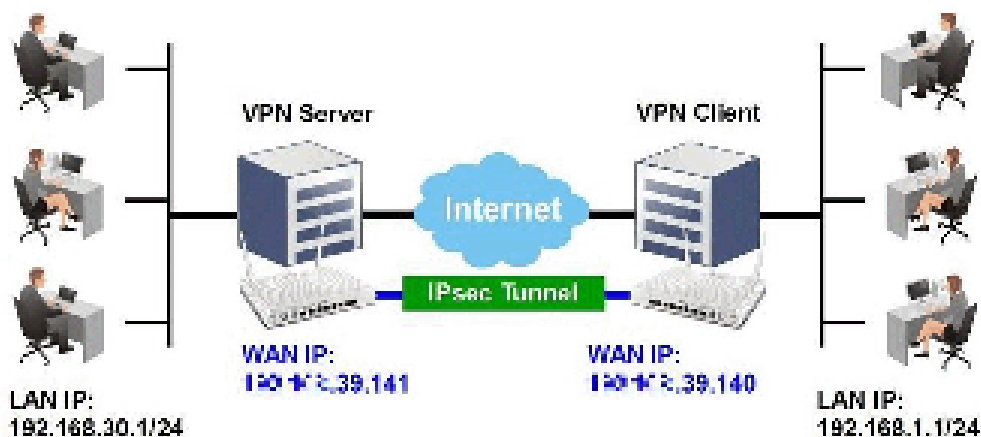
VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(bps)	Rx Pkts	Rx Rate(bps)	Up time
xxxxxxxx: Data is encrypted								
xxxxxxxx: Data isn't encrypted.								

Item	Description
Refresh	Click to manually reload the page to refresh VPN connection information.
Dial-out Tool	The Dial-out Tool section can be used to initiate outgoing LAN-to-LAN VPN sessions. Dial - Click this button to execute dial out function. If the connect is successfully made, it will show up in the VPN Connection Status section below.
VPN Connection Status	VPN - Displays the VPN profile number and the profile name. Type - Displays the VPN protocol used for the connection Remote IP - Displays the remote IP address of the VPN connection. Virtual Network - Displays the IP subnet used by the VPN connection. Tx Pkts - Displays the number of packets that have been transmitted through the VPN connection. Tx Rate(Bps) - Displays the current upstream speed of the VPN connection. Rx Pkts - Displays the number of packets that have been received through the VPN connection. Rx Rate(Bps) - Displays the current downstream speed of the VPN connection. UpTime - Displays the elapsed time of the VPN connection. Drop - Click this button to disconnect this VPN connection.

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.	???	☐	---	17.	???	☐	---
2.	???	☐	---	18.	???	☐	---
3.	???	☐	---	19.	???	☐	---
4.	???	☐	---	20.	???	☐	---

2. Set up the dial-in profile.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name	Host
☒ Enable this profile	
VPN Dial-Out Through	WAN1 First
Netbios Naming Packet	☒ Pass ☐ Block
Multicast via VPN	☐ Pass ☒ Block (for some IGMP, IP-Camera, DHCP Relay, etc.)
Cell Direction	☐ Both ☐ Dial-Out ☒ Dial-In
Always on	☐
Idle Timeout	300 second(s)
☐ Enable PING to keep IPsec tunnel alive	
PING to the IP	

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

- ☐ PPTP
- ☒ IPsec Tunnel
- ☐ L2TP with IPsec Policy: None
- ☐ SSL Tunnel

☒ Specify Remote VPN Gateway

Peer VPN Server IP: 192.168.1.10

or Peer ID:

Username: ???

Password (Max 11 char):

VT Compression: ☒ On ☐ Off

IKE Authentication Method

- ☒ Pre-Shared Key
- ☐ Digital Signature (X.509)

IKE Pre-Shared Key:

None ▼

Local ID:

- ☒ Alternative Subject Name First
- ☐ Subject Name First

IPsec Security Method

- ☒ Medium (AH)
- ☐ High (ESP)

☒ DES ☒ 3DES ☒ AES

IKE Authentication Method

Pre-Shared Key:

Confirm Pre-Shared Key:

OK

- (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: 0.0.0.0

Remote Gateway IP: 0.0.0.0

Remote Network IP: 192.168.1.1

Remote Network Mask: 255.255.255.0

Local Network IP: 192.168.30.1

Local Network Mask: 255.255.255.0

More

RIP Direction: Disable ▼

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

Route ▼

- ☒ IPsec VPN with the Same Subnets
- ☐ Change default route to this VPN tunnel (Only single WAN supports this)

OK **Clear** **Cancel**

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	???	☐	---	17	???	☐	---
2	???	☐	---	18	???	☐	---
3	???	☐	---	19	???	☐	---

2. Setup the dial-out profile.

In Common Settings,

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name: Client	Call Direction: ☐ Both ☒ Dial-Out ☐ Dial-in
☒ Enable this profile	☐ Always on:
VPN Dial-Out Through: WAN1 First	Idle Timeout: 300 second(s)
Natolas Naming Packet: ☒ Pass ☐ Block	☐ Enable PING to keep IPsec tunnel alive
Multicast via VPN: ☐ Pass ☒ Block	PING to the IP: 192.168.1.1
(for some IGMP, IP-Camera, DHCP Relay, etc.)	

- (a) Enter a **Profile Name**.
- (b) Enable this profile.
- (c) Set **Call Direction** to **Dial-Out**.

In Dial-out Setting,

2. Dial-Out Settings

Type of Server I am calling ☐ PPTP ☒ IPsec Tunnel ☐ L2TP with IPsec Policy: None ☐ SSL Tunnel	Username: Password (Max 15 char): PPP Authentication: PAP/CHAP/MS-CHAP/MS-CHAPv2 VJ Compression: ☒ On ☐ Off																														
Server IP/Host Name for VPN: (such as draytak.com or 123.45.67.89) 11.38.141	IKE Authentication Method ☒ Pre-Shared Key ☐ Digital Signature(X.509) Peer ID: None Local ID: ☒ Alternative Subject Name First ☐ Subject Name First Local Certificate: None																														
Server Port (for SSL Tunnel): 903	IPsec Security Method ☐ Medium(AH) ☒ High(ESP) DES without Authentication <input checked="" type="button" value="Advanced"/>																														
Index(1-15) in Schedule Setup: <table border="1"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td> </tr> <tr> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> </table>		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15																	

IKE Authentication Method
 Pre-Shared Key:
 Confirm Pre-Shared Key:

- (h) Select **IPsec Tunnel** for **Type of Sever I am Calling**.
- (i) Enter VPN Server's WAN IP or domain name in **Sever IP/Host Name for VPN**.
- (j) Click **IKE Pre-Shared Key** and enter the same Pre-Shared key as VPN Server.
- (k) Click on **Advanced** in IPsec Security Method.

In IKE advanced settings,

IKE advanced settings

IKE phase 1 mode	☒ Main mode	☐ Aggressive mode
IKE phase 1 proposal	Auto	
IKE phase 2 proposal	DES	
IKE phase 1 key lifetime	28800 (900 ~ 86400)	
IKE phase 2 key lifetime	3600 (600 ~ 86400)	
Perfect Forward Secrecy	☒ 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 pro
DES_(MD5/SHA)_G1, 3DES_MD5_G1, 3DES_MD5_G2, 3DES_(MD5/SHA)_G3, AES128_MD5_(G2/G3), AES256_SHA_(G2/G3), AES256_

- (l) Select **Main Mode** for IKE phase 1 mode.
 - (m) Make sure phase 1 and phase 2 proposal are using the security methods which are accepted by VPN server.
 - (n) Click **OK** to save.
3. In TCP/IP Network Settings, enter VPN Server's LAN Network in **Remote Network IP** and **Remote Network Mask**. Click **OK** to save the profile.

5. TCP/IP Network Settings

My WAN IP	0.0.0.0	RIP Direction	Disable ▼
Remote Gateway IP	0.0.0.0	From first subnet to remote network, you have to do	
Remote Network IP	192.168.30.1	Route ▼	
Remote Network Mask	255.255.255.0	☐ IPsec VPN with the Same Subnets	
Local Network IP	192.168.1.1	☐ Change default route to this VPN tunnel (Only single WAN supports this)	
Local Network Mask	255.255.255.0		
More			

OK Clear Cancel

VPN Tunnel Establishment

To initiate the VPN connection, go to **VPN and Remote Access >> Connection Management** on VPN Client, select the profile to VPN Server and click Dial.

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds : 10 Refresh

General Mode:	{ Client } 192.168.39.141	Dial
Backup Mode:		Dial
Load Balance Mode:		Dial

If all the settings are matched, the VPN will be established, and the statistics will be displayed on the same page.

VPN Connection Status Page No. Go >>

Current Page: 1

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime
1	IPsec Tunnel	192.168.39.141	192.168.30.1/24	0	0	2	0	0:0:1
{ Client } DES-No Auth		via WAN2						

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

V-2 Certificate Management

A digital certificate is an electronic document issued by a certification authority (CA) to an entity to prove ownership of a public key. It contains identifying information including the issued-to party's 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. Vigor router supports digital certificates that conform to the X.509 standard.

In this section, you can generate and manage local digital certificates, and import trusted CA certificates. Be sure that the system time is correct on the router so that certificates will not be erroneously considered to be invalid because of an incorrect system time falling outside of the certificate's valid time period. The easiest way to accomplish this is by periodically synchronizing the system time to a Network Time Protocol (NTP) server.

Web User Interface

The image below shows the menu items for Certificate Management.



V-2-1 Local Certificate

You can generate, import or view local certificates on this page.

Certificate Management > Local Certificate

X8664 Local Certificate Configuration

Name	Subject	Status	Modify	
openvpn client	AC-TWIST-HsinChun-L-HuKangU-D...	● Not Valid Yet	View	Delete
openvpn server	AC-TWIST-HsinChun-L-HuKangU-D	● Not Valid Yet	View	Delete
			View	Delete

Note:

1. Please setup the "System Maintenance" > "Time and Date" correctly before signing the local certificates.
2. The Time Zone MUST be setup correctly!!

GENERAL IMPORT RESET

Available settings are explained as follows:

Item	Description
Name	Displays the Name that identifies the certificate.
Subject	Displays the Subject Name entries of the certificate.
Status	Displays the status of the certificate. Status is one of Requesting.
Modify	View - Click to view details about the certificate. A screen that looks like the following will be displayed, showing the Subject Name, Subject Alternative Name, and the certificate content.

	 Delete - Click to remove the certificate.
Generate	Click to fill out details about a certificate, and start the generation process.
Import	Click to update an existing certificate.
Refresh	Click to refresh the page to display the latest certificate information.

GENERATE

Use this screen to submit a request to your root CA to generate a certificate.

[Certificate Management](#) >> [Local Certificate](#)

Generate Certificate Signing Request

Certificate Name	
Subject Alternative Name	
Type	IP Address
IP	
Subject Name	
Country (C)	
State (ST)	
Location (L)	
Organization (O)	
Organization Unit (OU)	
Common Name (CN)	
Email (E)	
Key Type	RSA
Key Size	2048 Bit
Algorithm	SHA 256

Generate

Available settings are explained as follows:

Item	Description
Certificate Name	Name that identifies the certificate.
Type	Select the type of Subject Alternative Name and enter its value.

Country (C)	Country in which your organization is located.
State (ST)	State or province where your organization is located.
Location (L)	City where you're your organization is located.
Organization (O)	Legal name of your organization.
Organization Unit (OU)	Department within your organization that you wish to be associated with this certificate.
Common Name (CN)	Fully-qualified domain name / WAN IP that will be used to reach your server.
Email (E)	Email address of the entry.
Key Type	Key type is hard set to RSA.
Key Size	Choose between 1024 and 2048 bit.
Algorithm	Choose between SHA-1 and SHA-256.
Generate	Click to submit generate request to the CA server.



Info

Please be noted that “Common Name” must be configured with router’s WAN IP or domain name.

After clicking the **Generate** button, you will be taken back to the main Local Certificate screen, showing the certificate request in progress:

Certificate Management >> Local Certificate

Local Certificate Configuration

Name	Subject	Status	Modify	
Router	/C=TW/ST=Hsinchu/OU=Vigor/CN=	Requesting	View	Delete
---	---	---	View	Delete
---	---	---	View	Delete

Note:

- 1. Generation of the Local Certificate is Time and Date sensitive and requires the local certificate.
- 2. The time zone must be set up correctly.

[GENERATE](#)

[IMPORT](#)

[DELETE](#)

IMPORT

Vigor router allows you to generate a certificate request and submit it the CA server, then import it as “Local Certificate”. If you have already gotten a certificate from a third party, you may import it directly. The supported types are PKCS12 Certificate and Certificate with a private key.

Click this button to import a saved file as the certification information. There are three types of local certificate supported by Vigor router.

Certificate Management >> Local Certificate

Import X509 Local Certificate

Upload Local Certificate

Select a local certificate file.

Certificate File:

Click **Import** to upload the local certificate.

Upload PKCS12 Certificate

Select a PKCS12 file.

PKCS12 file:

Password:

Click **Import** to upload the PKCS12 file.

Upload Certificate and Private Key

Select a certificate file and a matchable Private Key.

Certificate file:

Key file:

Password:

Click **Import** to upload the local certificate and private key.

Available settings are explained as follows:

Item	Description
Upload Local Certificate	Certificate file - Click Browse to select a local certificate file. Import - Click to import selected certificate file to router. Cancel - Click to return to the main Local Certificate screen.
Upload PKCS12 Certificate	It allows users to import the certificate whose extensions are usually .pfx or .p12. And these certificates usually need passwords. 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. PKCS12 file - Click Browse to select a PKCS12 certificate file. Password - Enter the password associated with the certificate and key files. Import - Click to import selected certificate file to router. Cancel - Click to return to the main Local Certificate screen.
Upload Certificate and Private Key	It is useful when users have separated certificates and private keys. And the password is needed if the private key is encrypted. Certificate file - Click Browse to select a local certificate file. Key file - Click Browse to select a private key file. Password - Enter the password associated with the certificate and key files. Import - Click to import selected certificate file to router. Cancel - Click to return to the main Local Certificate screen.

REFRESH

Click this button to refresh the information listed below.



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.

V-2-2 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.

You can create, import and view root and trusted certificate authority certificates on this screen

Certificate Management >> Trusted CA Certificate

X509 Trusted CA Certificate Configuration

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

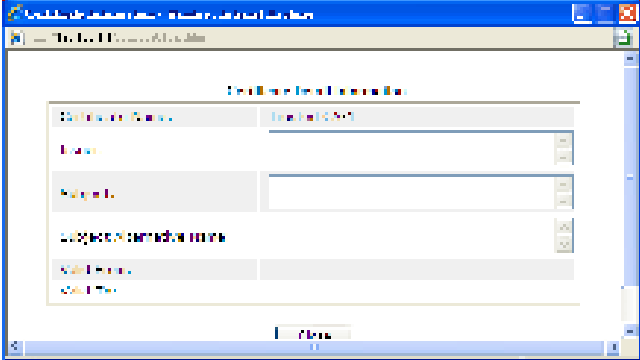
Note:

1. Please setup the "System Maintenance >> Time and Date" correctly before you try to generate a Root CA!
2. The Time Zone MUST be setup correctly!

IMPORT REFRESH

Available settings are explained as follows:

Item	Description
Create Root CA	Click to create a new root CA.
Name	Name that identifies the certificate.
Subject	Shows the Subject Name of the certificate.
Status	Displays the status of the certificate.
Modify	Create –Click to fill out details about a certificate, and start the generation process. View –Click to view details of the certificate.

	 Delete – Click to delete the certificate.
Import	Click to import an existing certificate.
Refresh	Click to refresh the page to display the latest certificate information.

Creating a RootCA

Click **Create Root CA** to open the following page.

[Certificate Management](#) >> [Root CA Certificate](#)

Generate Root CA

Certificate Name	Root CA Fill the default value
Subject Alternative Name	
Type	IP Address ▾
IP	
Subject Name	
Country (C)	
State (ST)	
Location (L)	
Organization (O)	
Organization Unit (OU)	
Common Name (CN)	
Email (E)	
Key Type	RSA ▾
Key Size	1024 Bit ▾
Algorithm	SHA-256 ▾

Available settings are explained as follows:

Item	Description
Certificate Name	Display the name of root CA. Fill the default value - Click to enter the default value for this Root CA.
Type	Select the type of Subject Alternative Name and enter its value.
Country (C)	Country in which your organization is located.

State (ST)	State or province where your organization is located.
Location (L)	City where you're your organization is located.
Organization (O)	Legal name of your organization.
Organization Unit (OU)	Department within your organization that you wish to be associated with this certificate.
Common Name (CN)	Fully-qualified domain name / WAN IP that will be used to reach your server.
Email (E)	Email address of the entry.
Key Type	Key type is hard set to RSA.
Key Size	Choose between 1024 and 2048 bit.
Algorithm	Choose between SHA-1 and SHA-256.
Generate	Click to submit generate request to the CA server.

Certificate Management => Trusted CA Certificate

X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify
Openvpn Root CA	/C=TW/ST=Hsinchu/L=HuKou/O=Dr...	☒ Not Valid Yet	Export View Delete
Trusted CA-1	/C=TW/ST=HsinChu/L=HuKou/O=Dr...	☒ Not Valid Yet	View Delete
Trusted CA-2			View Delete
Trusted CA-3	---	---	View Delete

Notice:

1. Please setup the "System Maintenance => Time and Date" correctly before you try to generate a Root CA!
2. The Time Zone MUST be setup correctly!

IMPORT RESET

Importing a Trusted CA

To import a pre-saved trusted CA certificate, please click **IMPORT** to open the following window.

Certificate Management => Trusted CA Certificate

Import X509 Trusted CA Certificate

Select a trusted CA certificate file

Click Import to upload the certification

Available settings are explained as follows:

Item	Description
Browse	Click Browse to select a local certificate file.
Import	Click to import selected certificate file to router. The one you imported will be listed on the Trusted CA Certificate window.
Cancel	Click to return to the main Trusted CA Certificate screen.

V-2-3 Certificate Backup

You can back up Local and Trusted CA certificates on the router to a file.

Certificate Management >> Certificate Backup

Certificate Backup / Restoration

Backup
Encrypt password: Max: 20 characters
Confirm password:
Click **Backup** to download certificates to your local PC as a file.

Restoration
Select a backup file to restore.

Decrypt password:
Click **Restore** to upload the file.

Available settings are explained as follows:

Item	Description
Backup	
Encrypt password/ Confirm password	Enter the password with which you wish to encrypt the certificate.
Backup	Click to download the certificate.
Restoration	
Select a backup file to restore	Click Browse to select the backup file you wish to restore.
Decrypt password	Enter the password that was used to encrypt the certificates.
Restore	Click to retrieve the certificate.

V-2-4 Self-Signed Certificate

A self-signed certificate is a *unique* identification for the device (e.g., Vigor router) which generates the certificate by itself to ensure the router security. Such self-signed certificate is signed with its own private key.

The self-signed certificate will be applied in SSL VPN, HTTPS, and so on. In addition, it can be created for free by using a wide variety of tools.

Certificate Management >> Self Signed Certificate

Self-Signed Certificate Information

[illegible]

Notes:

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!!

Generate

Click **Regenerate** to open the Regenerate Self-Signed Certificate window. Enter all requested information including certificate name (used to differentiate different certificates), subject alternative name type and relational settings for subject name. Then click GENERATE.

This page is left blank.

Part VI Security



Firewall



CSM

While the broadband users demand more bandwidth for multimedia, interactive applications, or distance learning, security has been always the most concerned. The firewall of the Vigor router helps to protect your local network against attack from unauthorized outsiders. It also restricts users in the local network from accessing the Internet.

CSM is an abbreviation of Central Security Management which is used to control IM/P2P usage, filter the web content and URL content to reach a goal of security management.

VI-1 Firewall

Basic

A network firewall monitors traffic travelling between networks, with the ability to selectively allow or block traffic using a predefined set of security rules. This helps to maintain the integrity of networks by stopping unauthorized access and the exchange of sensitive information.

Firewall Facilities

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

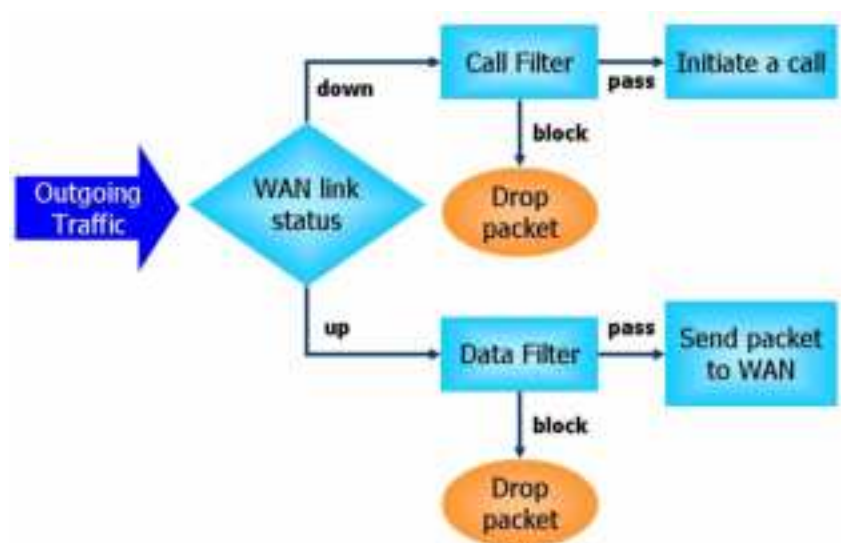
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

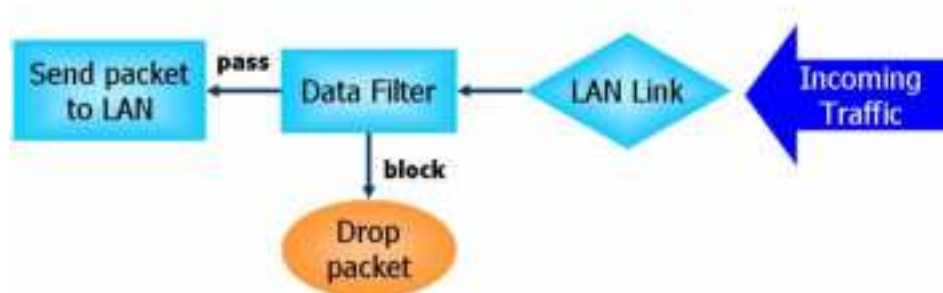
IP Filters

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** - Whenever the router needs to initiate a PPP connection (such as PPPoE, PPPoA, and VPN connections) to route traffic to the Internet, the traffic pattern that triggers the connection is checked against the Call Filter rules. If the traffic is not blocked by the filter, the router establishes the PPP connection to send the packet to the Internet.
- **Data Filter** - All traffic, both incoming and outgoing, that does not trigger a PPP connection attempt (either because a PPP connection is not necessary, or the required PPP connection has already been established) is checked against the Data Filter, and will be allowed or blocked according to the rules configured within.

The following flowcharts show how the router treats 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

DoS attacks are categorized into two types: flooding-type attacks and vulnerability attacks. Flooding-type attacks attempts to exhaust system resources while vulnerability attacks attempts to paralyze the system by exploiting vulnerabilities of protocols or operation systems.

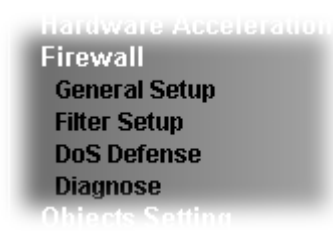
Vigor's DoS Defense functionality detects DoS attacks and mitigates their damage by inspecting every incoming packet, and malicious packets will be blocked. If Syslog is enabled, alert messages will also be sent. Abnormal traffic flow such as flood and port scan attacks that exceed allowable thresholds are also blocked.

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

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

Web User Interface

Below shows the menu items for Firewall.



VI-1-1 General Setup

General Setup Page

Such page allows you to enable / disable Call Filter and Data Filter, determine general rule for filtering the incoming and outgoing data.

Firewall > General Setup

General Setup

General Setup

Default Rule

Data Filter

☒ Enable ☐ Disable

Start Filter Set | Set Filter

☒ Allow pass inbound fragmented large packets (required for certain games and streaming)

☒ Enable Strict Security Firewall

Block routing connections initiated from WAN ☐ IPv4 ☒ IPv6

Note:
Packets are filtered by firewall functions in the following order:
1. Data Filter Sets and Rules, 2. Block routing connections initiated from WAN, 3. Default Rule

OK

Cancel

Backup Firewall:

Backup

Restore Firewall:

選擇檔案

上傳檔案到設備

Restore

Note:
This will not backup the detail setting of Quality of Service and Schedule

Available settings are explained as follows:

Item	Description
Call Filter	Check Enable to activate the Call Filter function. Assign a start filter set for the Call Filter.
Always pass inbound fragmented large packets	Certain games and video streaming service use fragmented UDP packets to transfer data. Enabling this option allows these applications to function properly. If this option is not enabled, the router will attempt to

	reassemble fragmented packets up to a certain value (e.g., 15xx-2102) kilobytes long. Packets larger than the certain value will be discarded. If this option is enabled, the router always passes fragmented packets without reassembling them, regardless of the size of the packet.
Enable Strict Security Firewall	If this option and the Web Content Filter (WCF) are both enabled, web traffic will be blocked if the WCF server fails to respond to lookup requests.
Block routing connections initiated from WAN	IPv6 - IPv6 does not make use of Network Address Translation (NAT), so all LAN hosts receive public IPv6 IP addresses that are exposed to the WAN. Enable this option to block WAN hosts from connecting to LAN hosts using IPv6. IPv4 - For LAN hosts receiving WAN IPv4 addresses using the IP routed subnet, enable this option to prevent WAN hosts from connecting to LAN hosts. This option has no effect on LAN hosts on private LAN subnets.
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.

To save changes on the page, click **OK**. To discard changes, click **Cancel**.

Traffic is filtered by firewall functions in the following order:

1. Data Filter Sets and Rules
2. Block connections initiated from WAN
3. Default Rule

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.

The default rule applies to all traffic that is not constrained by other filters or rules.

Firewall >> General Setup

General Setup

General Setup

Default Rule

Actions for default rule:

Application	Action/Profile	Syslog
Filter	Pass	
Sessions Control	0 / 60000	
Quality of Service	None	
User Management	None	
APP Enforcement	None	
URL Content Filter	None	
Web Content Filter	None	
DNS Filter	None	

Advanced Setting

Full

OK

Cancel

Backup Firewall: Backup

Restore Firewall: 選擇檔案 本地庫中恢復

Restore

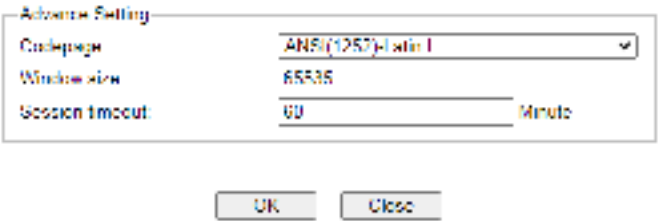
Note:

This will not backup the detail setting of Quality of Service and Schedule.

Available settings are explained as follows:

Item	Description
Filter	Select Pass or Block for the packets that do not match with the filter rules. When the setting is Block, all other fields on the page are disabled because they are not applicable.
Sessions Control	The current number of sessions is shown before the slash, followed by the maximum number of concurrent sessions allowed, which is configurable. The default maximum is 60000, which is also the upper limit of the value.
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	This setting is only available when Rule-Based is selected in User Management>>General Setup. The default firewall rule will be applied to the selected user or user group. Refer to the chapter on User Management for more details on the feature. None: User Management does not apply to the default rule.

	● User Object: The default rule only applies to the selected user. ● [Create New User]: Select this to create a new user. ● User Group: The default rule only applies to the selected User Group. ● [Create New Group]: Select this to create a new user group. ● ALL: The default rule applies to all defined users. ● Create New User or Create New Group item will appear for you to click to create a new one if there is no user profile or group profile existed. Syslog - Select to allow User Management to log messages in Syslog.
APP Enforcement	Select an APP Enforcement profile for application blocking, or None to disable APP Enforcement for the Default Rule. Select [Create New] from the dropdown list to create a new profile. Refer to the chapter on APP Enforcement for more details on the feature. Syslog - Select to allow APP Enforcement to log messages in Syslog.
URL Content Filter	Select a URL Content Filter profile to be used, or None to disable URL Content Filter for the Default Rule. Select [Create New] from the dropdown list to create a new profile. Refer to the chapter on URL Content Filter for more details on the feature. Syslog - Select to allow URL Content Filter to log messages in Syslog. Logging action is configured at the profile level in CSM>>URL Content Filter Profile, Log.
Web Content Filter	Select a Web Content Filter profile to be used, or None to disable Web Content Filter for the Default Rule. Select [Create New] from the dropdown list to create a new profile. Syslog - Select to allow Web Content Filter to log messages in Syslog. Logging action is configured at the profile level in the Web Content Filter Profile Table section in CSM>>Web Content Filter Profile, Log.
DNS Filter	Select the DNS Filter profile to be used, or None to disable DNS Filter for the Default Rule. Select [Create New] from the dropdown list to create a new profile. Syslog - Select to allow DNS Filter to log messages in Syslog. Logging action is configured at the profile level in the DNS Filter Profile Table section in CSM>>DNS Filter Profile, SysLog.
Advance Setting	Click Edit to open the configuration window for Advanced Settings. However, it is recommended to use the default settings.

	Firewall General Setup  Codepage - Sets the codepage used by the URL content filter to match URLs against keywords in profiles. Choosing the appropriate codepage can increase the accuracy of the URL Content Filter. The default value is ANSI 1252 Latin I. If the setting is None, no decoding of URL will be performed. If you are unsure of which codepage to use, please start the Syslog application, and the recommended codepage will be shown in the Codepage Information tab in the Setup dialog box.  Window size - Sets the TCP window size as described in RFC 1323. Valid values are from 0 to 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 - Sets the timeout sessions are allowed to idle before they are removed from the system.
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.

VI-1-2 Filter Setup

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

Firewall >> Filter Setup ?

Filter Setup [Set to Factory Default]

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

To edit a filter set, click on its set number. The following Filter Set page will be shown. Each filter set contains up to 7 rules.

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1
Comments : Default Data Filter

Rule	Enable	Comments	Direction	Src IP	Dst IP	Service Type	Action	CSM	Move Up	Move Down
1	☒	shutBox > DNS	LAN/RT/VPN > WAN	Any	Any	TCP/UDP Port from 137-139 to 53	Block Immediately			Down
2	☐		LAN/RT/VPN > WAN	Any	Any	Any	Pass Immediately		UP	Down
3	☐		LAN/RT/VPN > WAN	Any	Any	Any	Pass Immediately		UP	Down
4	☐		LAN/RT/VPN > WAN	Any	Any	Any	Pass Immediately		UP	Down
5	☐		LAN/RT/VPN > WAN	Any	Any	Any	Pass Immediately		UP	Down
6	☐		LAN/RT/VPN > WAN	Any	Any	Any	Pass Immediately		UP	Down
7	☐		LAN/RT/VPN > WAN	Any	Any	Any	Pass Immediately		UP	

Filter Set 1 2 3 4 5 6 7 8 9 10 11 12 Next Filter Set: None

☐ Wizard Mode: most frequently used settings in three pages
☒ Advanced Mode: all settings in one page

OK Cancel

Available settings are explained as follows:

Item	Description
Rule	To edit the filter rule, click the filter rule number to bring up the Edit Filter Rule page. See the following section for details on the Edit Filter Rule page.
Enable	Select to enable the filter rule.
Comments	Optional comment entered in the settings page to identify the rule.
Direction	Displays the direction of packet.
Src IP / Dst IP	Displays the IP address of source /destination.
Service Type	Displays the type and port number of the packet.

Action	Displays the packets to be passed /blocked.
CSM	Displays the content security managed
Move Up/ Down	Use Up or Down link to change the order of the filter rules.
Next Filter Set	Select the filter set for the firewall to process after the current filter set, or None if the current filter set is the last one to be processed. Be careful not to create a loop when setting next filter sets.
Wizard Mode	Allow to configure frequently used settings of filter rule via three setting pages.
Advance Mode	Allow to configure detailed settings of filter rule in one page.

To use Wizard Mode, simple do the following steps:

1. Click the **Wizard Mode** radio button.
2. Click **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. LAN/RT/VPN -> WAN LAN/RT/VPN -> WAN LAN/RT/VPN -> WAN WAN -> LAN/RT/VPN LAN/RT/VPN -> LAN/RT/VPN End IP Address 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	(=) - 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.

- 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 block. Please

The current setting is:

☒ Pass Immediately

APP Enforcement: None

URL Content Filter: None

Web Content Filter: None

DNS Filter: None

☐ Block Immediately

Back Next Finish Cancel

Available settings are explained as follows:

Item	Description
Pass Immediately	Packets matching the rule will be passed immediately. APP Enforcement - Select an APP Enforcement profile for application blocking, or None to disable APP Enforcement for the Default Rule. Select [Create New] from the dropdown list to create a new profile. Refer to the chapter on APP Enforcement for more details on the feature. URL Content Filter - Select a URL Content Filter profile to be used, or None to disable URL Content Filter for the Default Rule. Select [Create New] from the dropdown list to create a new profile. Refer to the chapter on URL Content Filter for more details on the feature. Web Content Filter - Select a Web Content Filter profile to be used, or None to disable Web Content Filter for the Default Rule. Select [Create New] from the dropdown list to create a new profile. DNS Filter - Select the DNS Filter profile to be used, or None to disable DNS Filter for the Default Rule. Select [Create New] from the dropdown list to create a new profile.

Block Immediately	Packets matching the rule will be dropped immediately.

- After configuring the above settings, 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		xNetsUser > DNS	
Direction			
LAN/RT/VPN > WAN			
Criteria			
Source IP	Any		
Destination IP	Any		
Protocol	TCP/UDP, Port from 137 ~ 139 to 53		
More options			
Block Immediately		APP Enforcement:	None
		URL Content Filter:	None
		Web Content Filter:	None
		DNS Filter:	None

Back Next Finish Cancel

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

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

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

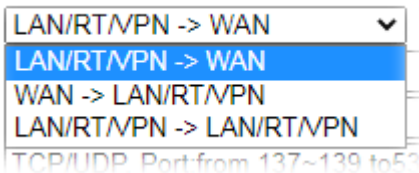
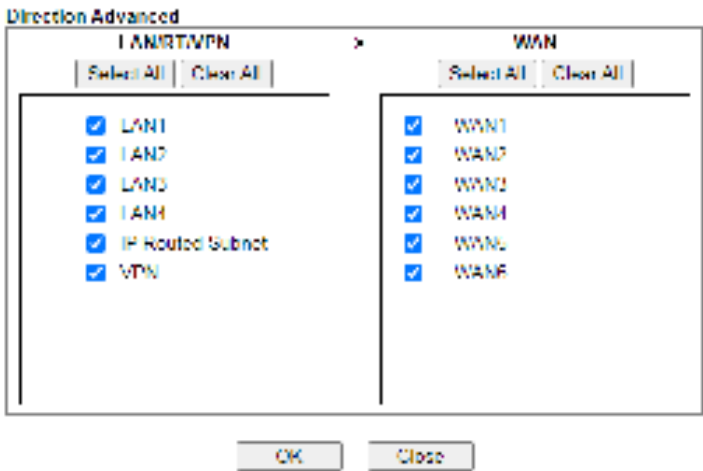
Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 1

☒ Enable	
Comments	xNetsUser > DNS
Schedule Profile	None None None None Clear sessions when schedule is ON
Direction	LAN/RT/VPN > WAN Advanced
Source IP/Country	Any Edit
Destination IP/Country	Any Edit
Service Type	TCP/UDP, Port from 137 ~ 139 to 53 Edit
Fragments	Don't Care
Application Filter	Action/Profile: Block Immediately Syncing: —
Branch to Other Filter Set	None
Session Control	On 50000
MAC Bind IP	None-Strict
Quality of Service	None
User Management	None
APP Enforcement	None
URL Content Filter	None
Web Content Filter	None
DNS Filter	None
Advanced Setting	Full

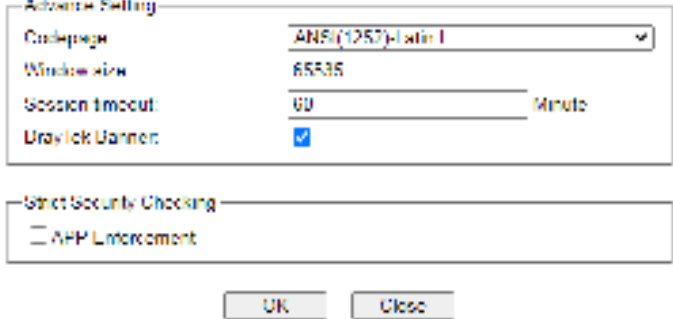
OK Clear Cancel

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable the filter rule.
Comments	Enter filter set comments/description. Maximum length is 14-character long.
Schedule Profile	Select Schedule indexes to allow the rule to be enabled at specific times. You may choose up to 4 out of the 15 schedules in Applications >> Schedule. The rule is always enabled when no indexes have been selected.
Clear sessions when schedule ON	Select this option to clear existing sessions when the rule is changes is enabled by a schedule profile. All connections will be reset.
Direction	Specify the direction of traffic flow to which this filter rule applies. Note that when the rule belongs to the Call Filter, the WAN -> LAN/RT/VPN option has no effect as Call Filter applies only to outgoing traffic.  Note: RT stands for the routing domain for 2nd subnet or other LAN. Advanced - After choosing the direction, click the Advanced button to specify interfaces for traffic flow. 
Source IP/ Country and Destination IP / Country	Click Edit to bring up the following dialog box to configure the source and destination IP addresses or country objects.

	To set the IP address manually, please choose an Address Type and enter required information. Address Type - Select from one of the following: ● Any Address - All IP addresses ● Single Address - Enter one IP address in Start IP address ● Range Address - Enter the Start and End IP Addresses ● Subnet Address - Enter the Start IP Address and the Subnet Mask. Example: Start IP Address 192.168.1.1 and Subnet Mask 255.255.255.128 means is the same as having the Start IP Address as 192.168.1.1 and the End IP Address as 192.168.1.127. ● Group and Objects - Allows selection of predefined IP Groups and IP Objects. For details on IP Groups and Objects, see the chapter on Objects Setting. ● Country Object - Allows selection of predefined country objects.
Service Type	Click Edit to bring up the following dialog box to configure the Service Type. Service Type - To set the service type manually, please choose User defined as the Service Type. ● User defined - Configure the protocol, source and destination ports manually. ● Group and Objects - Select preconfigured Service Groups or Objects. Protocol - Specify the protocol(s) which this filter rule will apply to. Source/Destination Port – ● (=) - any port that falls within the specified range ● (!=) - any port that falls outside of the specified range ● (>) - a port whose number is greater than the specified value ● (<) - a port whose number is smaller than the specified value Service Group/Object - Use the drop down list to select the

	desired Service Groups or Objects.
Fragments	Action to be taken for fragmented packets. This option is valid for Data Filter rules only. ● Don't care -No action will be taken towards fragmented packets. ● Unfragmented -Apply the rule to unfragmented packets. ● Fragmented - Apply the rule to fragmented packets. ● Too Short - Apply the rule only to packets that are too short to contain a complete header.
Filter	Action to be taken when packets match the rule. Block Immediately - Packets matching the rule will be dropped immediately. Pass Immediately - Packets matching the rule will be passed immediately. Block If No Further Match - Block the packet if this the last matching rule for this packet in the filter. Pass If No Further Match - Pass the packet if this is the last matching rule for this packet in the filter.
Branch to other Filter Set	If the packet matches the filter rule, and the Filter action is Block If No Further Match or Pass If No Further Match , you can specify the next filter set to be applied, thus skipping the rest of the rules in the current filter set.
Sessions Control	The current number of sessions is shown before the slash, followed by the maximum number of concurrent sessions allowed, which is configurable. The default maximum is 60000, which is also the upper limit of the value.
MAC Bind IP	Strict - Ensure that both the MAC address and the IP address of the source and/or destination clients. Non-Strict - Do not check the IP address when processing IP Objects that specify MAC addresses.
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	This setting is only available when Rule-Based is selected in User Management>>General Setup. The default firewall rule will be applied to the selected user or user group. Refer to the chapter on User Management for more details on the feature. ● None: User Management does not apply to the default rule. ● User Object: The default rule only applies to the selected user. ● [Create New User]: Select this to create a new user. ● User Group: The default rule only applies to the selected User Group. ● [Create New Group]: Select this to create a new user group. ● ALL: The default rule applies to all defined users. ● Create New User or Create New Group item will appear for you to click to create a new one if there is no user profile or group profile existed.

	Syslog - Select to allow User Management to log messages in Syslog.
APP Enforcement	Select an APP Enforcement profile for application blocking, or None to disable APP Enforcement for the Default Rule. Select [Create New] from the dropdown list to create a new profile. Refer to the chapter on APP Enforcement for more details on the feature. Syslog - Select to allow APP Enforcement to log messages in Syslog.
URL Content Filter	Select a URL Content Filter profile to be used, or None to disable URL Content Filter for the Default Rule. Select [Create New] from the dropdown list to create a new profile. Refer to the chapter on URL Content Filter for more details on the feature. Syslog - Select to allow URL Content Filter to log messages in Syslog. Logging action is configured at the profile level in CSM>>URL Content Filter Profile, Log.
Web Content Filter	Select a Web Content Filter profile to be used, or None to disable Web Content Filter for the Default Rule. Select [Create New] from the dropdown list to create a new profile. Syslog - Select to allow Web Content Filter to log messages in Syslog. Logging action is configured at the profile level in the Web Content Filter Profile Table section in CSM>>Web Content Filter Profile, Log.
DNS Filter	Select the DNS Filter profile to be used, or None to disable DNS Filter for the Default Rule. Select [Create New] from the dropdown list to create a new profile. Syslog - Select to allow DNS Filter to log messages in Syslog. Logging action is configured at the profile level in the DNS Filter Profile Table section in CSM>>DNS Filter Profile, SysLog.
Advance Setting	Click Edit to open the configuration window for Advanced Settings. However, it is recommended to use the default settings. Firewall >> Edit Filter Set >> Edit Filter Rule Filter Set 1 Rule 1 Advanced Setting  Codepage - Sets the codepage used by the URL content filter to match URLs against keywords in profiles. Choosing the appropriate codepage can increase the accuracy of the URL Content Filter. The default value is ANSI 1252 Latin I. If the setting is None, no decoding of URL will be performed. If you are unsure of which codepage to use, please start the Syslog application, and the recommended codepage will be

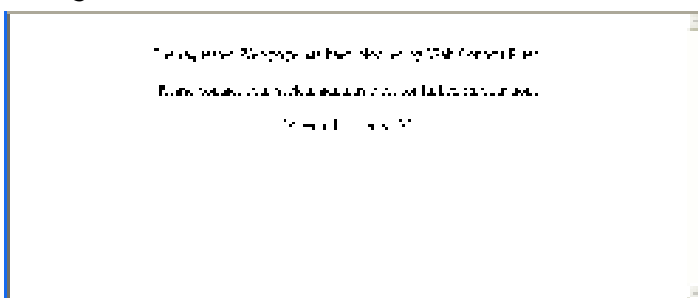
shown in the Codepage Information tab in the Setup dialog box.



Window size - Sets the TCP window size as described in RFC 1323. Valid values are from 0 to 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 - Sets the timeout sessions are allowed to idle before they are removed from the system.

DrayTek Banner - Select to display the following screen for web pages that are blocked by the Firewall. The default setting is Enabled.



Strict Security Checking

APP Enforcement - If this option is selected, when the router cannot identify the application that generated the outbound traffic due to limited system resources, the session will be blocked; if this option is not selected, the session will be allowed.

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

VI-1-3 Defense Setup

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.

VI-1-3-1 DoS Defense

To configure DoS Defense, select DoS Defense under the Firewall menu item on the Web UI menu bar.

Firewall >> Defense Setup

DoS Defense

DoS Defense

☒ Enable DoS Defense

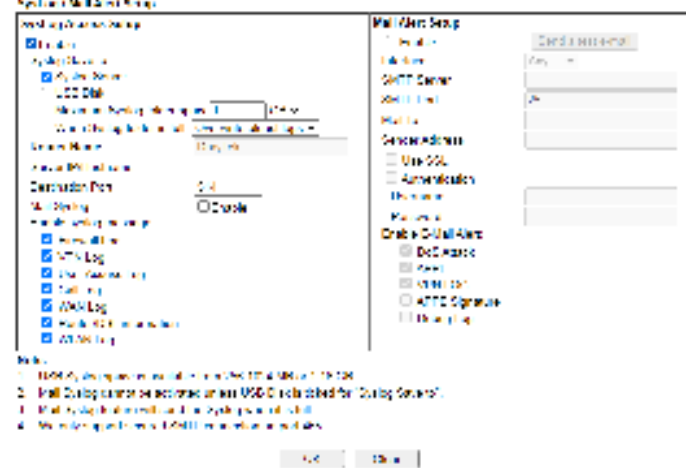
☐ Enable SYN flood defense	Threshold	2000	packets/sec
	Timeout	10	sec
☐ Enable UDP flood defense	Threshold	5000	packets/sec
	Timeout	10	sec
☐ Enable ICMP flood defense	Threshold	250	packets/sec
	Timeout	10	sec
☐ Enable Port Scan detection	Threshold	2000	packets/sec
☐ Block IP options	☐ Block TCP flag scan		
☐ Block Land	☐ Block tear drop		
☐ Block Smurf	☐ Block Ping of Death		
☐ Block trace route	☐ Block ICMP fragment		
☐ Block SYN fragment	☐ Block Unassigned Numbers		
☐ Block Fraggle Attack			

enable the defense function to prevent the attacks from hacker or crackers.

Available settings are explained as follows:

Item	Description
Enable Dos Defense	Select to enable DoS Defense. Select All - Click to select all DoS Defense options. White/Black List Option - Set white/black list of IPv4/IPv6 address.
Enable SYN flood defense	Select to enable SYN flood defense. When the arrival rate of SYN packets exceeds the Threshold value, the router will start to randomly discard TCP SYN packets for a period of time as defined in Timeout. This is to prevent TCP SYN packets from exhausting router resources. The default values of threshold and timeout are 2000 packets per second and 10 seconds, respectively.
Enable UDP flood defense	Select to enable UDP flood defense. When the arrival rate of UDP packets exceeds the Threshold value, the router will start to randomly discard TCP SYN packets for a period of time as defined in Timeout. The default values of threshold and timeout are 2000

	packets per second and 10 seconds, respectively.
Enable ICMP flood defense	Select to enable ICMP flood defense. When the arrival rate of ICMP packets exceeds the Threshold value, the router will start to randomly discard TCP SYN packets for a period of time as defined in Timeout. The default values of threshold and timeout are 250 packets per second and 10 seconds, respectively.
Enable PortScan detection	Select to enable Port Scan detection. Port Scans attack your network by sending packets to a range of ports in an attempt to find services that would respond. When Port Scan detection is enabled, the router sends warning messages when it detects port scanning activities that exceed the Threshold rate. The default threshold is 2000 packets per second.
Block IP options	Select to enable Block IP options. The Vigor router will ignore IP packets with IP option field set in the datagram header. IP options are rarely used and could be abused by attackers as they carry information about the private network otherwise not available to the external network, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messages, etc, which external eavesdroppers can use to discover details about the private network.
Block Land	Select to Block LAND attacks. LAND attacks happen when an attacker sends spoofed SYN packets with both source and destination addresses set to that of the target system, which causes the target to reply to itself continuously.
Block Smurf	Select to Block Smurf attacks. The router will ignore any broadcasting ICMP echo request.
Block trace route	Select to Block traceroutes. The router will not forward traceroute packets.
Block SYN fragment	Select to Block SYN packet fragments. The router will drop any packets having both the SYN and more-fragments bits set.
Block Fraggle Attack	Select to Block Fraggle Attacks. Broadcast UDP packets received from the Internet are blocked. Activating this feature might block some legitimate packets. Since all broadcast UDP packets coming from the Internet are blocked, RIP packets from the Internet could also be dropped.
Block TCP flag scan	Select to Block TCP Flag Scans. TCP packets with abnormal flag settings will be dropped. TCP flag scanning activities that are blocked include no flag scan, FIN without ACK scan, SYN FIN scan, Xmas scan and full Xmas scan.
Block Tear Drop	Select to Block Tear Drop attacks. Some clients may crash when they receive ICMP datagrams (packets) that exceed the maximum length. The router discards any fragmented ICMP packets having lengths greater than 1024 octets.
Block Ping of Death	Select to Block Ping of Death, where fragmented ping packets are sent to target hosts so that those hosts could crash as they reassemble the malformed ping packets.
Block ICMP Fragment	Select to Block ICMP Fragments. ICMP packets with the more-fragments bit set are dropped.

Block Unassigned Numbers	Select to Block Unassigned Protocol Numbers, and the router will block packets having unassigned protocol numbers. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and reject this kind of packets.
Warning Messages	We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client. All the warning messages related to DoS Defense will be sent to user and user can review it through Syslog daemon. Look for the keyword DoS in the message, followed by a name to indicate what kind of attacks is detected.  

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

VI-1-3-2 Spoofing Defense

Click the **Spoofing Defense** tab to open the setup page.

Firewall >> Defense Setup

DOS Defense	Spoofing Defense
ARP Spoofing Defense Log: Enable ▼	
☒ Block ARP replies with inconsistent source MAC addresses.	
☒ Block ARP replies with inconsistent destination MAC addresses.	
☒ Decline VRRP MAC into ARP table	
IP Spoofing Defense	
☒ Block IP packet from WAN with inconsistent source IP addresses.	
☐ Block IP packet from LAN with inconsistent source IP addresses.	
OK Cancel	

VI-1-4 Diagnose

The purpose of this function is to test when the router receiving incoming packet, which firewall rule will be applied to that packet. The test result, including firewall rule profile, IP address translation in packet transmission, state of the firewall functions and etc., also will be shown on this page.



Info

The result obtained by using Diagnose is offered for RD debug. It will be different according to actual state such as network connection, LAN/WAN settings and so on.

Firewall Diagnose

Mode: [ICMP] [UDP] [TCP] [IPv4] [IPv6]

Direction: [From LAN] [From WAN]

Test View

Src IP: []

Src Port: []

Src MAC: []

Dst IP: []

Dst Port: []

Analyze

Profile	Rule	Direction	Action
1	1	[From LAN]	[Deny]
2	2	[From WAN]	[Deny]

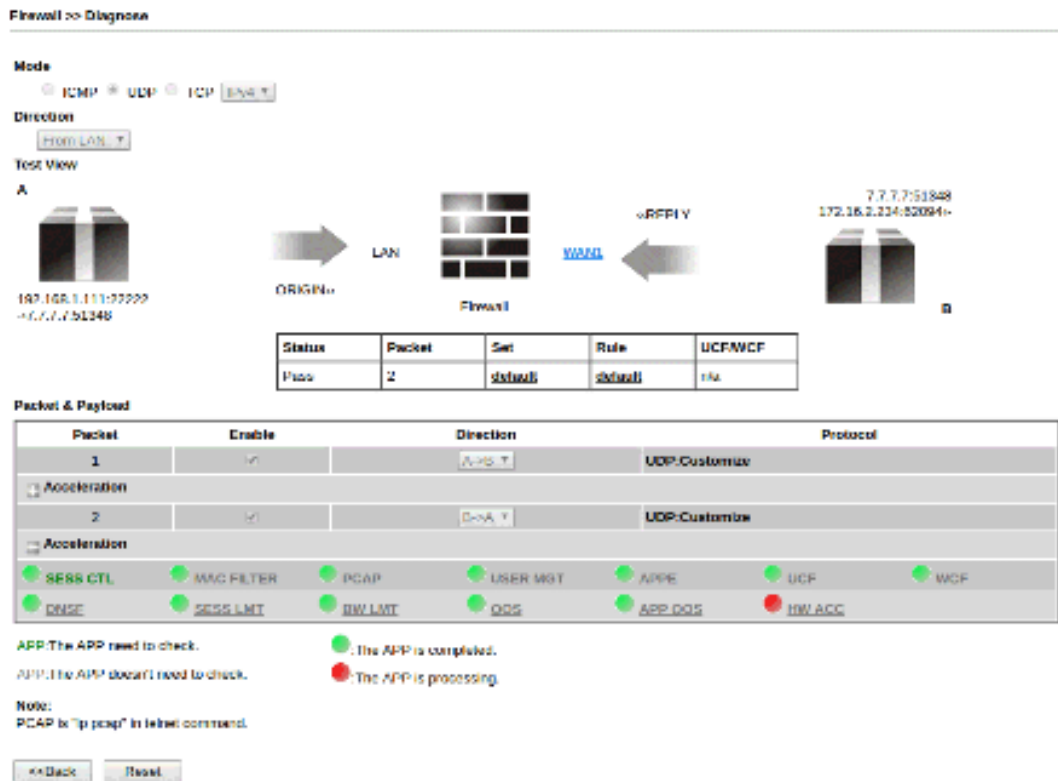
Note: []

Available settings are explained as follows:

Item	Description
Mode	To have a firewall rule test, specify the service type (ICMP, UDP, TCP) of the packet and type of the IP address (IPv4/IPv6).
Direction	Set the way (from WAN or from LAN) that Vigor router receives the first packet for test. Different way means the firewall will process the connection initiated from LAN or from WAN.
Test View	This is a dynamic display page. According to the direction specified, test view will display the figure to guide you typing IP address, port number, and MAC address. Later, after clicking the Analyze button, the information for the firewall rule profile and address translation will be shown on this page.
Src IP	Enter the IPv4/IPv6 address of the packet's source.
Src Port	Enter the port number of the packet's source.
Src MAC	Enter the MAC address of the packet's source.
Dst IP	Enter the IPv4/IPv6 address of the packet's destination.
Dst Port	Enter the port number of the packet's destination.

Packet & Payload	In firewall diagnose, two packets belong to one connection. In general, two packets are enough for Vigor router to perform this test. Enable - Check the box to send out the test packet. 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. Protocol - It displays the mode selected above and the state. 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.  ● Type - Choose Customize, DNS Query and Trace Route. ● Payload - It is available when Customzied is selected. Simply type 16 HEX characters which represent certain packet (e.g., DNS packet) if you want to set the data transferred 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.



VI-2 CSM (Central Security Management)

Content Security Management (CSM) allows the network administrator to restrict Internet traffic based on the content type, thus ensuring appropriate use of network resources and also reducing the likelihood of threats from malicious network content.

APP Enforcement Filter

The APP Enforcement Filter can be used to prevent users from using undesirable or inappropriate network applications such as online chat and peer-to-peer programs. The filter works by detecting and blocking network traffic of applications by means of traffic patterns.

URL Content Filter

The URL Content Filter scans URL strings in HTTP requests for predefined keywords to restrict browsing activities.

Web Content Filter

Users can also be prevented from browsing certain types of websites by using the Web Content Filter. This filter classifies website domain names into different categories, which can be selectively blocked.

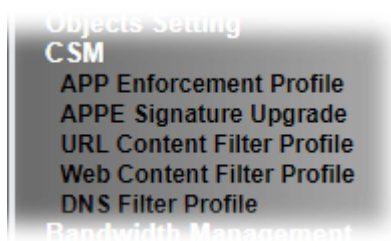
Filter profiles must first be created before these CSM Filters can be enabled. Once profiles have been configured, they can be applied to the Default Rule under Firewall>>General Setup, or Filter Rules in Filter Sets under Firewall>>Filter Setup.



Info

The priority of URL Content Filter is higher than Web Content Filter.

Web User Interface



VI-2-1 APP Enforcement Profile

Up to 32 policy profiles for APP Enforcement can be configured.

CSM >> APP Enforcement Profile

APP Enforcement Profile Table:

[Set to Factory Default](#)

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

Note:

To make APP Enforcement profile effective, please go to [Firewall >> Filter Setup](#) page to create a firewall rule and select the desired profile.

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Profile	Index of the profile. Click to bring up the configuration page of the profile.
Name	Name of the profile.

To configure a profile, click on its profile number, and the following profile configuration page will appear:

Profile Index : 1

Profile Name:

Clone Profile

Category	Application		
Instant Message	☐ AIM Login	☐ AIMWW	☐ Arcs
Select All	☐ BaibaiHi	☐ Facebook/Instagram	☐ Faim
Clear All	☐ GaduGadu Protocol	☐ ICQ	☐ IspQ
	☐ ICQ	☐ LINE	☐ LinkedIn
	☐ KikTalk	☐ KikCall	☐ Qnext
	☐ Signal	☐ Slack	☐ Snapchat
	☐ Telegram	☐ Tencent QQ	☐ UC
	☐ WebIM URL	☐ WhatsApp	☐ WhatsApp Call
VoIP			
Select All	☐ IRC Voice	☐ SkypeTeamx	☐ TeamSpeak
Clear All	☐ Telcel	☐ Wechat	
P2P	☐ Arcs	☐ Unicom	☐ Clubbox
Select All	☐ eDonkey	☐ FastTrack	☐ Gnutella
Clear All	☐ Luntune	☐ Kuwo	☐ Gocent

Available settings are explained as follows:

Item	Description
Profile Name	Name that identifies this profile. Maximum length is 15 characters.
Category	Apps are classified into several categories. Each category contains several apps to be blocked.
Clone Profile	Click it to clone settings configured by an existed profile.
Select All	Click to select all of the items on this page.
Clear All	Click to deselect all selected items.
Enable	Select this checkbox to block the app.

To save changes on the page, click **OK**. To discard changes, click **Cancel**.

VI-2-2 APPE Signature Upgrade

The APP Enforcement Profile feature identifies applications by matching their network traffic to signatures. DrayTek periodically releases APPE signature upgrades to ensure that new applications or new versions can be detected.

Upgrade checks can be performed manually or automatically.

CSM >> APPE Signature Upgrade

APP Enforcement License

Status: Inactivated

Activate

Upgrade Setting

APPE Module Version: 15.21 APPE Support List

Upgrade via interface: auto-selected (Waiting for WAN connection...)

Setup Download Server

auto-selected

Find more

Signature authentication / download message

[2024-01-01 00:00:00] Load APPE signature failed. System will use APPE default signature.

Upgrade Manually

Input

Upgrade Automatically

Scheduled Update

☒ Every: 1 (hour) 00 (minutes after the hour)

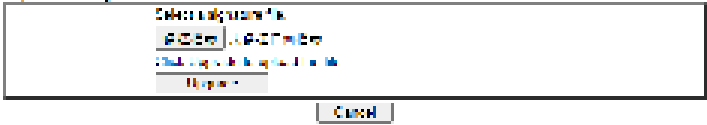
☐ Daily: 0 (hour) 00 (minute)

☐ Weekly: Sunday (day) 0 (hour) 00 (minute)

OK

Available settings are explained as follows:

Item	Description
Upgrade Setting	APPE Module Version - Display current version status of APPE signature. New version from the Internet - The Download button is enabled only when there is a newer version of APPE signature than the one present on the router. After clicking on the Download button, a dialog box will appear, displaying the release information of the new version. Click OK in the dialog box to proceed with the download. Upgrade via interface - Select a WAN interface to download the new APPE signature.
Setup Download Server	Specify a download server by typing its URL of the server. Click the <u>Find more</u> for a list of download servers. When the default value auto-selected is used, the server is determined automatically by looking up the geolocation of the WAN IP address. Signature authentication/download message -Displays download status messages.
Upgrade Manually	Use this functionality if you wish to upgrade using a

	previously-downloaded signature file. Import - Clicking the button brings up the following page.  Click Choose File to select the signature file. Click Upgrade to initiate the upgrade process.
Upgrade Automatically	Scheduled Update - Select to enable automatic periodic checking for signature updates.

Click **OK** to save changes on the page.

VI-2-3 URL Content Filter Profile

To set up URL Content Filter Profiles, click **CSM** on the Main Menu bar, and then 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.	

Note:

To make URL Content Filter profile effective, please go to Firewall >> Filter Setup page to create a firewall rule and select the desired profile.

Administration Message (Max 255 characters)

[Default Message](#)

Access to the requested web page has been blocked by URL Content Filter. Please contact your system administrator for further information.

OK

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Profile	Index number of the profile.
Name	Name that identifies the profile.
Administration Message	The message to be displayed in the browser when access to a URL has been blocked. A custom message can be entered with HTML formatting in the text box. Default Message - Click to reset the administration message to the factory default.

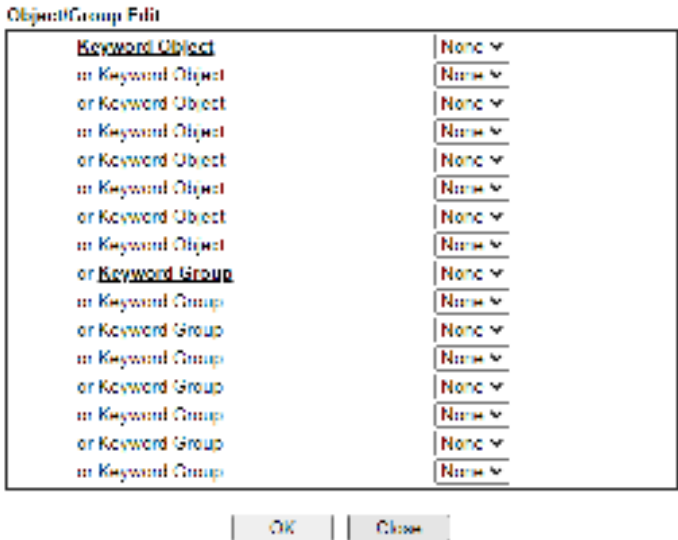
To set up a profile, click the profile number under Index column to bring up the configuration page.

Profile Index: 1

Profile Name:		
Priority:	Filter URL Access Control First ▼	Log: Block ▼
URL Access Control ☐ Enable URL Access Control ☐ Prevent web access from IP address Action: Pass ▼ Group/Object Selection: Edit ☐ Exception List Edit		
Web Feature ☐ Enable Web Feature Restriction ☐ Cookie ☐ Proxy ☐ Upload Action: Pass ▼ File Extension Profiles: None ▼		
OK Clear Cancel		

Available settings are explained as follows:

Item	Description
Profile Name	Name that identifies the URL Content Filter profile. The maximum length of the Profile Name is 15 characters.
Priority	The order of evaluation of URL Access Control and Web Feature below: Both: Pass - Router will allow access only to web resources that match conditions specified in both URL Access Control and Web Feature. The Action setting of both URL Access Control and Web Feature will be disabled and the values set to Pass. Both: Block - Router will block access to web resources that match conditions specified in both URL Access Control and Web Feature. The Action setting of both URL Access Control and Web Feature will be disabled and the values set to Block. Either: URL Access Control First - Router will block or allow access to web resources that match conditions specified in either URL Access Control or Web Feature. URL Access Control is applied first, followed by Web Feature. Either: Web Feature First - Router will block or allow access to web resources that match conditions specified in either URL Access Control or Web Feature. Web Feature is applied first, followed by URL Access Control.
Log	Pass - Only passed access attempts will be recorded in Syslog. Block - Only blocked access attempts will be recorded in Syslog. All - Both passed and blocked access attempts will be recorded in Syslog.
URL Access Control	Enable URL Access Control - Select to activate URL Access Control. Prevent web access from IP address - URLs containing IP addresses (e.g., 192.168.1.1) will be blocked. Only URLs with

	domain addresses (e.g., www.draytek.com) will be allowed. This is to prevent users from circumventing URL Access Control. Action - This setting is enabled only when Priority is set to Either: URL Access Control First or Either: Web Feature First. ● Pass – Allows access to web pages with URLs containing keywords that are in the selected keyword groups or objects. Access to other URLs is blocked. ● Block – Blocks access to web pages with URLs containing keywords that are in the selected keyword groups or objects. Access to other URLs is allowed. Exception List - Specify the object profile(s) as the exception list which will be processed in an opposite manner to the action selected above. Group/Object Selections - Shows the Keyword Groups and/or Objects selected for this URL Content Filter Profile. To add or remove Keyword Groups and Objects to the selection, click the Edit button to bring up the following screen.  Up to 8 Keyword Objects and 8 Keyword Groups can be selected. To add, remove or modify Groups or Objects, click the Keyword Object or Keyword Group hyperlinks to bring up the Objects Setting >> Keyword Object or Objects Setting >> Keyword Group pages.
Web Feature	Enable Restrict Web Feature - Check to enable the web feature restriction. Action - This setting is enabled only when Priority is set to Either: URL Access Control First or Either: Web Feature First. ● Pass - Allows access to web pages with URLs containing keywords that are in the selected keyword groups or objects. Access to other URLs is blocked. ● Block - Blocks access to web pages with URLs containing keywords that are in the selected keyword groups or objects. Access to other URLs is allowed. 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 - Select to block cookies from Internet websites. Proxy - Select to block web proxy servers that relay HTTP traffic. Upload - Select to block HTTP uploads from the LAN to the Internet.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To clear all settings, click **Clear**.

VI-2-4 Web Content Filter Profile

Trial WCF service can be activated using the **Service Activation Wizard**.

If you wish to continue using WCF beyond the trial period, you can obtain a full WCF subscription by contacting your local DrayTek channel partner or dealer. WCF subscriptions can be activated using the **Activate** link on **CSM >> Web Content Filter Profile** (described in this section) or **System Maintenance**.

From the main menu, click **CSM**, followed by **Web Content Filter Profile** to load the profile configuration page.



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>

[illegible]

Available settings are explained as follows:

Item	Description
Activate	Click to visit the MyVigor website to activate WCF service. You will need to log in to your MyVigor account to proceed with the activation process. If you do not already have a MyVigor account, you can create one at this time.
Setup Query Server	Specify a WCF query server by typing address of the server. Click the Find more for a list of query servers. When the default value auto-selected is used, the server is determined automatically by looking up the geolocation of the WAN IP address. It is recommended that the default setting auto-selected be used.
Setup Test Server	Specify a WCF test server by typing address of the server. Click the Find more for a list of test servers. When the default value auto-selected is used, the server is determined automatically by looking up the geolocation of the WAN IP address. It is recommended that the default setting auto-selected be used.
Cache	None - The router verifies every HTTP URL requested by communicating with the WCF server on the Internet. This mode provides the most precise URL matching but has the lowest performance. L1 - The router caches the HTTP URLs that have been checked against the WCF server. URLs will be looked up in the L1 cache before reaching out to the WCF server. When the cache is full, the oldest entry will be deleted to accommodate new URLs. L2 - After a URL has been checked and found to pass WCF, the source and destination IPs are cached for about 1 second in the L2 cache. This is to allow a webpage to be loaded without further verifying the same URLs against the L1 cache or the WCF server. L1+L2 Cache - The router will utilize both L1 and L2 caches.
Set to Factory Default	Clear all profile settings.
Profile	Index number of the profile.
Name	Name that identifies the profile.
Administration Message	The message to be displayed in the browser when access to a website has been blocked. A custom message can be entered with HTML formatting in the text box. You can embed the following variables in the message: %SIP% - The source IP address that attempted the HTTP access. %DIP% - The destination IP address to which access was attempted. %URL% - The URL of the destination website. %CL% - The category to which the URL belongs. %RNAME% - The name of the router. Default Message - Click to reset the administration message to the factory default.

Up to 8 WCF profiles can be set up. To configure a profile, click its profile number to bring up its configuration page. Filter profile settings are specific to WCF providers. If you already

have an active WCF subscription, activating a WCF subscription to a provider that is different from your current provider will clear all existing profile configuration.

Available settings are explained as follows:

Item	Description
Profile Name	Name that identifies the WCF profile. The maximum length of the Profile Name is 15 characters.
Log	Pass - Only passed access attempts will be recorded in Syslog. Block - Only blocked access attempts will be recorded in Syslog. All - Both passed and blocked access attempts will be recorded in Syslog.
Black/White List	Keyword objects and groups can be applied to the URL to override WCF category filtering. Enable – Select to enable blacklisting or whitelisting. Action - Action to take when a URL matches keyword group and object selections. ● Pass - Allow access to the URL. ● Block - Disallow access to the URL. URL Keywords – Displays selected keyword group and objects. Click the Edit button to modify keyword selections.
Groups and Categories	Select categories to be included in the filter. Action - Action to take when a URL matches keyword group and object selections. ● Pass - allow access to the URL. ● Block - disallow access to the URL. Select All - Click to select all categories within the group. Clear All - Click to deselect all categories within the group.

To save changes on the page, click **OK**. To discard changes, click **Cancel**.

VI-2-5 DNS Filter Profile

DNS Filter blocks or allows traffic to the WAN by intercepting DNS queries, and applying UCF and WCF rules to hostnames. DNS filtering is especially useful when you wish to restrict access of protocols other than HTTP, such as HTTPS. Note that a WCF license must have already been activated before WCF rules could be used.

To configure DNS Filter Profiles, select **CSM >> Web Content Filter Profile** from the main menu.



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.

CyM $\Rightarrow$ DNS Filter

DNS Filter Profile Table		Set to Factory Default	
Profile	Name	Profile	Name
1.		2.	
2.		3.	
3.		4.	
4.		5.	

To make DNS Filter profile effective, please go to Firewall > Filter Setup page to create a firewall rule and select the desired profile.

UNS Filter Local Setting

UNS Filter	☐ Enable	
Web Content Filter	None ▾	
URL Content Filter	None ▾	
Syslog	None ▾	
Black/White List	☐ 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) (dir) (dir op) the requested web page (dir) from %SIP% (dir to %URL% (dir) that is categorized with %CLS% cannot be blocked by SRNAML's DNS Filter.op>Please contact your system administrator for further information. (center) (fbody)

Legend:

%SIP%	Source IP ,	%URL%	URI
%CLS%	- Category ,	%SRNAML%	- Router Name



Cancel

Available settings are explained as follows:

Item	Description
DNS Filter Profile Table	DNS Filter Profiles take effect when DNS servers on the WAN are used for DNS queries. The router intercepts all outgoing DNS queries on UDP port 53 and applies WCF and UCF rules on the domain names before passing the queries to the DNS servers. IP addresses of the domains are then blocked or allowed as per applicable WCF and UCF rules. DNS Filter Profiles can be applied by selecting from Firewall filter rules. Profile - Index number of the profile. Click to bring up the configuration page for the profile entry. Name - Name that identifies the profile.
Set to Factory Default	Clear all DNS Filter profile settings.
DNS Filter Local Setting	By setting the IP address of the DNS lookup server to the router's address, the router serves as a DNS lookup proxy server. When DNS Filter Local Setting is enabled, all DNS queries sent to the router will have WCF and UCF rules applied to the hostnames, and access to the resolved IP addresses will be allowed or blocked as configured in the rules. DNS Filter - Select to enable DNS Filter Local Setting. Web Content Filter - Select a WCF profile. URL Content Filter - Select a UCF profile. Syslog - The filtering result can be recorded according to the setting selected for Syslog. ● None – No log file will be created for this profile. ● Pass – Only passed access attempts will be recorded in Syslog. ● Block – Only blocked access attempts will be recorded in Syslog. ● Both – Both passed and blocked access attempts will be recorded in Syslog. 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.
Administration Message	The message to be displayed in the browser when access to a website has been blocked. A custom message can be entered with HTML formatting in the text box. You can embed the following variables in the message: ● %SIP% - The source IP address that attempted the HTTP access. ● %DIP% - The destination IP address to which access was attempted. ● %URL% - The URL of the destination website. ● %CL% - The category to which the URL belongs. ● %RNAME% - The name of the router. Default Message - Click to reset the administration message to the factory default.

To save changes on the page, click **OK**. To discard changes, click **Cancel**.

Application Notes

A-1 How to Create an Account for MyVigor

The website of MyVigor (a server located on <http://myvigor.draytek.com>) provides several useful services (such as Anti-Spam, Web Content Filter, Anti-Intrusion, and etc.) to filtering the web pages for the sake of protecting your system.

To access into MyVigor for getting more information, please create an account for MyVigor.

Create an Account via Vigor Router

1. Click **CSM>> Web Content Filter Profile**. The following page will appear.

CSM>> Web Content Filter Profile 

Web Filter License Activate
(Status: Inactivated)

Setup Query Server	auto selected	Find more
Setup Test Server	auto selected	Find more

Web Content Filter Profile Table Cache: 1 1 1 2 Cache | [Set to Factory Default](#) |

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

Note:
To make Web Content Filter profile effective, please go to [Firewall Filter Setup](#) page to create a firewall rule and select the desired profile.

Administration Message (Max 255 characters) Default Message

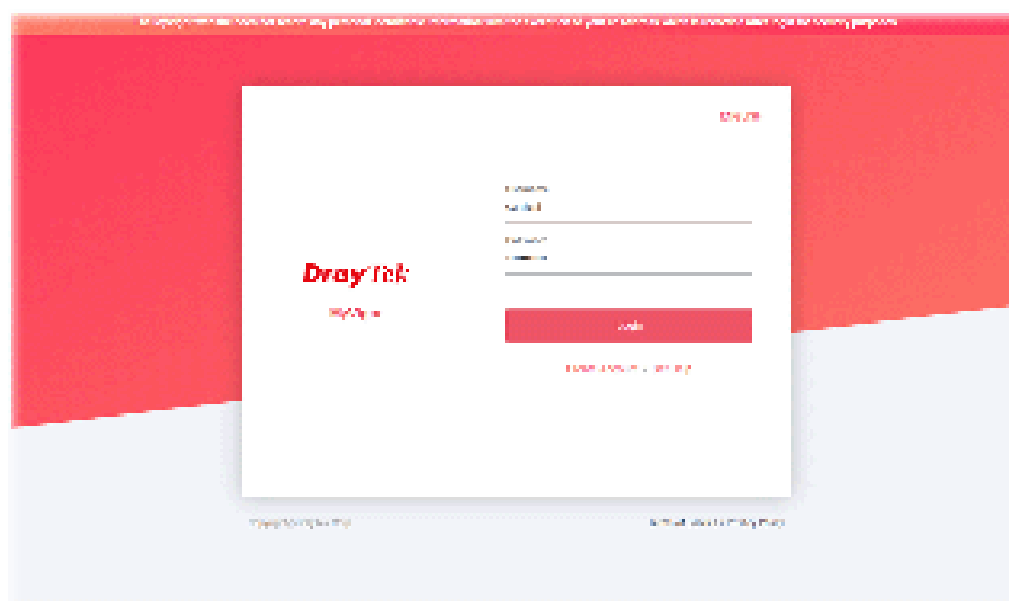
default-message-content-contentThe requested Web page does not exist. HTTP/1.0 404 Not Found. Content is not provided with HTML content type. Blocked by: DRAYTEK Web Content Filter. For more information, please contact your system administrator. For further information, please contact: myvigor@draytek.com

Legend

%SIP% - Source IP , %DIP% - Destination IP , %URL% - URL
%CI% - Category , %RNAME% - Router Name

OK

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



3. Click the link of **Create Account**.
4. The system will ask if you are 16 years old or over.
 - If yes, click **I am 16 or over**.

Terms of Service / Privacy Policy

Agreement

DrayTek provides MyVigor (myvigor.draytek.com) service according in this agreement. When you use MyVigor service, it means that you have read, understood and agreed to accept the terms listed in this agreement. DrayTek reserves the right to update the Terms of Use at any time without notice you. 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, understood and agreed to accept the modifications and changes. If you do not agree the contents of this agreement, please stop using MyVigor service.

Registration

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

About Us

DrayTek Corporation
Address: No. 26, Foshing Rd., Hsiao, Hsinchu Industrial Park, Hsinchu, 303, Taiwan
Tel: +886 3 5973327
Fax: +886 3 5973121
Personal Data Related Issue: privacy@draytek.com
Data Protection Officer: dpo@draytek.com

DrayTek Corp.
Version: V3.5
Date: 21 May 2019

I am under 16 years old
I am 16 or over

- If not, click **I am under 16 years old** to get the following page. Then, click **I and my legal guardian agree**.



GrayTek Corp.
Version: V3.3
Date: 21 May, 2018

[I and my legal guardian agree](#) [Disagree](#)

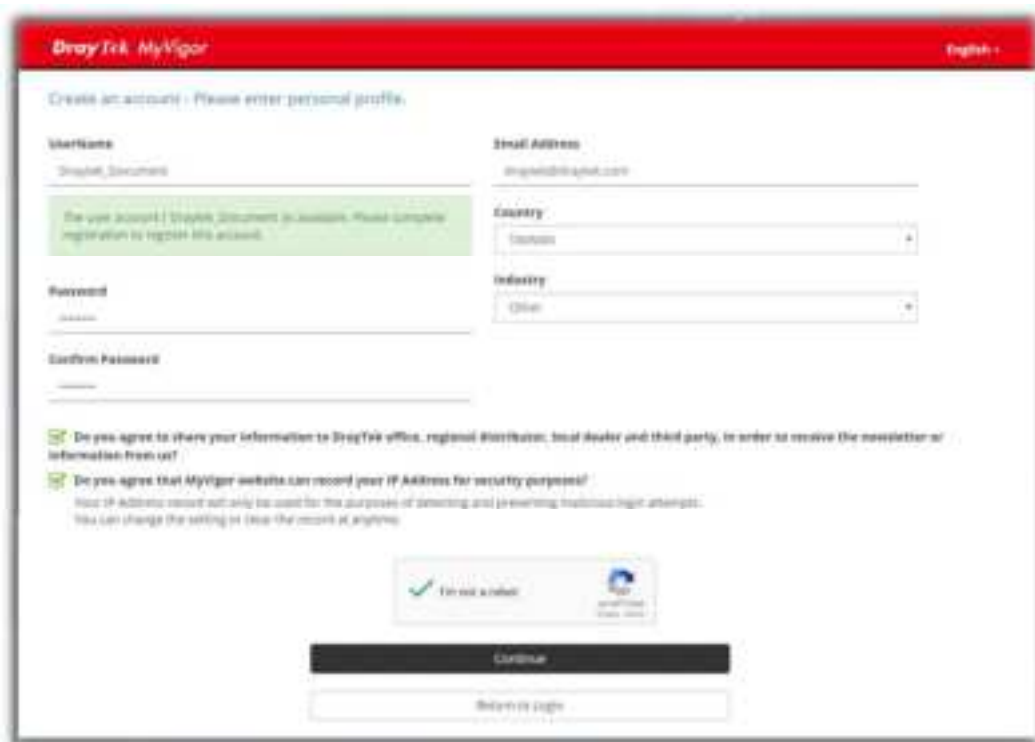
5. After reading the terms of service/privacy policy, click **Agree**.



GrayTek Corp.
Version: V3.3
Date: 21 May, 2018

[Agree](#) [Disagree](#)

6. In the following page, enter your personal information in this page and then click **Continue**.



GrayTek MyVigor English

Create an account - Please enter personal profile.

UserName: Graytek, Document

Email Address: graytek@graytek.com

Country: Taiwan

Industry: Other

Password:

Confirm Password:

The user account (Graytek, Document) is available. Please complete registration to register this account.

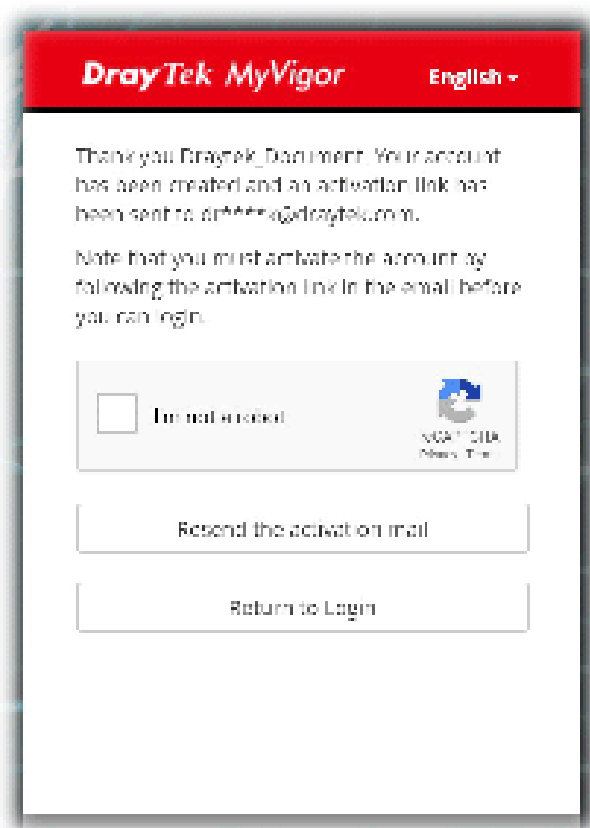
Do you agree to share your information to GrayTek office, regional distributor, local dealer and third party, in order to receive the newsletter or information from us?

Do you agree that MyVigor website can record your IP Address for security purposes?

Return to login

Continue

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



8. Now you have created an account successfully. Click **START**.
9. Check to see the confirmation **email** with the title of **New Account Confirmation Letter from myvigor.draytek.com**.

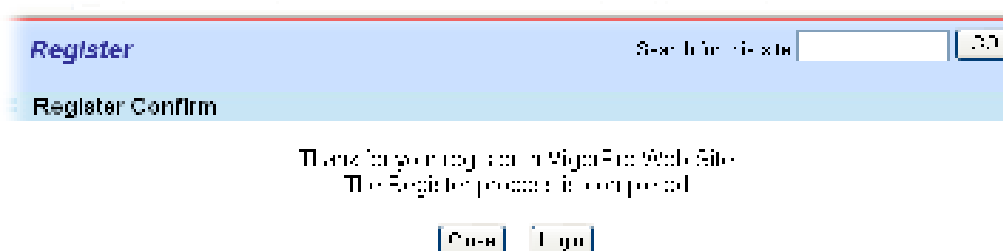
***** This is an automated message from myvigor.draytek.com. *****

Thank you (**Mary**) for creating an account.

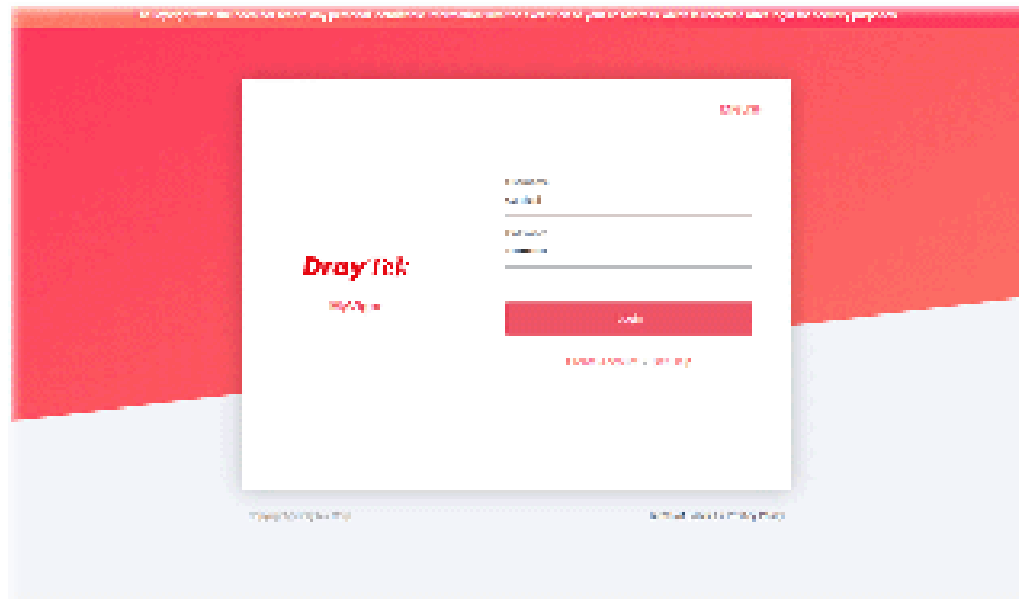
Please click on the activation link below to activate your account

Link : [Activate my Account](#)

10. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.



11. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**.



12. Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

A-2 How to Block Facebook Service Accessed by the Users via Web Content Filter / URL Content Filter

There are two ways to block the facebook service, Web Content Filter and URL Content Filter.

Web Content Filter,

Benefits: Easily and quickly implement the category/website that you want to block.

Note: License is required.

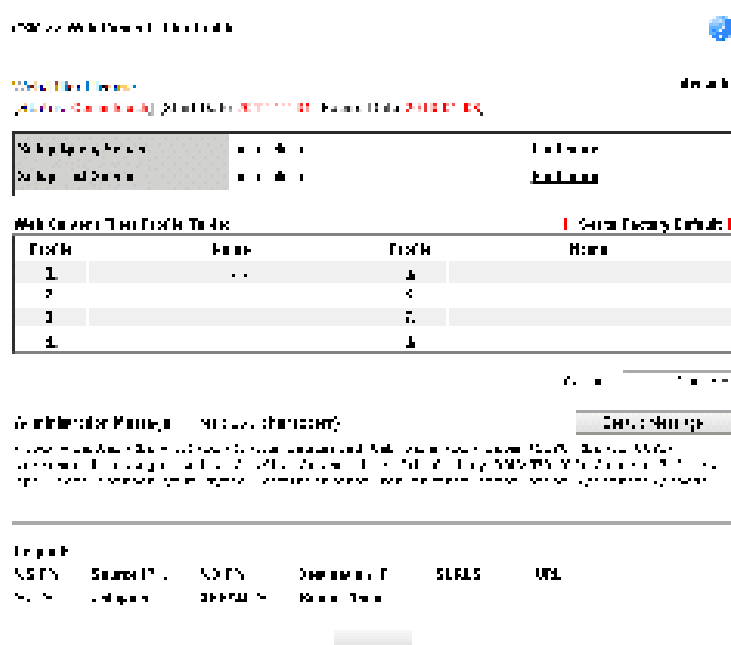
URL Content Filter,

Benefits: Free, flexible for customize webpage.

Note: Manual setting (e.g., one keyword for one website.)

I. Via Web Content Filter

1. Make sure the Web Content Filter (powered by Commtouch) license is valid.

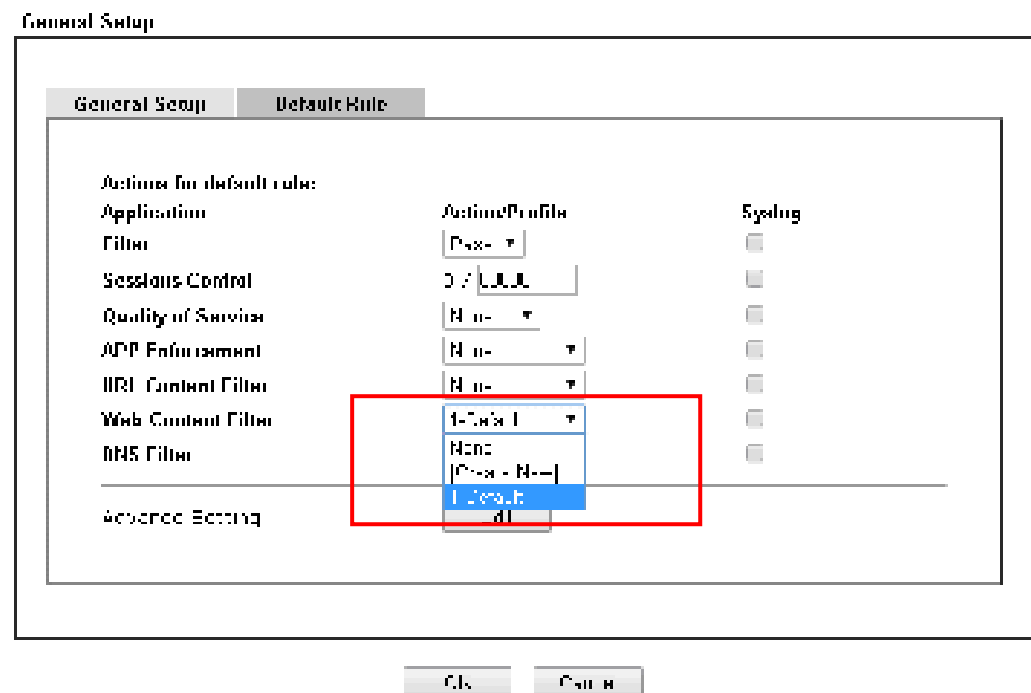


- Open **CSM >> Web Content Filter Profile** to create a WCF profile. Check **Social Networking** with Action, **Block**.



- Enable this profile in **Firewall>>General Setup>>Default Rule**.

Firewall >> General Setup



- 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.

Object Setting >> Keyword Object Setup

Profile Index : 1

Name	Facebook
Contents	facebook

Limit of Contents: Max 3 Words and 60 Characters.
Each word should be separated by a single space.

You can replace a character with %HEX.
Example:
Contents: backdoor%73 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: L1: URL Access Control List Log: Block

URL Access Control

☒ Enable URL Access Control ☐ Prevent web access from IP address

Actions: Block Facebook Edit

☐ Exception List Edit

Web Feature

☐ Enable Web Feature Restriction

Actions: Pass File Extension Profile: None Cookie Proxy Upload

OK Clear Cancel

5. When you finished the above steps, click **OK**. Then, open **Firewall>>General Setup**.

- Click the **Default Rule** tab. Choose the profile just configured from the drop down list in the field of **URL Content Filter**. Now, users cannot open any web page with the word “facebook” inside.

Firewall >> General Setup

General Setup

General Setup Default Rule

Actions for default rule:

Application	Action/Profile	Syslog
Filter	[Pass ▼]	☐
Sessions Control	0 / 00000	☐
Quality of Service	[None ▼]	☐
User Management	[None ▼]	☐
URL Enforcement	[None ▼]	☐
URL Content Filter	[1-Facebook ▼]	☐
Web Content Filter	[None ▼]	☐
DNS Filter	[None ▼]	☐

Advanced 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 null ().

Examples:
Contents: facebook 20 mins keepout

Result:
1. facebook
2. 20 mins
3. keep out

[OK] [Clear] [Cancel]

- Open **CSM>>URL Content Filter Profile**. Click an index number to open the setting page.
- Configure the settings as the following figure.

CSM >> URL Content Filter Profile

Profile Index: 2

Profile Name: face apps

Priority: Filter: URL Access Control First Log: Block

URL Access Control

☒ Enable URL Access Control ☐ Prevent web access from IP address

Action: Pass Group/Object Selections: faceapps Edit

Exception List Edit

Web Feature

☐ Enable Web Feature Restriction

Action: Block File Extension Profiles: None Cookie Proxy Upload

OK Clear Cancel

- When you finished the above steps, please open **Firewall>>General Setup**.
- Click the **Default Rule** tab. Choose the profile just configured from the drop down list in the field of URL Content Filter. Now, users cannot open any web page with the word “facebook” inside.

Firewall >> General Setup

General Setup

General Setup **Default Rule**

Actions for default rule:

Application	Action/Profile	Syslog
Filter	<u>Pass</u>	☐
Sessions Control	<u>0 / 90000</u>	☐
Quality of Service	<u>None</u>	☐
User Management	<u>None</u>	☐
URL Enforcement	<u>None</u>	☐
URL Content Filter	<u>face apps</u>	☐
Web Content Filter	<u>None</u>	☐
DNS Filter	<u>None</u>	☐

Advanced Setting Edit

This page is left blank.

Part VII Management



System
Maintenance

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.



Bandwidth
Management

It is used to control the bandwidth of data transmission through configuration of Sessions Limit, Bandwidth Limit, and Quality of Service (QoS).



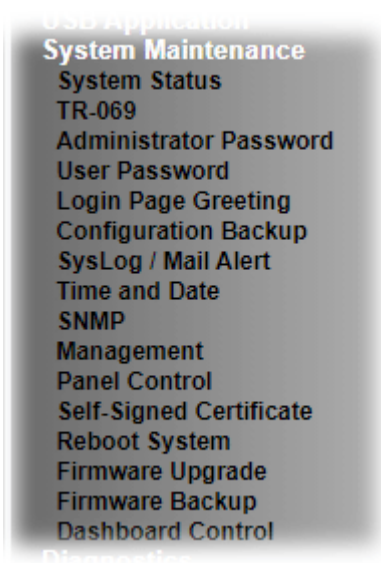
User
Management

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.

VII-1 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: System Status, TR-069, Administrator Password, User Password, Login Page Greeting, Configuration Backup, Syslog /Mail Alert, Time and Date, SNMP, Management, Panel Control, Self-Signed Certificate, Reboot System, Firmware Upgrade, Firmware Backup and Dashboard Control.

Below shows the menu items for System Maintenance.



Web User Interface

VII-1-1 System Status

The **System Status** displays basic network information of Vigor router including LAN and WAN interface status. Also available is the current firmware version and firmware related information.

System Status

Model Name : Vigor2765Max
Firmware Version : 4.0.1 STD
Build Date/Time : Apr 26 2021 10:19:42

LAN					
	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-1D-AA-15-B0-C8	192.168.1.1	255.255.255.0	ON	8.8.8.8
LAN2	00-1D-AA-15-B0-C9	192.168.2.1	255.255.255.0	ON	0.0.0.0
LAN3	00-1D-AA-15-B0-C8	192.168.3.1	255.255.255.0	ON	8.8.8.8
LAN4	00-1D-AA-15-B0-C9	192.168.4.1	255.255.255.0	ON	0.0.0.0
IP Routed Subnet	00-1D-AA-15-B0-C8	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-15-B0-C8	Europe	5.0.4.0	DrayTek

Wireless LAN(5GHz)			
MAC Address	Frequency Domain	Firmware Version	SSID
00-1D-AA-15-B0-C8	Europe	5.0.4.0	DrayTek_5G

WAN					
	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Disconnected	00-1D-AA-15-B0-C9	PPPoE	---	---
WAN2	Disconnected	00-1D-AA-15-B0-CA	---	---	---
WAN3	Disconnected	00-1D-AA-15-B0-CB	---	---	---

IPv6			
	Address	Scope	Internet Access Mode
LAN	FE80::21D:A4FF:FE15:B0C8C9	Link	---

VoIP			
Port	Profile	Reg. No.	In/Out
Phone1		No	On
Phone2		No	On

User Mode is **Off** now.

Available settings are explained as follows:

Item	Description
Model Name	Displays the model name of the router.
Firmware Version	Displays the firmware version of the router.
Build Date/Time	Displays the date and time of the current firmware build.
LAN	MAC Address - Displays the MAC address of the LAN Interface. IP Address - Displays the IP address of the LAN interface. Subnet Mask - Displays the subnet mask address of the LAN interface. DHCP Server

	- Displays the current status of DHCP server of the LAN interface. DNS - Displays the assigned IP address of the primary DNS.
WAN	Link Status - Displays current connection status of the WAN interface. MAC Address - Displays the MAC address of the WAN Interface. Connection - Displays the connection type of the WAN interface.. IP Address - Displays the IP address of the WAN interface. Default Gateway - Displays the assigned IP address of the default gateway.
IPv6	Address - Displays the IPv6 address for LAN. Scope - Displays the scope of IPv6 address. For example, IPv6 Link Local is non-routable and can only be used for local connections. Internet Access Mode – Displays the connection mode of the WAN interface.

VII-1-2 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through an Auto Configuration Server, e.g., VigorACS.

System Maintenance >> TR-069 Setting



ACS and CPE Settings
Reporting Configuration
Export Parameters

TR-069
☒ Enable
☐ Disable

ACS Server On

☒ Enable TR069 Server on System Maintenance >> Management >> Internet Access Control

ACS Server

URI

☐ Acquire URI from DHCP option 43

Username

Password

Event Code

Last Inform Response Time: (N/A)

CPL Client

Protocol
☒ HTTP
☐ HTTPS

URL

Port

Username

Password

Periodic Inform Settings

☐ Enable
☒ Disable

Time Interval

STUN Settings

☐ Enable
☒ Disable

Server Address

Server STUN Port

Minimum Keep Alive Period

Maximum Keep Alive Period

Apply Settings to APN(Switches)

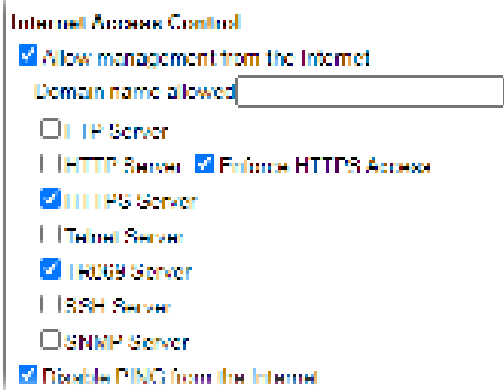
☐ Enable
☒ Disable

APN(Switches) Password

☐ APN(Switches) Password

Available settings are explained as follows:

Item	Description
TR-069	Enables or disables TR-069 functionality.
ACS Server On	Choose the interface for connecting the router to the Auto Configuration Server. Enable TR069 Server on System Maintenance>>Management>>Internet Access Control - If enabled, a user will be allowed to access into TR-069 from WAN.

	
ACS Server	This section specifies the settings of the ACS Server. URL – Enter the URL for connecting to the ACS. Please refer to the Auto Configuration Server user’s manual for detailed information. ● Wizard - Click it to enter the IP address of VigorACS server, port number and the handler. ● Acquire URL form DHCP option 43 - Select to acquire the ACS URL from DHCP option 43. Username/Password – Enter the credentials required to connect to the ACS server. ● Test With Inform - Click to send an inform message using the selected Event Code to test if the CPE is able to communicate with the VigorACS server. ● Event Code - Select an event for the inform test. Last Inform Response Time - Displays the time of the most recent Inform Response message received from the VigorACS.
CPE Client	This section specifies the settings of the CPE Client. Protocol - Select Https if the connection is encrypted; otherwise select Http. Port - In the event of port conflicts, change the port number of the CPE. Username and Password - Enter the username and password that the VigorACS will use to connect to the CPE.
Periodic Inform Settings	Enable - The default setting is Enable, which means the CPE Client will periodically connect to the ACS Server to update its connection parameters at intervals specified in the Interval Time field. ● Time Interval - Set interval time or schedule time for the router to send notification to CPE. Disable - Select Disable to turn off periodic notifications.
STUN Settings	STUN allows the ACS Server to connect to the CPE Client even when the client is behind a network address translator (NAT). Disable - The default setting is Disable. Enable - Please Enter the relational settings listed below: ● Server Address – Enter the IP address of the STUN server. ● Server Port – Enter the port number of the STUN server.

	● Minimum Keep Alive Period – If STUN is enabled, the CPE must periodically transmit binding requests to the server for the purpose of maintaining the binding with the Gateway. Enter the minimum interval between keep-alive messages that the CPE client sends to the ACS server. The default setting is 60 seconds. ● Maximum Keep Alive Period – If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding with the Gateway. Enter the maximum interval between keep-alive messages that the CPE client sends to the ACS server. A value of -1 indicates that no maximum period is specified.
Apply Settings to APs	This feature is able to apply TR-069 settings (including STUN and ACS server settings) to all of APs managed by Vigor2765 at the same time. Disable - TR-069 and Related settings will not be applied to VigorAPs. Enable - TR-069 settings will be applied to VigorAPs after clicking OK. The VigorAP password must be specified. ● AP Password - Enter the password of the VigorAP that you want to apply Vigor2765's TR-069 settings. Specify STUN Settings for APs - After clicking the Enable radio button for Apply Settings to APs, if you want to apply specific STUN settings (i.e., different from the Vigor2765 STUN settings) to VigorAPs to meet specific requirements, check this box and enter the server IP address, server port, and minimum and maximum keep alive periods respectively.

Select **OK** to save changes on the page, or **Clear** to reset all settings to factory defaults.

VII-1-2-2 Reporting Configuration

Information related to the router's health are divided into several categories and listed in this field. After checking the item(s), Vigor router will arrange and send corresponding data to VigorACS as a reference for the system administrator.

System Maintenance => TR-069 Setting

The screenshot shows a web interface for 'System Maintenance => TR-069 Setting'. There are three tabs: 'ACS and CPE Settings', 'Reporting Configuration' (which is selected), and 'Export Parameters'. Under the 'Reporting Configuration' tab, there is a section titled 'CPE Notification Settings'. It contains four checkboxes: 'Enable' (which is checked), 'Web Login', 'Web Changed', and 'Bandwidth Utilization'. At the bottom right of the window is an 'OK' button.

Available settings are explained as follows:

Item	Description
CPE Notification Settings	Enable - Check the box to select the notification item(s). Vigor router will send the utilization status to VigorACS.

Click **OK** to save changes on the page.

VII-1-2-3 Export Parameters

Click **Export** to save the TR-069 parameter settings as an ".xml".

System Maintenance >> TR-069 Setting

ACS and CPE Settings	Reporting Configuration	Export Parameters
Export Export TR-069 parameters by xml Export		

VII-1-3 Administrator Password

This page allows you to set or change the administrator password.

System Maintenance >> Administrator Password Setup

Administrator Password

Old Password	
New Password	
Confirm Password	

Advanced Settings

☐ Enable Advanced Authentication (Advanced Authentication is not supported by some routers.)
☐ Enable Advanced Authentication (Advanced Authentication is not supported by some routers.)
☐ Enable Advanced Authentication (Advanced Authentication is not supported by some routers.)
☐ Enable Advanced Authentication (Advanced Authentication is not supported by some routers.)

Old Password: New Password:

☐ Enable Advanced Authentication

Advanced Authentication

☐ Local Profile	1234567890	Advanced Authentication	1234567890
☐ Remote Profile	1234567890	Advanced Authentication	1234567890

Note:
Parameters can be modified only in Advanced Authentication Setup.

Advanced Authentication

☐ Enable Local User

Advanced Authentication

Old Password	
New Password	
Confirm Password	

☐ Enable Advanced Authentication (Advanced Authentication is not supported by some routers.)
☐ Enable Advanced Authentication (Advanced Authentication is not supported by some routers.)
☐ Enable Advanced Authentication (Advanced Authentication is not supported by some routers.)
☐ Enable Advanced Authentication (Advanced Authentication is not supported by some routers.)

Old Password: New Password:

☐ Enable Advanced Authentication

Advanced Authentication

☐ Local Profile	1234567890	Advanced Authentication	1234567890
☐ Remote Profile	1234567890	Advanced Authentication	1234567890

Local User List

Username	Advanced Authentication	Advanced Authentication
admin	Advanced Authentication	Advanced Authentication

Available settings are explained as follows:

Item	Description
Administrator Password	The administrator can login web user interface of Vigor router to modify all of the settings to fit the requirements. Old Password - Enter the current password. The factory default is “admin”. New Password - Enter the new password. The maximum length of the password is 23 characters. Confirm Password - Enter the new password again for confirmation. Password Strength - Shows the security strength of the password specified above. Enable ‘admin’ account login to Web UI from the Internet - Select to allow the administrator to log in from the Internet. This option is enabled when Administrator Local User is enabled (see below). Enable Advanced Authentication method when login from “WAN” - Advanced authentication method can offer a more secure network connection. Select to require mOTP or TOTP or 2-step authentication when logging in from the WAN. Time-based One-time Password (TOTP) - Please make sure the time zone of your router is correct. Then, install Google Authenticator APP on your cell phone. Open the APP to scan the QR code on this page. A one-time password will be shown on your phone.  In the field of Validation Code, enter the one-time password and click Verify.  Now, the configuration is finished. You will be asked to enter the 2FA code on the after passing the username and password authentication.  Mobile one-Time Password (mOTP) - Select to allow the use of mOTP passwords. Enter the PIN Code and Secret settings for getting one-time passwords.

	● 2-Step Auth code via SMS Profile and/or Mail Profile – Select the SMS and/or Mail profiles and the destination SMS number and/or email address for transmitting the password.
Administrator Local User	Usually, the system administrator has the highest privilege to modify the settings on the web user interface of the Vigor router. However, in some cases, it might be necessary to have other users in LAN to access into the web user interface of Vigor router. This feature allows you to add more administrators who can then log in to the web interface, with the same privileges as the administrator. Enable Local User - Check the box to allow other users to administer the router. Specific User – Create the new user account as the local user. Then specify the authentication method (dividing into Basic and Advanced) for the user account. ● User Name - Enter a user name. ● Password - Enter the password for the local user. ● Confirm Password - Enter the new password again for confirmation. Enable Advanced Authentication method when login from “WAN” - Advanced authentication method can offer a more secure network connection. Select to require mOTP or TOTP or 2-step authentication when logging in from the WAN. ● Time-based One-time Password (TOTP) - Please make sure the time zone of your router is correct. Then, install Google Authenticator APP on your cell phone. Open the APP to scan the QR code on this page. A one-time password will be shown on your phone.  In the field of Validation Code, enter the one-time password and click Verify.  Now, the configuration is finished. You will be asked to enter the 2FA code on the after passing the username and password authentication.



- **Mobile one-Time Password (mOTP)** - Select to allow the use of mOTP passwords. Enter the mOTP PIN Code and Secret that will be used to generate the one-time passwords.
- **2-Step Authentication via SMS Profile and/or Mail Profile** –Select the SMS and/or Mail profiles and the destination SMS number and/or email address for transmitting the password.
- **Add** - After entering the user name and password above, click this button to create a new local user. The new user will be shown on the Local User List immediately.
- **Edit** - If you wish to change a user in the Local User List, select it, perform the necessary modifications, and click this button to update the user.
- **Delete** - If you wish to delete a user in the Local User List, select it and click this button to remove it.

Local User List - Shows all the users that are set up to administer the router.

Click **OK** to save changes on the page, and you will be directed to the login screen. Please log in with the new password.

VII-1-4 User Password

This page allows you to set new password for user operation.

System Maintenance >> User Password

☐ **Enable User Mode for simple web configuration**
User Password

[Set to Factory Default](#)

Password	Max: 31 characters
Confirm Password	Max: 31 characters
Password Strength:	Weak Medium Strong
Strong password requirements: 1. Have at least one upper case letter and one lower case letter. 2. Including non-alphanumeric characters like plus.	

Note:

1. Password can contain a-z A-Z 0-9 , _ " ! @ # \$ % ^ & * ()
2. Password can't be all asterisks(*). For example, "*" or "" is illegal, but "123*" or "*45" is OK.

OK

Available settings are explained as follows:

Item	Description
Enable User Mode for simple web configuration	Check this box to enable User Mode for web user interface with the password typed here for simple web configuration. The simple web user interface settings differ from those on the full web user interface seen when logged in using the administrator password.
Password	Enter the password. The maximum length of the password is 31 characters.
Confirm Password	Enter the password again for verification.
Password Strength	Shows the security strength of the password specified above.
Set to Factory Default	Click to return to the factory default setting.

Click **OK** to save changes on the page, and you will be directed to the login screen. Please window will appear. Please log in with the new password.

Here are the steps involved in setting up the router for User Mode Access:

1. Navigate to **System Maintenance>>User Password** in the web user interface.
2. Check the box of **Enable User Mode for simple web configuration** to enable user mode operation. Enter a new password in the Password field and click **OK**.

System Maintenance » User Password

☒ Enable User Mode for simple web configuration

User Password [Set to Factory Default](#)

Password	*****
Confirm Password	*****
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 character 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**.

DrayTek **Vigor2765 Series**

Login

Username:	admin
Password:	*****
Language:	English

Login

Security Warning: You are logging in without encryption which is not recommended. To login securely [click here](#).

Copyright© 2000-2021 DrayTek Corp. All Rights Reserved.

6. The main screen with User Mode will be shown as follows.



Only basic settings are available in User Mode. These are a subset of the Admin Mode settings.



Info

Setting in User Mode can be configured as same as in Admin Mode.

Below shows an example of a customized login page with the values entered in the **Login Page Title** and **Welcome Message and Bulletin** fields.



DrayTek **Vigor2765 Series**

Login

Router Login

Username

Password

Language ▼

Login

Security Warning: You are logging in without encryption which is not recommended. To login securely [click here](#).

Copyright© 2000-2021 DrayTek Corp. All Rights Reserved.

Welcome Message

This welcome message is displayed in the Login page of the router. Replace this text with your own message:

1. This welcome message can be written in HTML, so links such as this one can be created.
2. Other markup tags such as p, font or img can be used.

VII-1-6 Configuration Backup

Such function can be used to apply the router settings configured by Vigor2760 to Vigor2765. This function allows the backup and restoration of router settings.

Backing up the Configuration

Follow the steps below to backup your configuration.

1. Go to **System Maintenance >> Configuration Backup**. The following page will be shown.

System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restore
Restore settings from a configuration file

☒ [選擇檔案](#) [本地儲存位點](#)

☐ USB Storage 

☐ Restore configuration except the login password.

Note:
This will work only if the selected configuration file was created from this device.

[Restore](#)

Backup
Backup the current settings into a configuration file.

☐ Protect with password

[Backup](#)

Note:
The router's certificates are not part of the configuration file. Please use [Certificate Management >> Certificate Backup](#) for backup.

Auto Backup to USB storage

☐ Enable

Backup folder 

☒ Periodic backup

Cycle duration days and hours

☐ Backup after changed configuration

[OK](#)

Note:

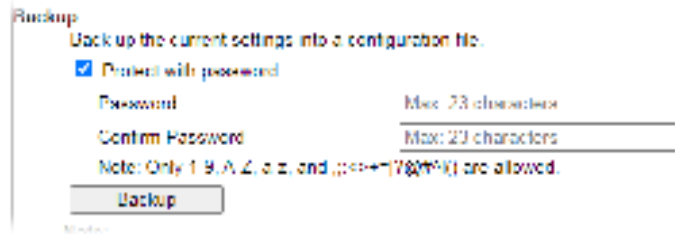
1. When loading a configuration file from a model in the Supported Model List please note that features and functionality may vary between models so please manually verify the settings after the restoration.
2. Auto backup to USB: if settings do not change, configuration doesn't backup.
3. Auto backup to USB: if configuration backup multiple times in one hour, the old file will be overwritten with the same filename.

Supported Model List

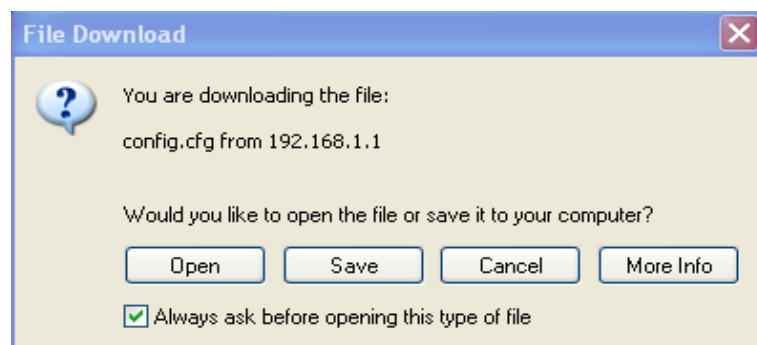
Model	Firmware Version
Vigor2760	3.0.9.4
Vigor2762	3.0.2 or later

Available settings are explained as follows:

Item	Description
Restore	Restore settings from a configuration file - Click the Select File button to specify a file to be restored or click USB Storage (if a USB storage disk connected) to choose the configuration file.
	Restore configuration except the login password - Select to exclude the password from getting restored from the backup.

	Restore - Click to initiate restoration of configuration. If the backup file is encrypted, you will be asked to enter the password.
Backup	Click it to perform the configuration backup of this router. Protect with password- Select to encrypt the backup with a password. You will be prompted to enter the password as shown below:  ● Password - Enter a new password for encrypting the configuration file. ● Confirm Password - Enter the new password again for confirmation. Backup - Click to initiate the backup process.
Auto Backup to USB storage	The configuration can be stored to a USB connecting to Vigor router as a backup. Enable - Check the box to enable the function. Backup folder - Set the path for downloading. Periodic backup - Set the circle duration for backup. Backup after change configuration - Backup will be executed whenever the configuration is changed.

- Click the **Backup** button, and the File Download dialog will be shown. Depending on your browser, you may be prompted to select a location to save the file, or the file may be saved in the default download location of your browser.



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

Configuration Backup does not include certificates stored on the router. Please back up certificates separately by going to Certificate Management >> Certificate Backup.

Restoring Configuration

1. Go to **System Maintenance >> Configuration Backup**. The following windows will be popped-up as shown below.

System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restore

Restore settings from a configuration file

☒ **選擇檔案** 本機儲存位點檔案

☐ USB Storage

☐ Restore configuration except the login password.

Note:
This will work only if the selected configuration file was created from this device.

Backup

Backup the current settings into a configuration file.

☐ Protect with password

Note:
The router's certificates are not part of the configuration file. Please use [Certificate Management](#) or [Certificate Backup](#) for backup.

Auto Backup to USB storage

☐ Enable

Backup folder

☒ Periodic backup

Cycle duration days and hours

☐ Backup after change configuration

Note:

1. When loading a configuration file from a model in the Supported Model List please note that features and functionality can vary between models so please manually verify the settings after the restoration.
2. Auto backup to USB: if settings do not change, configuration doesn't backup.
3. Auto backup to USB: if configuration backup multiple times in one hour, the old file will be overwritten with the same filename.

Supported Model List

Model	Firmware Version
Vigor2760	3.0.9.4
Vigor2762	3.0.2 or later

2. Click the **Choose File** button under **Backup** to bring up the open file dialog box to select the configuration file to be uploaded and restored.
3. Click the **Restore** button and wait for few seconds.

VII-1-7 SysLog/Mail Alert

SysLog function is provided for users to monitor router.

System Maintenance >> SysLog / Mail Alert Setup

SysLog / Mail Alert Setup

SysLog Access Setup ☒ Enable Syslog Save to ☒ Syslog Server ☐ USB Disk Maximum Syslog folder space: 1 GB When Syslog folder is full: Overwrite oldest logs Router Name : DanyTel Server IP/hostname : Destination Port : 514 Mail Syslog : ☐ Enable Enable syslog messages: ☒ Firewall Log ☒ VPN Log ☒ User Access Log ☒ Call Log ☒ WAN Log ☒ Router/DSL Information ☒ WLAN Log	Mail Alert Setup ☐ Enable Send test email Interface : Any SMTP Server : SMTP Port : 25 Mail to : Sender Address : ☐ Use SSL ☐ Authentication Username : Password : Enable E-Mail Alert ☒ DoS Attack ☒ ARP ☒ VPN LOG ☐ ARP Signature ☐ Debug Log

Note:
1. USB Syslog space is available from 256-1024 MB or 1-16 GB.
2. Mail Syslog cannot be activated unless USB Disk is ticked for "Syslog Save to".
3. Mail Syslog feature will send the Syslog when it is full.
4. We only support secured SMTP connection on port 465.

Available settings are explained as follows:

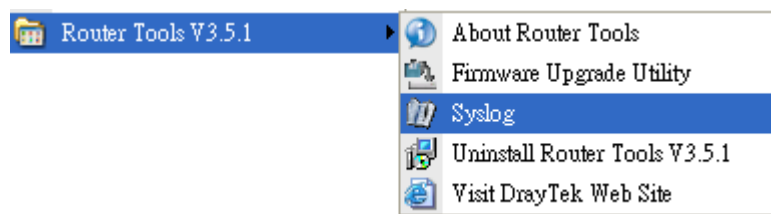
Item	Description
SysLog Access Setup	Enable - Select to enable the Syslog function. Syslog Save to - Check Syslog Server and / or USB Disk. ● Syslog Server - Events will be sent to a Syslog server. ● USB Disk - Events will be saved to a USB storage device connected to the router. ● Maximum Syslog folder space - Set a space (unit GB/MB) to store event logs. ● When Syslog folder is full - Specify the action (overwrite the oldest logs or stop logging) to be executed.
Router Name	Shows the name of the router set in System Maintenance >> Management . This name will be used to identify the router in the Syslog entries. To set or modify the router name, click the hyperlink and you will be taken to System Maintenance >> Management where you can enter the value. Server IP Address/Hostname - Enter the IP address / hostname of the Syslog server.

	Destination Port - Enter the port for the Syslog server. Mail Syslog – Select to enable sending Syslog messages by email. Enable syslog message - Select the events to be recorded by syslog.
Mail Alert Setup	Enable - Select to enable the Mail Alert. Send a test e-mail - Click to send a test email message using the settings below. Interface - Specify the WAN interface for a mail passing through. SMTP Server - Enter the address of the SMTP server used to send email. SMTP Port - Enter the port of the SMTP server. Default setting is 25. Mail To - Enter the email address of the recipient. Sender Address - Enter the return path of the email messages. Email messages that cannot be delivered will be returned to this address. Use SSL - Check this box to use port 465 for SMTP server for some e-mail server uses https as the transmission method. Authentication - Select this checkbox and enter the username and password if the SMTP server requires authentication. ● User Name - Enter the user name for authentication. ● Password - Enter the password for authentication. Enable E-mail Alert - Select the event types that will trigger email alerts.

Select **OK** to save changes on the page, or **Clear** to reset all settings to factory defaults.

To view the Syslog message, please follow the steps below:

1. On the **Syslog / Mail Alert Setup** screen, enter the monitor PC's IP address in the **Server IP Address** field.
2. Install the Router Tools from DrayTek web site. After installation, start Syslog by clicking on **Router Tools>>Syslog** in the Windows Start Menu.



-
- The screenshot displays the DrayTek Syslog Utility v3.3.3 interface. The main window features a toolbar with icons for file operations and a menu bar. The 'Syslog' tab is active, showing a list of log entries. A 'Filter' dialog box is open, allowing users to filter log entries based on various criteria. The dialog has tabs for 'Filter', 'Log', 'Syslog', 'Network', and 'Syslog'. The 'Filter' tab is selected, showing a list of log entries with columns for IP Address, Port, and Host. The 'Filter' dialog has a 'Filter' button and a 'Cancel' button.

VII-1-8 Time and Date

This section allows you to configure settings related to the system date and time.

System Maintenance >> Time and Date

Time Information

Current System Time	2000 Jan 6 Thu 23:33:2	Inquire Time

Time Setup

☐ Use Browser Time	
☒ Use Internet Time	
Time Server	pool.ntp.org
Priority	Auto
Time Zone	(GMT) Greenwich Mean Time (Dubai)
Enable Daylight Saving	☐ Advanced
Automatically Update Interval	30 mins
Send NTP Request Through	Auto

Available settings are explained as follows:

Item	Description
Current System Time	Click Inquire Time to retrieve the current time from the time server.
Use Browser Time	Select this option to let the router set its system time using the time reported by the web browser.
Use Internet Time	Select this option to let the browser set its system time by retrieving time information from the specified network time server using the Network Time Protocol (NTP).
Time Server	Enter the address of the time server.
Priority	Select 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 to enter a custom schedule to enable DST. Daylight Saving Advanced ☒ Default Start: Last Sunday in March End: Last Sunday in October ☐ Customized: By Date Start: Month Day 00:00 End: Month Day 00:00 ☐ Customized: By Weekday Start: January 1st Sunday 00:00 End: January 1st Sunday 00:00 OK Close Use the default time setting or set user defined time for your requirement.

	Default - Uses the default DST schedule for the time zone. By Date - Select this option if DST starts and ends on fixed dates. By Weekday - Select this option if DST starts and ends on certain days of the week.
Automatically Update Interval	Select the time interval at which the router updates the system time.
Send NTP Request Through	Specify a WAN interface to send NTP request for time synchronization.

Select **OK** to save changes on the page, or **Cancel** to discard changes without saving.

VII-1-9 SNMP

This section allows you to configure settings for SNMP and SNMPv3 services.

The SNMPv3 is more secure than SNMP through the use of encryption (supports AES and DES) and authentication (supports MD5 and SHA) for the management needs.

System Maintenance => SNMP

SNMP Setup

☐ Enable SNMP Agent

☒ Enable SNMPv1 Agent
 ☒ Enable SNMPv2c Agent

Get Community: public

 Set Community: private

Index	IP	Subnet Mask
1		
2		
3		

Index	IPv6 Address	Prefix Length
1		/0
2		/0
3		/0

Trap Community: public

Index	IP
1	
2	

Index	IPv6 Address
1	
2	

Trap Timeout: 10

☐ Enable SNMPv3 Agent

 USM User:

 Auth Algorithm: No Auth

 Auth Password:

 Privacy Algorithm: No Priv

 Privacy Password:

Note:

SNMP service also shall be enabled for Internet access in [System Maintenance => Management](#)

OK Cancel

Available settings are explained as follows:

Item	Description
Enable SNMP Agent	Check to enable SNMP function. Then, enable SNMPV1 agent/SNMPV2C agent.
Get Community	Enter the Get Community string. The default setting is public . Devices that send requests to retrieve information using get commands must pass the correct Get Community string. The maximum allowed length is 23 characters.
Set Community	Enter the Set Community string. The default setting is private . Devices that send requests to change settings using set commands must pass the correct Set Community string. The maximum length of the text is 23 characters.
Manager Host IP (IPv4)	Enter the IPv4 address of hosts that are allowed to issue SNMP commands. If this field is left blank, any IPv4 LAN host is allowed to issue SNMP commands.
Manager Host IP (IPv6)	Enter the IPv6 address of hosts that are allowed to issue SNMP commands. If this field is left blank, any IPv6 LAN host is allowed to issue SNMP commands.
Trap Community	Enter the Trap Community string. The default setting is public. Devices that send unsolicited messages to the SNMP console must pass the correct Trap Community string. The maximum length of the text is 23 characters.
Notification Host IP (IPv4)	Enter the IPv4 address of hosts that are allowed to be sent SNMP traps.
Notification Host IP (IPv6)	Enter the IPv6 address of hosts that are allowed to be sent SNMP traps.
Trap Timeout	The default setting is 10 seconds.
Enable SNMPV3 Agent	Check to enable SNMPV3 function.
USM User	USM means user-based security mode. Enter the username to be used for authentication. The maximum allowed length is 23 characters.
Auth Algorithm	Choose one of the hashing methods to be used with the authentication algorithm.
Auth Password	Enter a password for authentication. The maximum allowed length is 23 characters.
Privacy Algorithm	Choose an encryption method as the privacy algorithm.
Privacy Password	Enter a password for privacy. The maximum allowed length is 23 characters.

Select **OK** to save changes on the page, or **Cancel** to discard changes without saving.

VII-1-10 Management

This page allows you to manage the settings for Internet/LAN Access Control, Access List from Internet, Management Port Setup, Brute Force Protection, TLS/SSL Encryption Setup, AP Management and Device Management.

The management pages for IPv4 and IPv6 protocols are different.

VII-1-10-1 IPv4 Management Setup

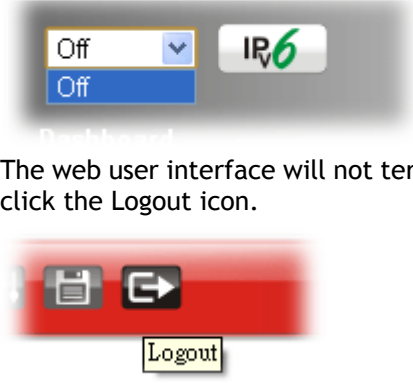
System Maintenance » Management ?

IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup																																	
Router Name Draytek																																			
☐ Default/Disable Auto-Logout ☐ Enable Validation Code in Internet/LAN Access Note: ILU and below version does NOT support DrayOS CAPTCHA with code																																			
Internet Access Control ☐ Allow management from the Internet Domain name allowed:																																			
☐ FTP Server ☐ HTTP Server ☒ Enforce HTTP Access ☒ HTTPS Server ☐ Telnet Server ☐ TR069 Server ☐ SSH Server ☐ SNMP Server ☒ Disable PING from the Internet																																			
Access List from the Internet ☐ Apply Access List to PING																																			
<table border="1"> <thead> <tr> <th>List Type</th> <th>Index</th> <th>Description</th> </tr> </thead> <tbody> <tr><td>1</td><td>IP Object</td><td>None</td></tr> <tr><td>2</td><td>IP Object</td><td>None</td></tr> <tr><td>3</td><td>IP Object</td><td>None</td></tr> <tr><td>4</td><td>IP Object</td><td>None</td></tr> <tr><td>5</td><td>IP Object</td><td>None</td></tr> <tr><td>6</td><td>IP Object</td><td>None</td></tr> <tr><td>7</td><td>IP Object</td><td>None</td></tr> <tr><td>8</td><td>IP Object</td><td>None</td></tr> <tr><td>9</td><td>IP Object</td><td>None</td></tr> <tr><td>10</td><td>IP Object</td><td>None</td></tr> </tbody> </table>			List Type	Index	Description	1	IP Object	None	2	IP Object	None	3	IP Object	None	4	IP Object	None	5	IP Object	None	6	IP Object	None	7	IP Object	None	8	IP Object	None	9	IP Object	None	10	IP Object	None
List Type	Index	Description																																	
1	IP Object	None																																	
2	IP Object	None																																	
3	IP Object	None																																	
4	IP Object	None																																	
5	IP Object	None																																	
6	IP Object	None																																	
7	IP Object	None																																	
8	IP Object	None																																	
9	IP Object	None																																	
10	IP Object	None																																	
Note: Access list type: Hostname, single IP address supported for corresponding domain name																																			
Management Port Setup ☒ Use Define Ports ☐ Default Ports																																			
<table border="1"> <tr><td>Telnet Port</td><td>23</td><td>(Default: 23)</td></tr> <tr><td>HTTP Port</td><td>80</td><td>(Default: 80)</td></tr> <tr><td>HTTPS Port</td><td>443</td><td>(Default: 443)</td></tr> <tr><td>FTP Port</td><td>21</td><td>(Default: 21)</td></tr> <tr><td>TR069 Port</td><td>8069</td><td>(Default: 8069)</td></tr> <tr><td>SSH Port</td><td>22</td><td>(Default: 22)</td></tr> </table>			Telnet Port	23	(Default: 23)	HTTP Port	80	(Default: 80)	HTTPS Port	443	(Default: 443)	FTP Port	21	(Default: 21)	TR069 Port	8069	(Default: 8069)	SSH Port	22	(Default: 22)															
Telnet Port	23	(Default: 23)																																	
HTTP Port	80	(Default: 80)																																	
HTTPS Port	443	(Default: 443)																																	
FTP Port	21	(Default: 21)																																	
TR069 Port	8069	(Default: 8069)																																	
SSH Port	22	(Default: 22)																																	
Note: Ports 8001 and 8043 are used for Hotspot Web Portal																																			
Brute Force Protection ☐ Enable brute force login protection																																			
☐ HTTP Server ☐ HTTPS Server ☐ Telnet Server ☐ TR069 Server ☐ SSH Server ☐ VPN Server																																			
Maximum login failures: 0 times Penalty period: 0 seconds																																			
Blocked IP List																																			
TLS/SSL Encryption Setup ☒ Enable TLS 1.3 ☒ Enable TLS 1.2 ☒ Enable TLS 1.1 ☒ Enable TLS 1.0 ☐ Enable SSL 3.0																																			
AP Management ☒ Enable AP Management																																			
☒ Device Management ☐ Respond to network device																																			

OK

Available settings are explained as follows:

Item	Description
Router Name	Enter the router name as provided by ISP.
Default: Disable Auto-Logout	If enabled, the auto-logout function for web user interface will be disabled.

	 The web user interface will not terminate until you manually click the Logout icon.
Enable Validation Code in Internet/LAN Access	If enabled, Vigor router will require users to enter a validation code as shown in an image when they log in.
Internet Access Control	Allow management from the Internet - Enable the checkbox to allow system administrators to login from the Internet, and then select the specific services that are allowed to be remotely administered. Domain name allowed - This setting is only available if DNS filtering is enabled, applying DNS filter profile in firewall rules, or enabling DNS Filter Local Setting. The router will only allow connections to the WebUI using domain addresses configured in either DDNS profiles or this section. If DNS filtering is disabled, this setting will be disabled, and any domain address that resolves to the router's WAN IP address can be used to connect to the WebUI. Disable PING from the Internet - Select to reject all PING packets from the Internet. For increased security, this setting is enabled by default.
Access List from the Internet	The ability of system administrators to log into the router can be restricted to up to 10 specific hosts or networks. Apply Access List to PING - When this option is checked and Disable PING from the Internet is unchecked, pings originating from the Internet will be accepted only if they are from one of the IP addresses and/or subnet masks specified below. This option has no effect if Disable PING from the Internet is checked, which blocks all pings from the Internet. Type - Select IP Object or Hostname. Index - Select the index number of a configured IP object, keyword object or IP group object. Description - Shows a brief comment for the selected IP object (with subnet mask).
Management Port Setup	User Define Ports - Check to specify user-defined port numbers for the Telnet, HTTP, HTTPS, FTP, TR-069 and SSH servers. Default Ports - Check to use standard port numbers for the Telnet and HTTP servers.
Brute Force Protection	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.

	Enable brute force login protection –Select to enable detection of brute force login attempts. Maximum login failures –Specify the maximum number of failed login attempts before further login is blocked. Penalty period –Set the lockout time after maximum number of login attempts has been exceeded. The user will be unable to attempt to log in until the specified time has passed. Blocked IP List –Display, in a new browser window, IP addresses that are currently blocked from logging into the router.
TLS/SSL Encryption Setup	Enable SSL 3.0/1.0/1.1/1.2/1.3 –Check the box to enable SSL 3.0/1.0/1.1/1.2/1.3 encryption protocols. For improved security, the HTTPS and SSL VPN servers that are built into the router have been upgraded to TLS 1.x protocol. If you are using an old web browser (eg. IE 6.0) or an old version of the SmartVPN Client, you may need to enable SSL 3.0 to connect to the router. However, it is recommended that you instead upgrade your web browser or SmartVPN client to a version that supports TLS protocols that are far more secure than SSL.
AP Management	Enable AP Management –Check to enable the access point management function. If not, menu items related to Central Management>>AP will be hidden.
Device Management	Check to enable the device management function. Respond to external device –If selected, Vigor2765 will function as a slave device. When an external device (master device) sends packets to the Vigor2765 to attempt to manage it, the Vigor2765 will respond to the request coming from the external device which is able to manage Vigor2765.

Select **OK** to save changes on the page.

VII-1-10-2 IPv6 Management Setup

System Maintenance >> Management



IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup	
Management Access Control ☐ Allow management from the Internet ☐ Telnet Server (Port: 23) ☐ HTTP Server (Port: 80) ☐ Enable HTTP Access ☐ HTTPS Server (Port: 443) ☐ SSH Server (Port: 22) ☐ SNMP Server (Port: 161) ☒ Disable PING from the Internet IPv6 Address Security Option ☒ Enable Random Interface Identifiers (IIDs) instead of LUI 64 IIDs			
Access List from the Internet ☐ Apply Access List to PING			
List	Type	Index Description	
1	IP Object	None	
2	IP Object	None	
3	IP Object	None	
4	IP Object	None	
5	IP Object	None	
6	IP Object	None	
7	IP Object	None	
8	IP Object	None	
9	IP Object	None	
10	IP Object	None	
Note: 1 Telnet/HTTP server port is the same as IPv4. 2 Access list type: Hostname, single IP address supported for corresponding domain name.			
OK			

Available settings are explained as follows:

Item	Description
Management Access Control	Allow management from the Internet - Check to enable the function. Select the servers that system administrators are allowed to manage from the Internet. Disable PING from the Internet - Check to reject all PING packets from the Internet. For increased security, this setting is enabled by default.
IPv6 Address Security Option	Enable Random Interface Identifiers (IIDs)... - The IPv6 address will be generated randomly but not using LAN/WAN MAC to prevent the attack from the hacker.
Access List from the Internet	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed. Apply Access List to PING - When this option is checked and Disable PING from the Internet is unchecked, pings originating from the Internet will be accepted only if they are from one of the IP addresses and/or subnet masks specified below. This option has no effect if Disable PING from the Internet is checked, which blocks all pings from the Internet. Type - Select IP Object or Hostname.

	Index - Select the index number of a configured IPv6 object.

Select **OK** to save changes on the page.

VII-1-10-3 LAN Access Control

System Maintenance >> Management



IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup
☒ Allow management from LAN		
☒ HTTP Server ☐ Enable HTTP Access		
☒ HTTPS Server		
☒ Telnet Server		
☒ SSH Server		
☒ SSH Server		
Apply to Subnet	Index in IP Object	
☒ LAN1	..	..
☒ LAN2	..	..
☒ LAN3	..	..
☒ LAN4	..	..
☒ IP Routed Subnet	..	..

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 - Enter the index number of the IP object profile. Related IP address will appear automatically.

Select **OK** to save changes on the page.

VII-1-11 Panel Control

You may customize the behavior of the LEDs, buttons, WLAN, USB and LAN ports on the front panel.

For LED

By default, LEDs on the front panel illuminate or blink during operation to show the status of the various functions on the router. However, you may configure them to remain off at all times, or remain off until a button is pressed to wake them up.

System Maintenance >> Panel Control

LED	Button	USB	LAN Port	Refresh								
☒ Enable LED ☐ Enable Sleep Mode Turn off LED after 1 minutes (Default: 1 minute)												
Note: Enabling the Sleep Mode will make the functions of "Wireless Button" and "Factory Reset Button" on the front panel as below: <table border="1"><thead><tr><th>LED Status</th><th>LED On</th><th>LED Off</th></tr></thead><tbody><tr><td>Wireless Button</td><td>Wireless On/Off/WPS</td><td rowspan="2">Turn LED On*</td></tr><tr><td>Factory Reset Button</td><td>Press 1 second: Turn LED off immediately! Press till the AG1 light flashing: Reset router</td></tr></tbody></table> *Still functional even the buttons are disabled					LED Status	LED On	LED Off	Wireless Button	Wireless On/Off/WPS	Turn LED On*	Factory Reset Button	Press 1 second: Turn LED off immediately! Press till the AG1 light flashing: Reset router
LED Status	LED On	LED Off										
Wireless Button	Wireless On/Off/WPS	Turn LED On*										
Factory Reset Button	Press 1 second: Turn LED off immediately! Press till the AG1 light flashing: Reset router											
OK												

Available settings are explained as follows:

Item	Description
Refresh	Click to refresh the page to display the latest information.
Enable LED	Select to enable the LEDs to function according to the configured settings. Deselect to disable LEDs entirely.
Enable Sleep Mode	Select to let the system turn off the LEDs after the specified number of minutes has elapsed. When Sleep Mode is enabled, the LEDs can be woken up by pressing one of the following buttons: ● Wireless LAN ON/OFF/WPS on the front panel ● Factory Reset on the front panel ● Wake up LED on this configuration page

	
Status	Shows the status of the LEDs. When the following is shown, the LEDs are in sleep mode. Status : Sleep Wake up LED To wake them up, do one of the following actions: ● press the Wake up LED button on this page ● press the Wireless On/Off/WPS button on the front panel ● press the Factory Reset button on the front panel. When the following is shown, the LEDs are awake. Status : Awake, sleep after 1 minutes LED sleep immediately To put them to sleep immediately, perform one of the following actions: ● press the LED sleep immediately button on this page ● press the Factory Reset button on the front panel
Wake up LED	Click to resume operation of the LED after they have gone to sleep.

Select **OK** to save changes on the page.

For Button

The primary functions of the **Factory Reset** and **Wireless ON/OFF/WPS** front-panel buttons (reset to factory defaults and wireless control, respectively) are enabled by default, but they can be enabled or disabled as needed.

When the **Factory Reset** button is set to **Disabled**, the router cannot be reset during normal operation. Other functions of the reset button (such as starting up the TFTP server to upload firmware during power on, and controlling the illumination of the front panel LEDs when LED sleep mode is enabled) can still be used.

When the **Wireless ON/OFF/WPS** button is set to **Disabled**, the button cannot be used to turn on or off the wireless network, nor can it be used to start the WPS pairing process. However, the front panel LEDs can be woken up when LED sleep mode is enabled.

Click the **Button** tab to get the following page.

LED	Button	USB	LAN Port	Refresh
Enable Button ☒ Wireless ☒ Factory Reset				

Note:

Enabling the Sleep Mode will make the functions of "Wireless Button" and "Factory Reset Button" on the front panel as below:

LED Status	LED On	LED Off
Wireless Button	Wireless On/Off/WPS	Turn LED On*
Factory Reset Button	Press 1 second, Turn LED off immediately* Press till the WUI light flashing, Reset router	

*Still functional even the buttons are disabled

OK

Available settings are explained as follows:

Item	Description
Refresh	Click to refresh the page to display the latest information.
Enable Wireless Button	The default value is Enabled. Deselect to disable the ability of the Wireless button to control WLAN and WPS functions. Disabling the wireless button only prevents it from being used to control WLAN functions. It can still be used to wake up the LEDs when LED sleep mode is enabled.
Enable Factory Reset Button	The default value is Enabled. Deselect to disable the reset function of the factory reset button. Disabling the Factory Reset button only prevents it from being used to reboot Vigor router with default settings. It can still be used to wake up the LEDs when LED sleep mode is enabled.

Select **OK** to save changes on the page.

For USB

The USB ports can be individually enabled or disabled. When a USB port is disabled, attached devices will not be recognized by the router.

LED	Button	USB	LAN Port	Refresh									
<table border="1"> <thead> <tr> <th>Port</th> <th>Enable</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>☒</td> <td>No Device</td> </tr> <tr> <td>2</td> <td>☒</td> <td>No Device</td> </tr> </tbody> </table>					Port	Enable	Status	1	☒	No Device	2	☒	No Device
Port	Enable	Status											
1	☒	No Device											
2	☒	No Device											

OK

Available settings are explained as follows:

Item	Description
Refresh	Click to refresh the page to display the latest information.
Port	The number corresponds to the USB port number shown on the front panel.
Enable	Deselect to disable the USB port. The default value is enabled.
Status	Shows the status of the USB port. No device - no USB device is connected to the port. Connected - a USB device is connected to the port. --- - the USB port is disabled.

Select **OK** to save changes on the page.

For LAN Port

The 4 LAN ports can be individually enabled or disabled. When a LAN port is disabled, attached devices will not be recognized by the router.

System Maintenance >> Panel Control

LED	Button	USB	LAN Port	Refresh

Port	Enable	Status	Speed
1	☒	Link Up	1000Mbps
2	☒	Link Down	
3	☒	Link Down	---
4	☒	Link Down	

OK

Available settings are explained as follows:

Item	Description
Refresh	Click to refresh the page to display the latest information.
Port	The number corresponds to the LAN port number shown on the front panel.
Enable	Deselect to disable the LAN port. The default value is enabled.
Status	Shows the status of the USB port. Link Up - An active Ethernet device is connected to the port. Link Down - No active Ethernet device is detected. --- - The LAN port is disabled.
Speed	Shows the negotiated speed of the LAN port. 1000Mbps - Negotiated speed of the LAN port is 1000 Mbps. 100Mbps - Negotiated speed of the LAN port is 100 Mbps. 10Mbps - Negotiated speed of the LAN port is 10 Mbps. --- - The LAN port is disabled or there is no active device connected.

Select **OK** to save changes on the page.

Click **Regeneration** to open **Regenerate Self-Signed Certificate** window.

System Maintenance >> Regenerate Self Signed Certificate

Regenerate Self Signed Certificate

Certificate Name	self-signed
Subject Alternative Name	
Type	IP Address ▾
IP	
Subject Name	
Country (C)	
State (ST)	
Location (L)	
Organization (O)	
Organization Unit (OU)	
Common Name (CN)	
Email (E)	
Key Type	RSA ▾
Key Size	2048 Bit ▾

Generate

Enter all requested information including certificate name (used to differentiate different certificates), subject alternative name type and relational settings for subject name. Then click **GENERATE**.

VII-1-13 Reboot System

The Web user interface may be used to restart your router. Click **Reboot System** from **System Maintenance** to bring up the following page.

System Maintenance > Reboot System

Reboot System

Do you want to reboot your router?

☒ Using current configuration

☐ Using factory default configuration

Reboot Now

Auto Reboot Time Schedule

Schedule Profile : | None | | None | | None | | None |

Note:
Action and Duration Time settings will be ignored.

OK Cancel

Available settings are explained as follows:

Item	Description
Reboot System	Select one of the following options, and press the Reboot Now button to reboot the router. Using current configuration - Select this option to reboot the router using the current configuration. Using factory default configuration - Select this option to reset the router's configuration to the factory defaults before rebooting.
Auto Reboot Time Schedule	Schedule Profile - Select up to 4 user-configured schedules to reboot the router on a scheduled basis.

Select **OK** to save changes on the page, or **Cancel** to discard changes without saving.

	
Info	When the system pops up Reboot System web page after you configure web settings, please click Reboot Now to reboot your router for ensuring normal operation and preventing unexpected errors of the router in the future.

VII-1-14 Firmware Upgrade

Click **System Maintenance>> Firmware Upgrade** to upgrade firmware upgrade.

System Maintenance >> Firmware Upgrade



Firmware Version Status

Current Firmware/Version: 4.3.1_STB	Download Directly Latest Firmware Detail
Latest Firmware/Version: 4.3.1	

Download Link: <https://www.edinortek.com/support/latest-firmware/>

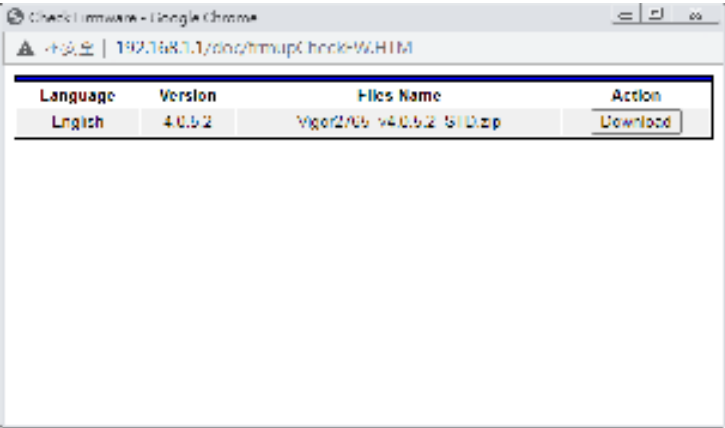
Web Firmware Upgrade

Select a firmware file:	
Browse... Select File	
Click Upgrade to upload the file	Upgrade Preview

Note:

Upgrade using the ALL file will retain existing router configuration, whereas using the RST file will reset the configuration to factory defaults.

Available settings are explained as follows:

Item	Description
Firmware Version Status	Check The Latest Firmware - Click to check for updated firmware. Any available new firmware files will be displayed and you can download any one of them by clicking Download. After the file has been downloaded, click Select followed by Upgrade to perform the firmware upgrade. 
Web Firmware Upgrade	Click Browse... to select the firmware file, followed by Upgrade to start the upgrade process, or Preview to display detailed information about the selected firmware file:

VII-1-15 Firmware Backup

The firmware for Vigor router can be saved on the host as a backup firmware. After that, if the router crashes due to the firmware error, the backup firmware will be applied to make the router run normally.

System Maintenance >> Firmware Backup

Automatic Firmware Recovery

☐ Enable automatic firmware recovery
If the router unexpectedly reboots three times in a row then the backup firmware will be restored to the unit on the third reboot.

Backup Setting

☐ Backup after reboot

☒ Backup after system uptime of 1 day 0 hour (max 7 days)

☐ Backup manually

Backup Firmware: 4.7.1_RC5_BTD
Last backup: 2000/01/01 23:49:18

Available settings are explained as follows:

Item	Description
Automatic Firmware Recovery	Enable automatic firmware recovery - If this option is enabled, the router will restore the most recently backed-up firmware after the router reboots unexpectedly three times.
Backup Setting	This option controls the backup behavior of the router. ● Backup after reboot - The router makes a copy of the current firmware immediately after it reboots ● Backup after system uptime... - The router makes a copy of the current firmware after it has run for the specified length of time after boot-up. ● Backup manually - the router will not automatically create a backup copy of the firmware. Click this option and click OK, firmware backup will be performed immediately. Backup Firmware - Displays recent firmware backup version. Last backup - Displays the time of recent firmware backup.

Select **OK** to save changes on the page, or **Cancel** to discard changes without saving.

VII-1-16 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



The screenshot shows a dialog box titled "System Maintenance => Dashboard Control". Inside the dialog, there is a list of nine items, each with a checkbox. The first two items, "Front Panel" and "System Information", have unchecked checkboxes. The remaining seven items, "IPv4 LAN Information", "IPv4 Internet Access", "IPv6 Internet Access", "Interface", "Security", "System Resource", and "Quick Access", all have checked checkboxes. Below the list, there are two buttons: "OK" and "Cancel".

Item	Checked
Front Panel	☐
System Information	☐
IPv4 LAN Information	☒
IPv4 Internet Access	☒
IPv6 Internet Access	☒
Interface	☒
Security	☒
System Resource	☒
Quick Access	☒

OK Cancel

VII-2 Bandwidth Management

Sessions Limit

When LAN clients share a common public IP address by means of Network Address Translation (NAT), the router must track NAT sessions so that traffic to and from the WAN can reach the intended destinations. There is a finite number of sessions that can be tracked by the router, and by setting session limits will ensure that the router does not run out of resources. This is especially important when P2P applications are used. P2P applications, such as BitTorrent, that attempt to simultaneously establish connections to as many WAN hosts as possible.

Bandwidth Limit

Bandwidth Limit ensures LAN clients get their fair share of network bandwidth by placing restrictions on upstream and downstream network speeds.

Quality of Service (QoS)

QoS (Quality of Service) ensures that all LAN clients receive their fair share of bandwidth that is required for applications to function properly and efficiently.

Without QoS, it is possible that certain applications may consume excessive network resources that they degrade performance of more important applications, especially ones that are less tolerant of jitter (delay variation) or lost or delayed packets. Additionally, at times of network congestion, QoS is able to prioritize different types of traffic according to their predefined priority, thus ensuring traffic of higher importance gets processed first.

A typical QoS deployment consists of two components:

- **Classification:** Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.
- **Scheduling:** Prioritizing packets by assigning them to different queues and service types according to service levels.

APP QoS

APP QoS allows QoS to be applied to select protocols and applications.

Protocols and applications fall into two categories: Traceable and Untraceable. Traceable applications are those whose traffic can be 100% traced, and can be assigned a specific QoS class. Untraceable applications, on the other hand, are detected when they attempt to establish connections to remote hosts, and all traffic between the remote hosts and the local network will be placed under QoS, within the same QoS class.

Web User Interface

Bandwidth management ensures efficient allocation of network bandwidth for various applications.

To set up Bandwidth Management, from the Main Menu, select **Bandwidth Management**.



VII-2-1 Sessions Limit

To configure Sessions Limit, from the **Bandwidth Management** menu, select **Sessions Limit** to open the setup page.

Bandwidth Management >> Sessions Limit

IPv4

IPv6

☐ Enable ☒ Disable

Default Max Sessions:

5 entries per page

Limitation List (Max 10 entries)

Index	Start IP	End IP	Max Sessions

Specific Limitation

Start IP: End IP:

Maximum Sessions:

Administration Message (Max 255 characters)

Default Message

You have reached the maximum number of permitted internet sessions. If possible, please use up more applications to allow further Internet access. Contact your system administrator for further information.

Time Schedule

Schedule Profile: None

None

None

None

None

Note: Action and Idle Timeout settings will be ignored

To activate the function of limit session, simply click **Enable** and set the default session limit. Available settings are explained as follows:

Item	Description
Session Limit	Enable - Select to activate session limit function.
	Disable - Select to deactivate session limit function.
	Default Max Session - The default maximum number of sessions allowed per LAN client, unless overridden by

	specifying a different number in the Limitation List.
Limitation List	Displays specific limitation entries.
Specific Limitation	Start IP - The beginning IP address for this limit entry. End IP - The ending IP address for limit entry. Max Sessions - The maximum number of NAT sessions allowed per LAN client. If no value is entered, the Default Max Sessions value is used. Add - Creates a new limit entry using the above Specific Limitation values. Edit - To edit an existing entry, select the entry from the Limitation List, make the appropriate changes in Specific Limitation, then click Edit. Delete - To delete an entry, select it from the Limitation List, then click the Delete button.
Administration Message	Message to be displayed in a web browser on the LAN client when the maximum number of NAT sessions has been reached. Default Message - Click to reset the administration message to the factory default.
Time Schedule	Schedule Profile - Specify up to 4 time schedule entries to enable or disable the WAN.

To save changes on the page, click **OK**.

VII-2-2 Bandwidth Limit

To configure the Bandwidth Limit feature, from the **Bandwidth Management** menu, select **Bandwidth Limit** to bring up the configuration page.

Bandwidth Management >> Bandwidth Limit

IPv4

IPv6

☐ Enable
 ☒ Disable
 ☐ IP Routed Subnet

Default Limit (Per User)
 TX Limit 2000 Kbps
 RX Limit 8000 Kbps

5 entries per page

Limitation List (Max: 10 entries)

Index	Start IP/Group	End IP/Object	TX limit	RX limit	Shared
Add Entry By: ☒ IP Range ☐ IP Object Start IP End IP					
☐ Each ☐ Shared TX Limit Kbps RX Limit Kbps					
Add Edit Delete					

Auto-Adjustment
☐ Allow users to use more bandwidth than the assigned limit when there are no bandwidth available

Smart Bandwidth Limit
☐ Apply the below limit to users not in Limitation List and user more than sessions

TX Limit 200 Kbps
 RX Limit 800 Kbps

Time Schedule
 Schedule Profile:

Note:

1. Use "0" for TX/RX Limit for unlimited bandwidth.
2. The Action and Idle Timeout settings in the Schedule Profile will be ignored.

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

Available settings are explained as follows:

Item	Description
Enable / Disable	Disable - Select to deactivate bandwidth limit function. Enable - Select to activate bandwidth limit function. ● IP Routed Subnet - Check this box to apply the bandwidth limit to the traffic via IP routed subnet. Default Limit (Per User) ● TX Limit - Default upstream speed limit for each LAN client. Unit can be either Kbps or Mbps. Value must be between 0 (unlimited) and 30000. ● RX limit - Default downstream speed limit for each LAN client. Unit can be either Kbps or Mbps. Value must be between 0 (unlimited) and 30000.
Limitation List	Displays specific limitation entries.
Add Entry By	IP Range - All the IPs within the range defined will be restricted by bandwidth limit defined by TX Limit and RX

	Limit below. ● Start IP - The beginning IP address for this limit entry. ● End IP - The ending IP address for limit entry. IP Object - All the IPs specified by the selected IP object or IP group will be restricted by bandwidth limit defined by TX Limit and RX Limit below. ● IP Group - Specify an IP group by using the drop down list. ● IP Object - Specify an IP object by using the drop down list. Each - The specified bandwidth is the limit per LAN client. Shared - The specified bandwidth limits are the total allowed for all LAN clients within the range of IP addresses. ● TX limit - The upstream limit. Unit can be either Kbps or Mbps. Value must be between 0 (unlimited) and 30000. ● RX limit - The downstream limit. Unit can be either Kbps or Mbps. Value must be between 0 (unlimited) and 30000. Add - Creates a new limit entry using the above Specific Limitation values. Edit - To edit an existing entry, select the entry from the Limitation List, make the appropriate changes in Specific Limitation, then click Edit. Delete - To delete an entry, select it from the Limitation List, then click the Delete button.
Auto-Adjustment	Allow user to use more bandwidth --- - Select to let the router automatically adjust the upstream and downstream limits based on available bandwidth.
Smart Bandwidth Limit	This option restricts the bandwidth of LAN clients that are not in the limitation list when the network sessions exceed a predefined threshold. Apply the below limit to ... - The number of sessions a LAN client is allowed to have before Smart Bandwidth Limit activates. ● TX limit - Upstream speed limit for each LAN client. Unit can be either Kbps or Mbps. Value must be between 0 (unlimited) and 30000. ● RX limit - Downstream speed limit for each LAN client. Unit can be either Kbps or Mbps. Value must be between 0 (unlimited) and 30000.
Time Schedule	Schedule Profile - Specify up to 4 time schedule entries to enable or disable the WAN.

VII-2-3 Quality of Service

To configure **Quality of Service**, from the main menu, select **Bandwidth Management** menu, then click **Quality of Service** to bring up the configuration page.

Bandwidth Management >> Quality of Service

General Setup

Index

Enable

Direction

Inbound/Outbound Bandwidth

Class 1

Class 2

Class 3

Others

Status

WAN1	☐	BOTH	100 Mbps / 100 Mbps	25 %	25 %	25 %	25 %	Status
WAN2	☐	BOTH	100 Mbps / 100 Mbps	25 %	25 %	25 %	25 %	Status
WAN3	☐	BOTH	100 Mbps / 100 Mbps	25 %	25 %	25 %	25 %	Status

Note:

QoS may not work properly if the bandwidth entered is not correct. Before enable QoS, you may run speed test (from e.g., <http://speedtest.net>) or consult your ISP for the accurate bandwidth.

Class Rule

Index	Enable	Qos Class	Local Address	Remote Address	DSCP	Service Type
Add						

Note:

- The packets that don't match any class rules above will be classified into 'Others'.
- Go to [User Defined Service Type](#) to edit/delete user defined service type profiles.
- Hardware Acceleration will not work on wired WAN interfaces with QoS enabled.

Voice Prioritization

☒ Enable the First Priority for VoIP SIP/RTP:

SIP DSCP Port

5060 (Default: 5060)

Tag Outbound Traffic

Class 1	☐ Add DSCP or Precedence Value	Default
Class 2	☐ Add DSCP or Precedence Value	Default
Class 3	☐ Add DSCP or Precedence Value	Default

OK

Cancel

Available settings are explained as follows:

Item	Description
General Setup	Index - Link of WAN interface. Enable - Check the box to enable the QoS function for WAN interface. If it is enabled, you can configure general QoS setting for each WAN interface. Direction - Direction of traffic to which QoS is to be applied (Inbound, Outbound, or Both). IN - Apply QoS to incoming traffic only. OUT - Apply QoS to outgoing traffic only. BOTH - Apply to both incoming and outgoing traffic. Inbound/Outbound Bandwidth - The inbound / outbound bandwidth of the WAN. This option is not available on ADSL/VDSL WAN1 interface. Class 1 ~ 3 / Others - Percentage of bandwidth reserved for each class. Status - Click to bring up the Online Statistics page that shows snapshots of statistics for the given WAN interface.
Class Rule	Define and list the Class rules. Index - Displays the class number that you can edit. Enable - Displays the status of this class rule.

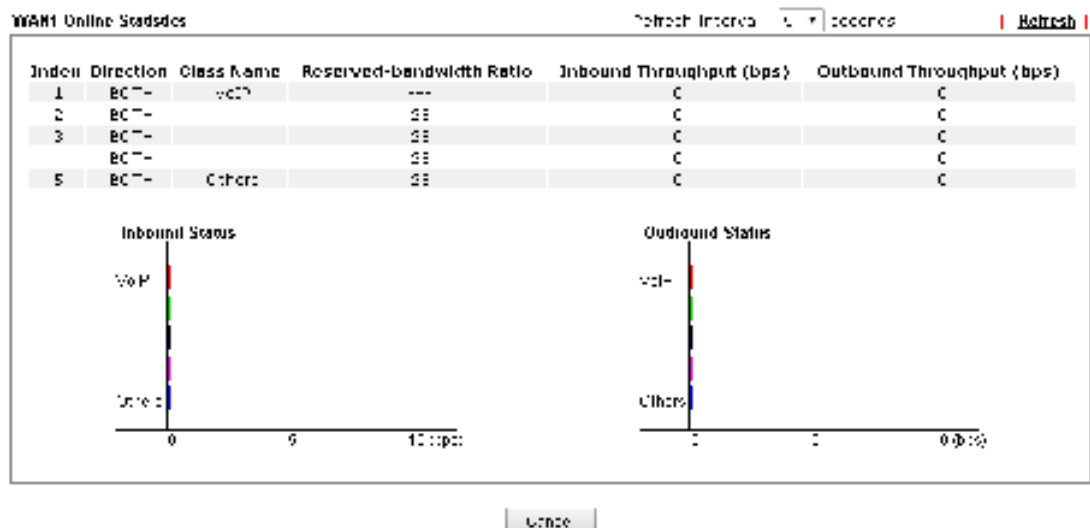
Item	Description
	QoS Class - Displays the QoS class level. Local Address - Displays the local IP address for the rule. Remote Address - Displays the remote IP address for the rule. DSCP - Displays the levels of the data for processing with QoS control. Service Type - Displays detailed settings for the service type. Add - Click it to create a class rule for QoS.
VoIP Prioritization	Enable the First Priority for VoIP SIP/RTP - Select to allow VoIP traffic to receive the highest priority. SIP UDP Port - Port number to be monitored for SIP traffic.  - Click this icon to display the VoIP QoS Status.
Tag Outbound Traffic	Tag the outgoing traffic with the DSCP or Precedence value. Add DSCP or Precedence Value for Class 1 to Class 3 - Check to apply the DSCP or precedence value for each class.

To save changes, click **OK**; to discard changes, click **Cancel**.

Online Statistics

Click the Status link in the General Setup section to show real-time online statistics of the WAN interface.

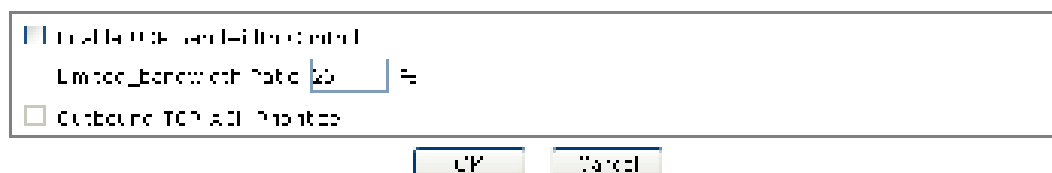
Bandwidth Management >> Quality of Service



General Setup for WAN Interface

Click WAN interface number link to configure the limited bandwidth ratio for QoS of the WAN interface.

Bandwidth Management >> Quality of Service >> WAN1



Available settings are explained as follows:

Item	Description
Enable UDP Bandwidth Control	Select to restrict the bandwidth available to UDP traffic. The Limited_bandwidth Ratio value is the maximum percentage of bandwidth that can be used by UDP traffic. ● Limited_bandwidth Ratio - Enter a percentage value.
Outbound TCP ACK Prioritize	Select to give outbound ACK packets priority over other packets to ensure traffic is not slowed down because the remote host is waiting for ACK packets before further traffic will be sent.



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.

Add / edit a Class Rule for QoS

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.

1. To add a rule, click **Add** to bring up the configuration page. To edit an existing rule, select the rule by clicking the radio button in front of the rule, and then click **Edit** to bring up the configuration page.

General Setup | Set to Factory Default

Index	Enable	Direction	Inbound/Outbound Bandwidth			Class 1	Class 2	Class 3	Others	Status	
WAN1	☐	Both	100	Mbps	100	Mbps	25 %	25 %	25 %	25 %	Status
WAN2	☐	Both	100	Mbps	100	Mbps	25 %	25 %	25 %	25 %	Status
WAN3	☐	Both	100	Mbps	100	Mbps	25 %	25 %	25 %	25 %	Status

Note:
QoS may not work properly if the bandwidth entered is not correct. Before enable QoS, you may run speed test (from e.g., <http://speedtest.net>) to confirm your ISP for the accurate bandwidth.

Class Rule

Index	Enable	QoS Class	Local Address	Remote Address	DSCP	Service Type
Add						

Note:
1. The packets that don't match any class rule above will be classified into 'Others'.
2. Go to [User Defined Service Type](#) to edit/delete user defined service type profiles.
3. Hardware Acceleration will not work on wired WAN interfaces with QoS enabled.

VoIP Prioritization

☒ Enable the First Priority for VoIP SIP/RTP:

SIP UDP Port: 5060 (Default: 5060)

Tag Outbound Traffic:

Class 1	☐ Add DSCP or Precedence Value	Default
Class 2	☐ Add DSCP or Precedence Value	Default
Class 3	☐ Add DSCP or Precedence Value	Default

OK Cancel

- For adding a new rule, click **Add** to open the following page.

Bandwidth Management >> Quality of Service

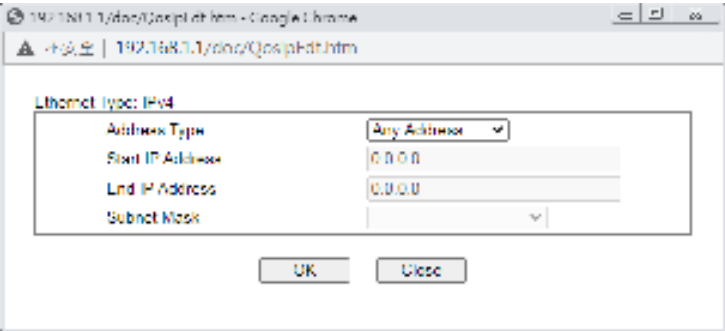
Rule 1

☒ Enable	
IP Version	Both IPv4 IPv6
Local IP Address	Any
	Edit
Remote IP Address	Any
	Edit
Diffserv CodePoint	ANY
Service Type	None (TOP/UDP 53)
QoS Class	Class 1

OK Delete Cancel

Available settings are explained as follows:

Item	Description
Enable	Select to enable this rule.
IP Version	Protocol (IPv4 or IPv6) to which this rule applies.
Local IP Address	Click the Edit button to set the local (LAN) IP address or address range for the rule.

Remote Address	Click the Edit button to set the remote (WAN) IP address or address range for the rule.  Address Type - Type of address: Any Address, Single Address, Range Address, Subnet Address. ● Single Address - Specify IP address. ● Range Address - Specify Start IP Address and End IP Address. ● Subnet Address - Specify Start IP Address and Subnet Mask.
DiffServ CodePoint	DSCP or ToS precedence of packets to which this rule applies.
Service Type	Service Type to which this rule applies. Service is a predefined or user-defined type of traffic that uses certain protocols or ports. To set up a custom service, select User Defined to set the service name, the protocol, and port number.
QoS Class	Specify the QoS class (1, 2 or 3) for this rule.

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

Bandwidth Management >> Quality of Service

General Setup Set to Factory Default

Index	Enable	Direction	Inbound Bandwidth	Outbound Bandwidth	Class 1	Class 2	Class 3	Others	Status
WAN1	☐	ROTH	100 Mbps	100 Mbps	75%	75%	75%	75%	Status
WAN2	☐	ROTH	100 Mbps	100 Mbps	75%	75%	75%	75%	Status
WAN3	☐	ROTH	100 Mbps	100 Mbps	75%	75%	75%	75%	Status

Note:
QoS may not work properly if the bandwidth set here is not correct. Before enable QoS, you may run speed test (from e.g. <http://speedtest.net>) or contact your ISP for the accurate bandwidth.

Class Rule

Index	Enable	QoS Class	Local Address	Remote Address	DSCP	Service Type
1	☒	Class 1	Any	Any	ANY	UNB (100UDP/52)

Note:
1. The packets that don't match any class rule above will be classified into 'Others'.
2. Go to [User Defined Service Type](#) to configure user defined service type profiles.
3. Hardware Acceleration will not work on wired WAN interfaces with QoS enabled.

VoIP Prioritization

☒ Enable the First Priority for VoIP SIP/RTP:
SIP UDP Port: 5060 (Default 5060)

Top Outbound Traffic:

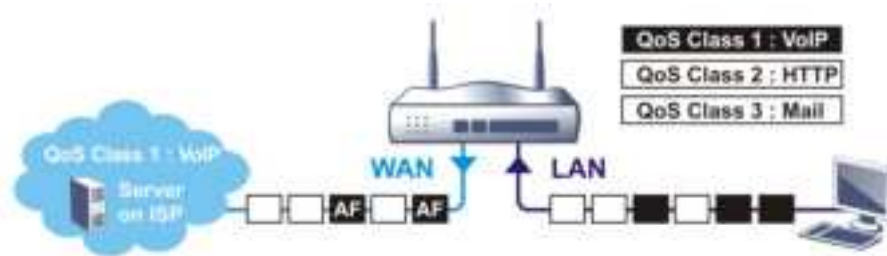
Class	Add DSCP or Precedence Value	Default
Class 1	☐	Default
Class 2	☐	Default
Class 3	☐	Default

OK Cancel

Retag the Packets for Identification

Packets originating from the LAN that are destined for the WAN can have the DS flag changed to a different value by enabling Tag Packet and specifying the DSCP or IP Precedence value.

In the following illustration, outbound VoIP packets from the LAN arrive at the Vigor router with the QoS value unset. The router sets the DSCP value to AF before forwarding them to the ISP server via the WAN interface.



QoS Class 1 : VoIP			
QoS Class 1 : VoIP	QoS Class 1 : VoIP	QoS Class 1 : VoIP	QoS Class 1 : VoIP
QoS Class 2 : HTTP	QoS Class 2 : HTTP	QoS Class 2 : HTTP	QoS Class 2 : HTTP
QoS Class 3 : Mail	QoS Class 3 : Mail	QoS Class 3 : Mail	QoS Class 3 : Mail

VII-2-4 APP QoS

To configure APP QoS, from the main menu, select **Bandwidth Management** menu, then click **APP QoS** to bring up the configuration page.

Bandwidth Management >> APP QoS

APP QoS

Enable	Instant Message	Version	Action
☒	Facebook/Instagram		QoS Class 1 (High)
☒	LINE	5.20.0.2104	QoS Class 1 (High)
☒	LinkedIn		QoS Class 1 (High)
☒	Signal	1.26.2	QoS Class 1 (High)
☒	Slack	4.0.0	QoS Class 1 (High)
☒	Snapchat	10.95.0	QoS Class 1 (High)
☒	Telegram	1.7.10	QoS Class 1 (High)
☒	WhatsApp	0.0.2040	QoS Class 1 (High)

Enable	VoIP	Version	Action

Available settings are explained as follows:

Item	Description
Enable/Disable	Enables or disables the APP QoS feature.
Traceable	Traceable applications are those whose traffic can be 100% traced. All protocols under this tab can have a specific QoS class assigned. Enable - Select to enable QoS for the application. Apply to all - Select a QoS class to be applied to all protocols. You can override the QoS class for specific protocols using the Action dropdown listbox.
Untraceable	Untraceable applications are detected when they attempt to establish connections to remote hosts, and all traffic between the remote hosts and the local network will be placed under QoS, within the same QoS class. All protocols under this tab can have a specific QoS class assigned. Enable - Select to enable QoS for the application. Action - Select a QoS class to be applied to all applications.
Select All	Click to select all Enabled checkboxes.
Clear All	Click to deselect all Enabled checkboxes.

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

VII-3 User Management

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



Info

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

Web User Interface

Firewall
User Management
General Setup
User Profile
User Group
User Online Status
Objects Settings

VII-3-1 General Setup

General Setup can determine the standard (rule-based or user-based) for the users controlled by User Management. The mode (standard) selected here will influence the contents of the filter rule(s) applied to every user.

User Management >> General Setup

General Setup

The screenshot shows the 'General Setup' configuration page. It includes sections for 'Mode Selection' with radio buttons for 'Rule-Based' (selected) and 'User-Based'. The 'Authentication page' section has radio buttons for 'Web Authentication' (selected) and 'HTTP', a 'Login Page Greeting' label, and a checkbox for 'Display IP address on the dialog box pops up after successful login.'. The 'Landing page' section has a text area for a URL, a 'Preview' button, and a 'Set to Factory Default' button. At the bottom are 'OK', 'Clear', and 'Cancel' buttons.

Available settings are explained as follows:

Item	Description
Mode Selection	There are two modes offered here for you to choose. Each mode will bring different filtering effect to the users involved. User-Based - If you choose such mode, the router will apply the filter rules configured in User Management>>User Profile to the users. Rule-Based -If you choose such mode, the router will apply the filter rules configured in Firewall>>General Setup and Filter Rule to the users.
Authentication page	Web Authentication - Choose the protocol for web

	authentication. Login Page Greeting - Such link allows you to access into the setting page for login greeting. For detailed information, refer to System Maintenance>>Login Page Greeting. Display IP Address on tracking window - Check the box to display the IP address of the client on the tracking window.
Landing Page	Type the information to be displayed on the first web page when the LAN user accessing into Internet via such router.

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

VII-3-2 User Profile

This page allows you to set customized profiles (up to 200) which will be applied for users controlled under **User Management**. Simply open **User Management>>User Profile**.

[User Management >> User Profile](#)

User Profile Table

[Set to Factory Default](#)

Select All	Clear All			Search	
Profile	Enable	Name	Profile	Enable	Name
1.	☒	admin	17.	☐	
2.	☒	Dial-In User	18.	☐	
3.	☐		19.	☐	
4.	☐		20.	☐	
5.	☐		21.	☐	
6.	☐		22.	☐	
7.	☐		23.	☐	
8.	☐		24.	☐	
9.	☐		25.	☐	
10.	☐		26.	☐	
11.	☐		27.	☐	
12.	☐		28.	☐	
13.	☐		29.	☐	
14.	☐		30.	☐	
15.	☐		31.	☐	
16.	☐		32.	☐	

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

[Next](#)

Note:

1. admin: To change the administrator password, please go to System Maintenance >> Administrator Password.
2. Dial-In User Profile: Dial-In User Profile is reserved for VPN authentication.
3. During authentication, Router will check all the local user profiles first, and then the profiles in external servers.

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

User Management >> User Profile

Profile Index 1

Common Settings

☒ Enable this account	
Username	admin (Only support A-Z a-z 0-9 - . @)
Password	****
Confirm Password	
External Server Authentication	None

Login Settings

User Online Status : Block/ Unblock

Allow Authentication via	☒ Web ☒ Alert Tool ☒ Telnet
Show Landing Page After Login	☐
Idle Timeout	0 min. (0: Unlimited)
Auto Logout After	0 min. (0: Off)
Pop up Time Tracking Window	0
Login Permission	Schedule None None None None

Policy

Max. Login Devices	0 (0: Unlimited)
☐ Enable Time Quota	0 min. 0
☐ Enable Data Quota	0 MB 0
☐ Reset Quota Automatically To	Time Limit 0 min. Data Limit 0 MB
When	☒ Login Permission Schedule Ends ☐ Schedule Starts

Other Services

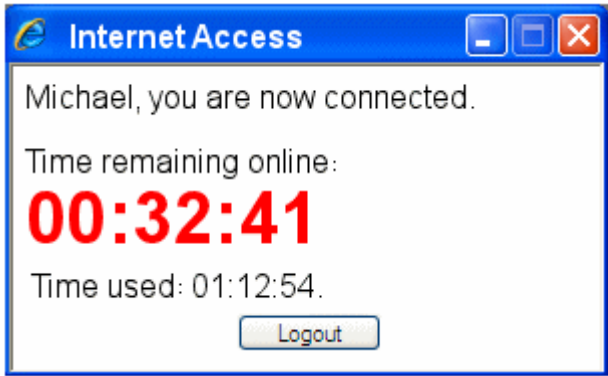
Log	None

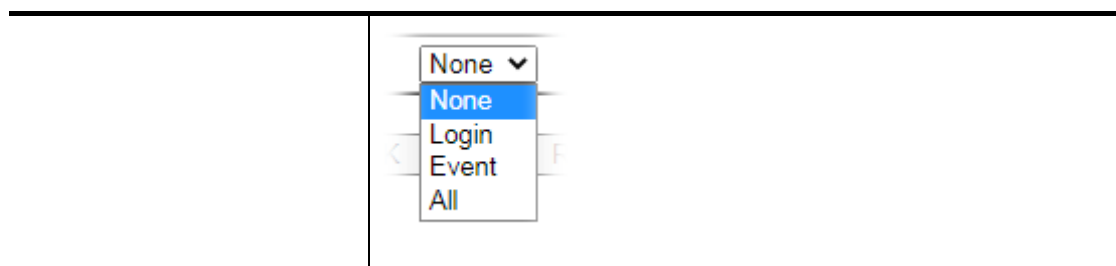
OK Refresh Clear Cancel

Available settings are explained as follows:

Item	Description
Common Settings	
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 authentication, he/she can access Internet via this router with the limitation configured in this user profile. The maximum length of the password you can set is 24

	characters.
Confirm Password	Type the password again for confirmation.
External Service Authentication	The router will authenticate the dial-in user by itself or by external service such as Radius server. If Radius is selected here, it is not necessary to configure the password setting above.
Login Settings	
Allow Authentication via	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. Web - If it is selected, the user can Enter the URL of the router from any browser. Then, a login window will be popped up and ask the user to Enter the user name and password for authentication. If succeed, a Welcome Message (configured in User Management >> General Setup) will be displayed. After authentication, the destination URL (if requested by the user) will be guided automatically by the router. Alert Tool - If it is selected, the user can open Alert Tool and Enter the user name and password for authentication. A window with remaining time of connection for such user will be displayed. Next, the user can access Internet through any browser on Windows. Note that Alert Tool can be downloaded from DrayTek web site. Telnet - If it is selected, the user can use Telnet command to perform the authentication job.
Show Landing Page After Login	When a user tries to access into the web user interface of Vigor router series with the user name and password specified in this profile, he/she will be lead into the web page configured in Landing Page field in User Management>>General Setup. Check this box to enable such function.
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.
Auto Logout After	Such account will be forced to logout after a certain time set here.
Pop up Time-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.
Login Permission Schedule	You can Enter 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.
Policy	
Max. Login Devices	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.

Enable Time Quota	Time quota means the total connection time allowed by the router for the user with such profile. Check the box to enable the function of time quota. The first box displays the remaining time of the network connection. The second box allows to Enter the number of time (unit is minute) which is available for the user (using such profile) to access Internet.  - Click this box to set and increase the time quota for such profile.  - Click this box to decrease the time quota for such profile. Note: A dialog will be popped up to notify how many time remained when a user accesses into Internet through Vigor router successfully.  When the time is up, all the connection jobs including network, IM, social media, facebook, and etc. will be terminated.
Enable Data Quota	Data Quota means the total amount for data transmission allowed for the user. The unit is MB/GB.  - Click this box to set and increase the data quota for such profile.  - Click this box to decrease the data quota for such profile.
Reset Quota Automatically To	Check the box to set default time quota and data quota for such profile. Vigor router will reset the quota automatically according to the factory quota settings. Time Limit - Enter the value for the time manually. Data Limit - Enter the value for the data manually. Login Permission Schedule Ends - When the scheduling time is up, the router will reset the quota with user-defined time/data values automatically. Schedule - The router will reset the quota with user-defined time/data values at the starting time configured in the selected schedule profile.
Other Services	
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).



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

VII-3-3 User Group

This page allows you to bind several user profiles into one group. These groups will be used in **Firewall>>General Setup** as part of filter rules.

User Management>>User Group

User Group Tables 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 FW Access Group A
5 FW Access Group B

Selected User Objects(Max 32 Objects)

OK

Clear

Cancel

Available settings are explained as follows:

Item	Description
Name	Type a name for this user group.
Available User Objects	You can gather user profiles (objects) from User Profile page within one user group. All the available user objects that you have created will be shown in this box. Notice that user object, Admin and Dial-In User are factory settings. User defined profiles will be numbered with 3, 4, 5 and so on.

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.

VII-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

LAN
Hotspot Web Portal
Profile Setup
Quota Management
Routing

VII-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.	☒		Click-through	None	Preview
2.	☐		Click-through	None	Preview
3.	☒		Click-through	None	Preview
4.	☐		Click-through	None	Preview

[Preview Hotspot from WAN and VPN](#)

Notes:

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.
3. If you want to enable Preview Hotspot from WAN and VPN, please set up Internet Access Control.

[OK](#)

Backup up: [Profile 1](#) [Backup](#) Restore: [Profile 1](#) [Restore](#) [Restore Quota Management Setting](#)

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.
Preview hotspot from WAN and VPN	Check the box to enable the function of previewing hotspot from WAN and VPN.
Backup up	Select Profile 1 (index 1) or Profile 2 (index 2) and click the Backup button to save the configuration settings as a backup file.
Restore ...	Specify an existed backup file first and select Profile 1 (index 1) or Profile 2 (index 2) to apply the backup file to. Click the Restore button to perform the job. Restore Quota Management Setting - After checking the box, those settings related to bandwidth/session limit will be restored at the same time.

VII-4-1-1 Login Method

There are several login methods to choose from for authenticating network clients. Each login mode will present a different web page to users when they connect to the network.

(A) Skip Login, landing page only

This mode does not perform any authentication. The user will be redirected to the landing page. The user can then leave the landing page to visit other websites.

(B) Click-through

The following page will be shown to the users when they first attempt to access the Internet through the router. After clicking **Accept** on the page, users will be directed to the landing page (defined in Captive Portal URL) and be granted access to the Internet.

(C) Various Hotspot Login

An authentication page will appear when users attempt to access the Internet for the first time via the router. After authenticating themselves using a Facebook, Google account, PIN code, password for RADIUS sever, they will be directed to the landing page and be granted access to the Internet.

(D) External Portal Server

External RADIUS server will authenticate the users when they attempt to access the Internet for the first time via the router.

VII-4-1-2 Steps for Configuring a Web Portal Profile



Login Method

Click the index link (e.g., #1) of the selected profile to display the following page.

1 Login Method 2 Background 3 Login Page Setup 4 Whitelist Setting 5 More Options

☐ Enable this profile

Comments:

Portal Server

Portal Method

- ☐ Skip Login, landing page only
- ☐ Click through
- ☒ Various Hotspot Login
- ☐ External Portal Server

Captive Portal URL portal.draytek.com

Login Methods

Chosen Login Method

- ☒ Login with Facebook
Note: When Login with Facebook is selected, the protocol of the Captive Portal URL will be changed to HTTPS.
- ☐ Login with Google
- ☐ Receive PIN via SMS
- ☐ Receive PIN via Mail
- ☐ Login with RADIUS

Available settings are explained as follows:

Item	Description
Enable this profile	Check to enable this profile.
Comments	Enter a brief description to identify this profile.
Portal Server	
Portal Method	There are four methods to be selected as for portal server. <i>When Skip Logging, landing page only or Click through is selected as Portal Method</i>
Captive Portal URL	Enter the captive portal URL. <i>When Various Hotspot Login is selected as Portal Method</i>
Captive Portal URL	Enter the captive portal URL.
Login Methods	This setting is available when Various Hotspot Login is selected as the portal method. Choose Login Method - Select one or more desired login methods. ● Login with Facebook ● Login with Google ● Receive PIN via SMS ● Receive PIN via Mail ● Login with RADIUS
Facebook (Login with	This setting is available when Login with Facebook is selected as the login method.

Facebook)	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.
Google (Login with Google)	This setting is available when Login with Google is selected as the login method. 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.
SMS Provider (Receive PIN via SMS)	This setting is available when Receive PIN via SMS is selected as the login method. Receiving PIN via SMS Provider - Select the SMS Provider to send PIN notifications. The SMS providers are configured in Objects Setting >> SMS/ Mail Service Object.
Mail Server (Receive PIN via Mail)	This setting is available when Receive PIN via Mail is selected as the login method. Receiving PIN via Mail Server - Select the mail server to send PIN notifications. The mail servers are configured in Objects Setting >> SMS/ Mail Service Object.
Radius Server (Login with RADIUS)	This setting is available when Login with RADIUS is selected as the login method. Authentication Method - Click link to configure the external RADIUS server for authenticating web portal clients. RADIUS MAC Authentication - Check Enable to activate user authentication by MAC address. MAC Address Format - Select the MAC address format that is used by the RADIUS server.
<i>When External Portal Server is selected as Portal Method</i>	
Redirection URL	Enter the URL to which the client will be redirected.
RADIUS Server	Authentication Method - To configure the RADIUS server, click the <u>External RADIUS Server</u> link and you will be presented with the configuration page. RADIUS MAC Authentication - If the RADIUS server supports authentication by MAC address, enable RADIUS MAC Authentication and select the MAC address format that is used by the RADIUS server. MAC Address Format - Select the MAC address format.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to save the configuration on this page and proceed to the next page.

If you have chosen **Skip Login, landing page only** or **External Portal Server** as the portal method, skip to step 4 *Whitelisting* below.

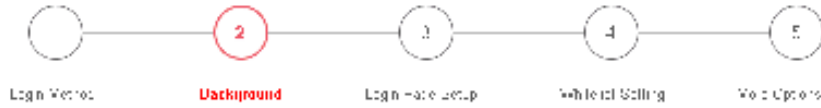
Otherwise, proceed to configure the login page by following steps 2 and 3.

2

Background

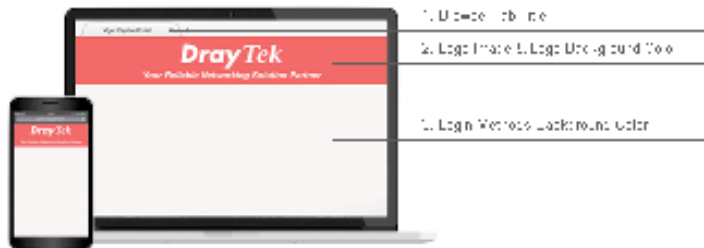
If you have selected a Login Mode that requires authentication, select a background for the login page.

Hisque Web Portal >> Profile Setup



Choose Login Background

☒ Color Background



☐ Image Background



Browser Tab Title

DrayTek Web Portal

Login Image

Default DrayTek Login Image



Login Background Color

Color Code

FFFFFF

Hex Color

Preview

Login Method Background Color

Color Code

FFFFFF

Hex Color

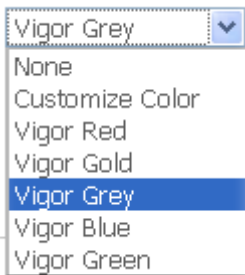
Preview

Cancel

OK

Available settings are explained as follows:

Item	Description
Choose Login Background	Select either Color Background or Image Background as the login page background scheme.
Browser Tab Title	Enter the text to be shown as the webpage title in the browser.

Logo Image	The DrayTek Logo will be displayed by default. However, you can enter HTML text or upload an image to replace the default logo.
Login Method Background Color	Select the background color of the login panel from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color. 
Opacity (10 ~ 100)	Available when Image Background is selected. Set the opacity of the background image.
Background Image	Available when Image Background is selected. Click Browse... to select an image file (.JPG or .PNG format), then click Upload to upload it to the router.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

If you have selected **Skip Login, landing page only** or **External Portal Server** as the portal method, proceed to Step 4 *Whitelist Setting*; otherwise, continue to Step 3 *Login Page Setup*.

3

Login Page Setup

In this step you can configure settings for the login page.

Click Through

This section describes the Login Page setup if you have selected **Click Through** as the Login Method.

Hotspot Web Portal >> Profile Setup



Configure Login Method and Details

Welcome! We are pleased to provide free Wi-Fi to you! By clicking the button below you agree to the Terms and Conditions Accept	Welcome Message Terms and Conditions Description and Content Accept Button Description and Color
Welcome Message By clicking the button below you agree to the Terms and Conditions. (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 1300 characters)	
Accept Button Description By clicking the button below you agree to the Terms and Conditions. (Max 170 characters) Default	
Accept Button Color Customize Color ☒ AAAA if used: FFFFFFFF; Reset Default	
Back and Next Cancel	

Available settings are explained as follows:

Item	Description
Welcome Message	Enter the text to be displayed as the welcome message.
Terms and	Enter the text to be displayed as the Terms and Conditions

Conditions Description	hyperlink text.
Terms and Conditions Content	Enter the text to be displayed in the Terms and Conditions pop-up window.
Accept Button Description	Enter the text to be displayed on the accept button
Accept Button Color	Select the color of the accept button from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

Various Hotspot Login

This section describes the Login Page setup step if you have selected Various Hotspot Login the login method. You will see only settings that are relevant to the selected login method(s).

Hotspot Web Portal >> Profile Setup



Configure Login Method and Details

Welcome!
Please log in to enjoy Wi-Fi.
By clicking here, you agree to the [Terms and Conditions](#).

Log in with Facebook

Log in with Google

Or login with PIN code

Receive PIN via SMS

Enter Captch PIN

Or login with your account

Username

Password

Welcome Message

Terms and Conditions Description and Content

Facebook Login

Google Login

Hint Message for PIN

Receive PIN via SMS Description

Enter PIN and Submit Option

Hint Message for RADIUS

RADIUS Login

Welcome Message

Enter the text to be displayed as the welcome message.

(Max 1360 characters)

Terms and Conditions Description

Enter the text to be displayed as the Terms and Conditions hyperlink text.

(Max 170 characters)

Terms and Conditions Content

Enter the text to be displayed in the Terms and Conditions pop-up window.

(Max 1100 characters)

Settings that are common to Facebook, Google, PIN, and RADIUS authentication are:

Item	Description
Welcome Message	Enter the text to be displayed as the welcome message.
Terms and Conditions Description	Enter the text to be displayed as the Terms and Conditions hyperlink text.
Terms and Conditions Content	Enter the text to be displayed in the Terms and Conditions pop-up window.

If you have selected Facebook login, the setting will appear:

Facebook Login Description

(Max 170 characters)

Save

Item	Description
Facebook Login Description	Enter the text to be displayed on the Facebook login button.

If you have selected Google login, the setting will appear:

Google Login Description

(Max 170 characters)

Save

Item	Description
Google Login Description	Enter the text to be displayed on the Google login button.

If you have selected PIN login, these settings will appear:

Hint Message for PIN	Log in with PIN code.
	(Max 100 characters) Default
Receiving PIN via SMS Description	Received PIN via SMS
	(Max 100 characters) Default
Receiving PIN via SMS Content	Message to Display: Received Your PIN is <PIN>. This PIN is valid for 10 min.
	(Max 150 characters) Default
Enter PIN Description	Enter Extending PIN
	(Max 100 characters) Default
Submit Button Description	Open Style: Color: #FFFFFF Submit Button
	(Max 100 characters) Default
Submit Button Color	Color Picker ADD Remove Pick Default

Item	Description
Hint Message for PIN	Enter the text used to suggest users to choose SMS authentication.
Receiving PIN via SMS Description	Enter the text to be displayed on the button that the user clicks to receive an SMS PIN.
Receiving PIN via SMS Content	Enter the message to be sent by SMS to inform the user of the PIN. The PIN variable is specified by <PIN> within the message.
Enter PIN Description	Enter message to be displayed in the PIN textbox to prompt the user to enter the PIN.
Submit Button Description	Enter the text to be displayed on the submit PIN button
Submit Button Color	Select the color of the submit button from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.

If you have selected RADIUS account login, these settings will appear:

The screenshot shows a configuration page with the following fields:

- Hint Message for RADIUS:** Text input with "Log in with your account." and "(Max 170 characters)".
- RADIUS Account Description:** Text input with "Reserve" and "(Max 170 characters)".
- RADIUS Password Description:** Text input with "Password" and "(Max 170 characters)".
- Login Button Description:** Text input with "Open Key Authentication Window To Login" and "(Max 170 characters)".
- Login Button Color:** A color selection interface with a dropdown menu showing "Customize Color", an RGB input field with "255, 255, 255", and a "Preview" button.

Item	Description
Hint Message for RADIUS	Enter the text used to suggest users to choose RADIUS authentication.
RADIUS Account Description	Enter a brief description for reminding the user about the account.
RADIUS Password Description	Enter a brief description for reminding the user about the password.
Login Button Description	Enter the text to be displayed on the login button.
Login Button Color	Select the color of the login button from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.

And finally, the save and cancel buttons are always displayed.

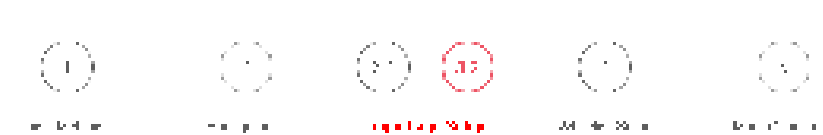


Item	Description
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

2nd-stage Page for PIN Login

If you have selected **PIN Login** as the login method, you will also need to configure the page that is displayed to users when they request a PIN.

to establish a "Library



• [Impressions and Clicks](#) • [CTR](#) • [Conversions](#)

[illegible]

Available settings are explained as follows:

Item	Description
Back Button Description	Enter text for the label of the hyperlink to return to the previous page.
PIN Code Message	Enter text to be displayed as the body text on the page.
Default Country	Select the default country code to be displayed using the dropdown

Code	menu.
Enter Mobile Number Description	Enter message to be displayed in the mobile number textbox to prompt the user to enter the mobile number.
Send Button Description	Enter the label text of the send button.
Send Button Color	Select the color of the send button from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.
Send Succeeded Message	Enter text to be displayed to notify the user after the PIN has been sent.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

4

Whitelist Setting

In this step you can configure the whitelist settings. Users are allowed to send and receive traffic that satisfies whitelist settings.

Hostpot Web Portal >> Profile Setup

1 2 3 4 5

Login Method Background Login Page Setup **Whitelist Setting** Web Options

NAT Rules	Dest Domain	Dest IP	Dest Port	Source IP
☐ Allow access to Internet without restriction ☐ Allow access to Internet with restriction ☐ Allow access to Internet with restriction				

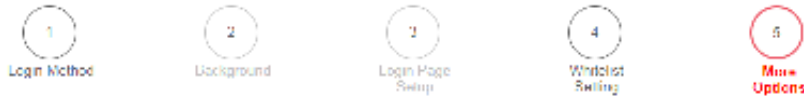
Save and Next Cancel

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.

In this step you can configure advanced options for the Hotspot Web Portal.

Hotspot Web Portal >> Profile Setup



Quota Management

Login Method	Quota Policy Profile	Valid Time	Device Allowed	Bandwidth Limit	Session Limit
Skip Login	1. Default	00:50:00	Unlimited	Unlimited	Unlimited
Bypass	1. Default	00:50:00	Unlimited	Unlimited	Unlimited

Note:

To modify the quota settings, please go to **Hotspot Web Portal >> Quota Management**

JSON API

☐ Enable JSON API

Server URL:

Get JSON and Update user status every hours min

Update information:

☐ NAS-Identifie ☐ MAC Address ☐ All User Number ☐ Wi-Fi User Number

Web Portal Options

HTTPS Redirection

☒ Enable

When an unauthorized 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 unauthorized 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 Redirection.

Bypass

☐ Enable

If the number of https sessions exceed the default limit, web portal would temporarily bypass them without authentication.
Those users would be redirected to web portal and authenticate later.

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

Force Landing Page Stay ☐ Enable for seconds

Note:

Landing Page may not update the complete button in some mobile browsers when the browser stay in the page too long.

Applied Interfaces

Subnet		☐ LAN1 ☐ LAN2 ☐ LAN3 ☐ LAN4
Wi-Fi	2.4G	☐ SSID1 (EasyTos)
		☐ SSID2 (EasyTos - Guest)
		☐ SSID3
		☐ SSID4
	5G	☐ SSID1 (EasyTos_5G)
		☐ SSID2 (EasyTos_5G - Guest)
		☐ SSID3
		☐ SSID4

Available settings are explained as follows:

Item	Description
Quota Management	
Quota Policy Profile	Choose a policy profile to apply to web portal client.
Web Portal Options	
HTTPS Redirection	If this option is selected, unauthenticated clients accessing HTTPS websites will be redirected to the login page, but the browser may alert the user of certificate errors. If this option is not selected, attempts to access to HTTPS website will time out without redirection.
Captive Portal Detection	If this option is selected, the web portal page is triggered automatically when an unauthenticated client tries to access the Internet. This function is not available when the Login Mode is Social Login , as the web portal page may not be shown correctly due to the limitations of the operating system's built-in Captive Portal Detection.
Landing Page After Authentication	
Fixed URL	Specifies the webpage that will be displayed after the user has successfully authenticated. The user will be redirected to the specified URL. This could be used for displaying advertisements to users, such as guests requesting wireless Internet access in a hotel.
User Requested URL	The user will be redirected to the URL they initially requested.
Bulletin Message	The message configured here will be briefly shown for a few seconds to the user. Default Message – This button is enabled when Bulletin Message is selected. Click to load the default text into the bulletin message textbox.
Applied Interfaces	
Subnet	The current Hotspot Web Portal profile will be in effect for the selected subnets.
WLAN	The current Hotspot Web Portal profile will be in effect for the selected WLAN SSIDs.
Finish	Click to complete the configuration.
Cancel	Click to abort the configuration process and return to the profile summary page.

VII-4-2 Quota Management

The system administrator can specify bandwidth and sessions quota which is only applicable to the web portal clients.

Settings configured in Quota Management will override the policies set in **Bandwidth Management>>Bandwidth Limit** and **Bandwidth Management>>Limit**.

Hotspot Web Portal >> Quota Management

Web Portal Bandwidth and Session Limit

The settings here will apply only to the web portal clients and will override the policies set in Bandwidth Management.

☐ Bandwidth Limit

☐ Session Limit

Quota Policy Profile

Index	Name	Expired Time after First Login	Device Allowed per Account	Reconnection Time Restriction	Bandwidth Limit	Session Limit
1	Default	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Add (up to 20)						

Available settings are explained as follows:

Item	Description
Bandwidth Limit	Check the box to override the policy configured in Bandwidth Management>>Bandwidth Limit .
Session Limit	Check the box to override the policy configured in Bandwidth Management>>Session Limit .
Quota Policy Profile	Add - Create up to 20 policy profiles in such page.

To create a new quota policy profile, click Add to open the following page.

Hotspot Web Portal => Management => Quota Policy Profile 2

Profile Name	level 2		
Account Validity			
Expired Time After the First Login	0	days	5
		hours	0
		min	0
☐ Idle Timeout	0	min	
Device Control			
Devices Allowed per account	Unlimited		
☐ Reconnection Time Restriction	☐ At 0:0 everyday Block the same user from reconnecting before the set time ☒ 0 hours 0 min Block the same user from reconnecting for the set period		
Bandwidth and Session Limit			
☐ Bandwidth Limit			
Download Limit	0	☒ Kbps ☐ Mbps	
Upload Limit	0	☒ Kbps ☐ Mbps	
☐ Session Limit	0	sessions	
Cancel OK			

Available settings are explained as follows:

Item	Description
Profile Name	Enter a name for a new profile.
Account Validity	Set a period of valid time for the client accessing Internet via web portal. Expired Time After the First Login - Set the days, hours, and minutes. After expired time, Vigor router will block the client to access into network/Internet. Idle Timeout - After checking the box, Vigor router will terminate the network connection if no activity for the user account after the time configured here.
Device Control	Set the number of devices that each account can control, and specify the time restriction for the client accessing Internet via web portal. Decices Allowed per account - Use the drop-down list to select a number. Each account allows the number of devices (defined here) for accessing into network. Reconnection Time Restriction - For each account, Vigor router can set a time for network connection ● At ... Everyday - Set the time to block the same client from reconnecting Vigor router before the time set here. ● Hours. min - Set the time period to block the same client from reconnecting Vigor router.
Bandwidth and	Bandwidth Limit - Check the box to configure bandwidth limit for

Session Limit	web portal client. ● Download/Upload Limit - Set a value. Session Limit - Check the box to configure session limit for web portal client.

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

Application Notes

A-1 How to allow users login to Vigor's Hotspot with their social media accounts (e.g., Facebook & Google)

Vigor Router supports Hotspot Web Portal function. The network administrator can set Vigor Router as a Hotspot provider with web authentication and allow users to log in with their social media accounts, such as Facebook and Google. We demonstrate how to set up the hotspot web portal with Facebook login in the following paragraphs.

Vigor Router Setup

1. Make sure the router is connected to the Internet.

Online Status

Physical Connection				System Uptime: 0day 0:11:28	
IPv4		IPv6			
LAN Status		Primary DNS: 168.95.1.1		Secondary DNS: 168.95.192.1	
IP Address	TX Packets	RX Packets			
192.168.60.1	5,950	6,130			
WAN 1 Status					
Enable	Line	Name	Mode	Up Time	>> Drop PPPoE
Yes	Ethernet		PPPoE	0:11:23	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
192.168.60.1	168.95.1.1	5,041	215	5,689	393

2. Go to **Hotspot Web Portal >> Profile Setup**, click on an available index.

Hotspot Web Portal >> Profile Setup

Hotspot Web Portal Profile:

Index	Enable	Comments	Login Mode	Applied Interface	
1.	☐		Click-through	None	Preview
2.	☐		Click-through	None	Preview
3.	☐		Click-through	None	Preview
4.	☐		Click-through	None	Preview

Note:

1. The router must connect to the Internet before webpage redirection will work.
2. If the LAN clients are using another DNS server on LAN, please make sure the DNS query for domain name "portal.draytek.com" will be resolved by the router.

OK

3. Enter the values as the following figure.

The screenshot displays a configuration window for a hotspot profile. At the top, there is a checkbox labeled 'Enable this profile' which is checked. Below it is a 'Comments' field containing the text 'Guest User'. The 'Portal Server' section includes a 'Portal Method' dropdown menu with three options: 'Skip Login, landing page only', 'Click through', and 'Various Hotspot Login', with the last option selected. The 'Captive Portal URL' field is set to 'http://portal.digicomm.com'. The 'Login Methods' section has a 'Choose Login Method' dropdown with three options: 'Login with Facebook', 'Login with Google', and 'Receive PIN via SMS', with the first two options selected. Below this, there are sections for 'Facebook' and 'Google'. The 'Facebook' section contains fields for 'Facebook APP ID' (238347750110670) and 'Facebook APP Secret'. The 'Google' section contains fields for 'Google App ID' (1010517584014-2158444444) and 'Google App Secret'. At the bottom right, there are 'Save and Next' and 'Cancel' buttons.

☒ Enable this profile

Comments: Guest User

Portal Server

Portal Method

- ☐ Skip Login, landing page only
- ☐ Click through
- ☒ Various Hotspot Login

Captive Portal URL: http:// portal.digicomm.com

Login Methods

Choose Login Method

- ☒ Login with Facebook
- ☒ Login with Google
- ☐ Receive PIN via SMS

Facebook

Facebook APP ID: 238347750110670

Facebook APP Secret:

Google

Google App ID: 1010517584014-2158444444

Google App Secret:

Save and Next Cancel

- Click **Enable this profile**.
- Enter the comments.
- Select **Various Hotspot Login** for Portal Method.
- Choose **Login with Facebook** or **Login with Google** as Login Method.

If **Login with Facebook** is selected, the protocol of the **Captive Portal URL** need to be changed to **HTTPS** instead of **HTTP** because Facebook force to use **HTTPS** URL in their policy.

- Enter the **APP ID** and **secret**.
- Click **Save and Next**.

- Choose the **Color Background**, customize the information a logo color, and click **Save and Next**.

Hotspot Web Portal Profile Setup



Choose Login Background

☒ Color Background

1. Browser Tab Title
2. Logo Image & Logo Background Color
3. Login Methods Background Color

☐ Image Background

1. Browser Tab Title
2. Logo Image
3. Login Methods Background Color and Opacity
4. Background Image

Login Page URL:
 Browser Tab Title:

Logo Image:

Logo Background Color:

Login Method Background Color:

You can click the Step Icon on the top of the page to go to the step you want. The router will save your setting automatically.

Or choose the **Image Background**, customize the information and background image, and click **Save and Next**.

Hotspot Web Portal > Profile Setup



Choose Login Background

☐ Color Background



☒ Image Background



Login Page URL	portal.draytek.com
Browser Tab Title	DrayTek Hotspot

Logo Image	[Default: DrayTek Logo Icon]

Login Method Background Color	VigenGold	default: #FFD700	Provide
Opacity(10 ~ 100)	90	%	

Background Image	Choose File No file chosen	(max size: 1MB) Upload

5. Customize the descriptions on the login page, then click **Save and Next**.

Configure Login Method and Details


Welcome!
 Please login to enjoy Wi-Fi.
 By clicking on these buttons you agree to the
[Terms and Conditions](#)


 Login with Facebook


 Login with Google

Welcome Message

Welcome to Wireless VideoShare />Please log in to enjoy Wi-Fi.
 (Max 1280 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 1280 characters)

Facebook Login Description

Log in with Facebook

(Max 170 characters)

Default

Google Login Description

Log in with Google

(Max 170 characters)

Default

Save and Next Cancel

6. You can set the **Whitelist** for the profile here to allow specific clients to access the internet or certain websites can be visited without login.

Hotspot Web Portal or Profile Setup

1

2

3

4

5

Login Method

Background

Login Page Setup

Whitelist Setting

Other Options

NAT Rules	Dest Domain	Dest IP	Dest Port	Source IP
Allows all outgoing connections from hosts in		☐ NAT rule Port Redirection ☐ NAT rule Open Ports ☐ NAT rule DMZ		

Save and Next Cancel

- Set up the **Expired Time After Activation** and **Landing Page After Activation** that Hotspot clients will see after they login successfully. Finally, select the interfaces to which you would like this hotspot profile apply to, then click **Finish** to save the setting.

Hotspot Web Portal >> Profile Setup

1
Login Method

2
Background

3
Login Page Setup

4
Website Setting

5
More Options

Web Portal Options

Expired Time After Activation: 0 min days 0 min hours 0 min mins

HTTP Proxy: ☐ Enable
 When an access point is detected logging in HTTP proxy page, internet will work but certificate error may be shown.
 If both the access point and only HTTP proxy, HTTP proxy will be used without redirection and also no certificate error.

Captive Portal Redirection: ☐ Enable
 If access point is detected logging in captive portal page, the Web Portal page will connect to WFTL.
 If the location is not available, redirection using default page because the page may not be shown correctly due to the limitation of the OS built-in Captive Portal.
 If enable

Landing Page After Activation:

④ Read URL:

⑤ Use Redirect URL: ☐

⑥ Public Message:

(Max 500 characters) Default Message

Note:
 Landing Page may not be shown correctly when using DHCP with the Captive Portal Redirection.

Applied Interfaces:

Interface	SSID	SSID	SSID	SSID	SSID
WLAN	2.4G	☒ LAN1	☒ LAN2	☒ LAN3	☒ LAN4
		☒ SSID1 (PAC_Vietnam_2022_VLC_park)	☒ SSID2 (DryTalk_Park-1)	☒ SSID3	☒ SSID4
		☒ SSID5	☒ SSID6	☒ SSID7 (DryTalk_5G)	☒ SSID8 (DryTalk_Park-2)
		☒ SSID9	☒ SSID10	☒ SSID11	☒ SSID12
		☒ SSID13	☒ SSID14	☒ SSID15	☒ SSID16
	5G				

Cancel Finish

- Then the Hotspot setup is finished. You may click Preview to check the login page.

Hotspot Web Portal >> Profile Setup

Hotspot Web Portal Profile:

Index	Enable	Comments	Login Mode	Applied Interface	
1	☒	DryTalk	Secret Login	LAN[1]	Preview
2	☐		Click-through	None	Preview
3	☐		Click-through	None	Preview
4	☐		Click-through	None	Preview

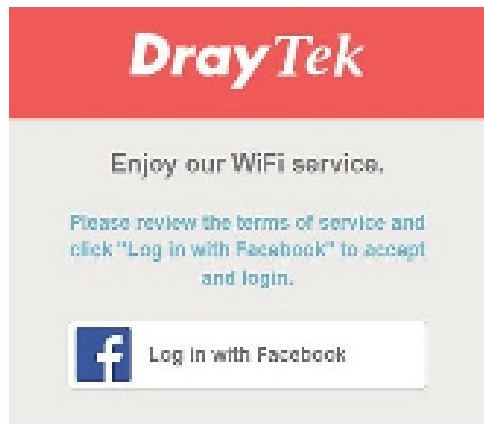
Note:

- The router must connect to the Internet before webpage redirection will work.
- If the LAN clients are using another DNS server on LAN, please make sure the DNS query for domain name "portal.thyaltalk.com" will be resolved by the router.

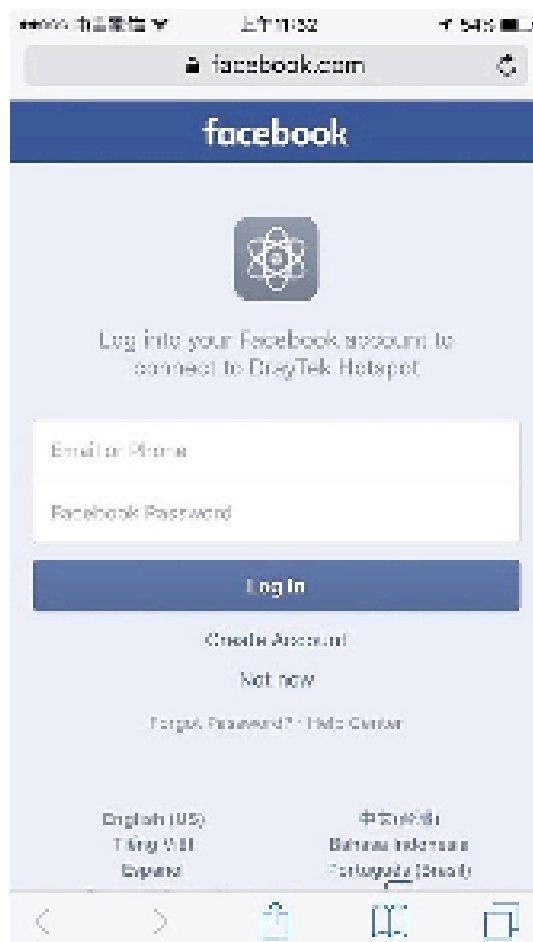
OK

Hotspot Clients Login

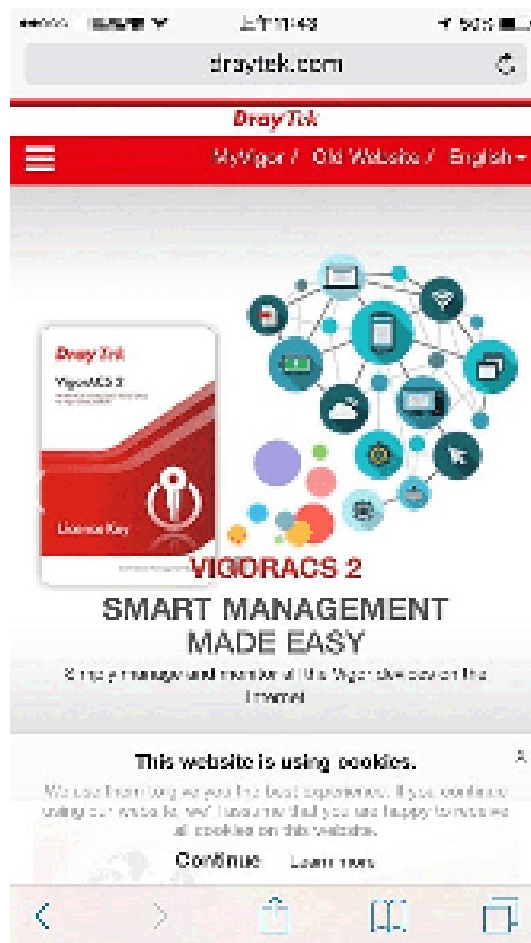
- Now, when clients connect to the selected router interface, and try to access internet, they will be redirected to "portal.draytek.com".



- Due to security concerns, the browser might warn that it cannot verify server identity, the clients would need to tap "Continue" before they can proceed to portal.draytek.com.
 - The client might not be able to access "portal.draytek.com" if this domain name is resolved by a DNS server on LAN. If so, set up LAN DNS to make sure the domain name will be resolved to the router's LAN IP.
- Tap on a login method, and it will open the social media login page. Enter the social media accounts and password to log in.



11. If the credentials are correct, the client will be redirected to the landing page and be able to access the Internet afterward.



User Information

Network administrator can plug the USB disk to router, to record the basic information of the users who connect to the Wi-Fi and login with their social media accounts. The users' basic information will be listed on Hotspot Web Portal >> Users Information page.

Hotspot Web Portal >> Users Information

User Info

Database Setup

☒ Select Columns to Filter Users

Profile	Login Method
☐ Profile 1	☐ Facebook
☐ Profile 2	☐ Google
☐ Profile 3	☐ Pincodes
☐ Profile 4	☐ Click

OK

User Table

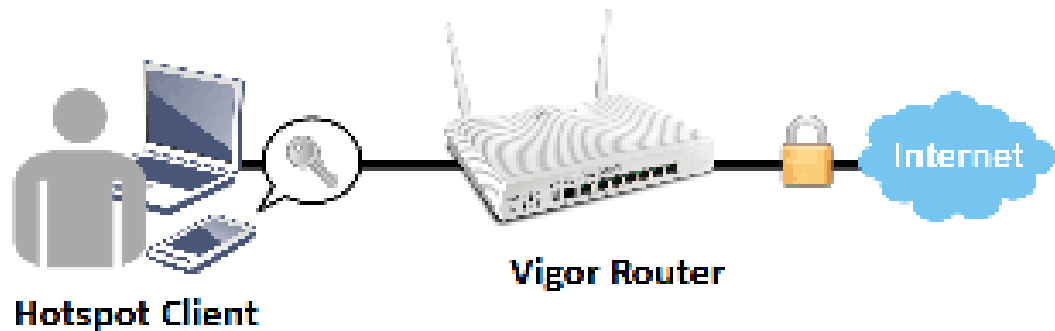
Auto Refresh (per min) | [Refresh Now](#)

2 Online Users / 2 All Users | User: | Search

Index	Status	Profile	User	Login Method	IP	MAC	Email	Phone Number	Expired Time	
1	Online	1	THINK Internet	facebook	192.168.162.10	00:7a:b9:1d:3d:c1	yves@ujt11@gmail.com	-	2017-10-25 22:04:04	
2	Online	1	www.Zhang	facebook	192.168.162.11	6c:8f:6c:1a:0a:0a	maykewendy@gmail.com	-	2017-10-25 11:08:57	

A-2 How to allow hotspot clients to get login PIN code via SMS?

Since 3.8.4.3 version firmware, Vigor Router can act as a hotspot gateway and provide internet access only to the authenticated clients. Network Administrator may set up the router to allow hotspot client to get the login PIN code from an SMS message. This note is going to demonstrate how to set up Vigor Router as a hotspot gateway and be able to send the PIN code to clients by SMS messages.



Vigor Router Setup

1. Make sure the router is connected to the Internet.

Online Status						
Physical Connection						
IPv4			IPv6			
LAN Status		Primary DNS: 168.95.1.1		Secondary DNS: 168.95.192.1		
IP Address	TX Packets		RX Packets			
192.168.60.1	5,950		6,130			
WAN 1 Status						Drop PPPoE
Enable	Line	Name	Mode	Up Time		
Yes	Ethernet		PPPoE	0:11:23		
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)	
115.168.158.95	168.95.1.1	5,841	215	5,685	303	

2. Create an SMS Object to send SMS messages. Go to **Objects Setting >> SMS Service Object**, and click on an available profile.

Objects Setting >> SMS / Mail Service Object

SMS Provider		Mail Server		Set to Factory Default	
Index	Profile Name	SMS Provider			
1		kdsms.com.tw (16)			
2		kdsms.com.tw (16)			
3		kdsms.com.tw (16)			
4		kdsms.com.tw (16)			
5		kdsms.com.tw (16)			
6		kdsms.com.tw (16)			
7		kdsms.com.tw (16)			
8		kdsms.com.tw (16)			
9	Custom 1				
10	Custom 2				

3. Enter the Service Provider details, and click **OK** to apply.

Objects Setting >> SMS / Mail Service Object

Profile Index: 1

Profile Name	hotspot
Service Provider	kdsms.com.tw (TW)
Username	*****
Password	*****
Quota	10
Sending Interval	3 (seconds)

4. Go to Hotspot Web Portal >> Profile Setup, click on an available profile.

Hotspot Web Portal >> Profile Setup

Hotspot Web Portal Profile:

Index	Enable	Comments	Login Mode	Applied Interface	
1	☐		Skip Login	None	Preview
2	☐		Skip Login	None	Preview
3	☐		Skip Login	None	Preview
4	☐		Skip Login	None	Preview

5. **Enable** the profile, give a comment, and choose “PIN Code Login”. Then click **Next**.

Hotspot Web Portal >> Hotspot Web Portal Setup

Profile 1

☒ Enable

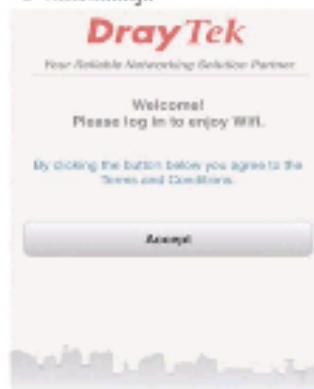
Comments:

Choose How Users Receive Internet Access:

☐ Skip Login

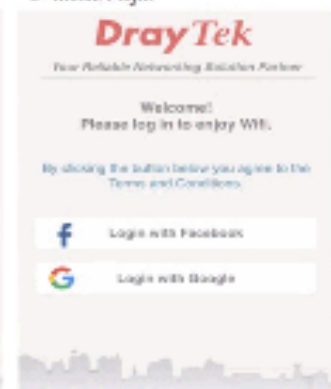
skip login phase and redirect to landing page immediately

☐ Click through



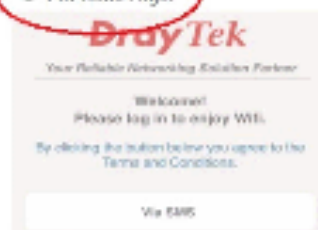
A space for you to display the terms and conditions. Users have to click 'Accept' button (wording configurable) to get WiFi access.

☐ Social Login



Login with Facebook or Google account.

☒ PIN Code Login



☐ Social or PIN Login



- Choose a login page design, customize the details, and click **Next**.

Hotspot Web Portal or Hotspot Web Portal Setup

Profile 1

Design Login Page Appearance

Color Background

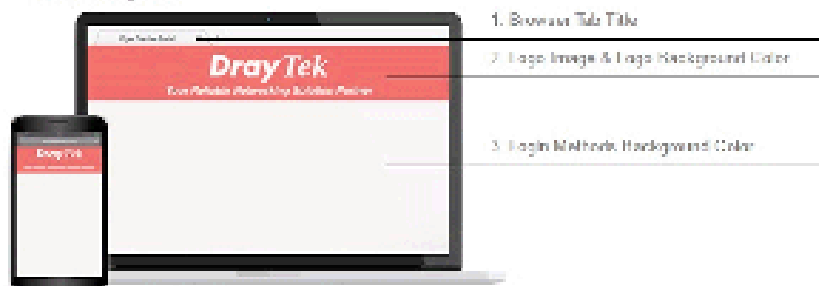


Image Background



- Edit the message on the login page, and click **Next**.

Receiving PIN via SMS Description	Get password via sms	
	(Max 170 characters)	Default
Receiving PIN via SMS Content	Welcome to DrayTek Hotspot ! Your password is <PIN>. This PIN will be valid for 10 min. (Max 150 characters)	Default
Receiving PIN via SMS Provider	1-hotspot Set SMS Provider in Objects Setting => SMS / Mail Service Object	
Enter PIN Description	Enter password	
	(Max 170 characters)	Default
Submit Button Description	Login/Font>	
	(Max 170 characters)	Default
Submit Button Color	A2A2A2 (format: FFFFFFFF)	Default

- Edit the details for SMS settings, then click **Next**.

Hotspot Web Portal Setup

Black Button Description

(Max 170 characters) Default

PIN Code Message

(Max 170 characters) Default

Default Country Code

+ 886 Taiwan

Enter Mobile Number Description

(Max 170 characters) Default

Send Button Description

(Max 170 characters) Default

Send Button Color

(hex) . FFFFFFF Default

Send Successful Message

(Max 170 characters) Default

9. Edit the landing page, choose the interfaces to which the SMS login should apply, and then click **Finish**.

Hotspot Web Portal => Hotspot Web Portal Setup

Profile 1

Configure Landing Page After Login

☒ Fixed URL

☐ User Requested URL

☐ Default Message

(Max 4095 characters) Default Message

Configure Applied Interfaces

Submit

WLAN 2.4G

☐ LAN1 ☐ LAN2

☐ SSID1 (DrayTek)

☒ SSID2 (DrayTek_Guest)

☐ SSID3

☐ SSID4

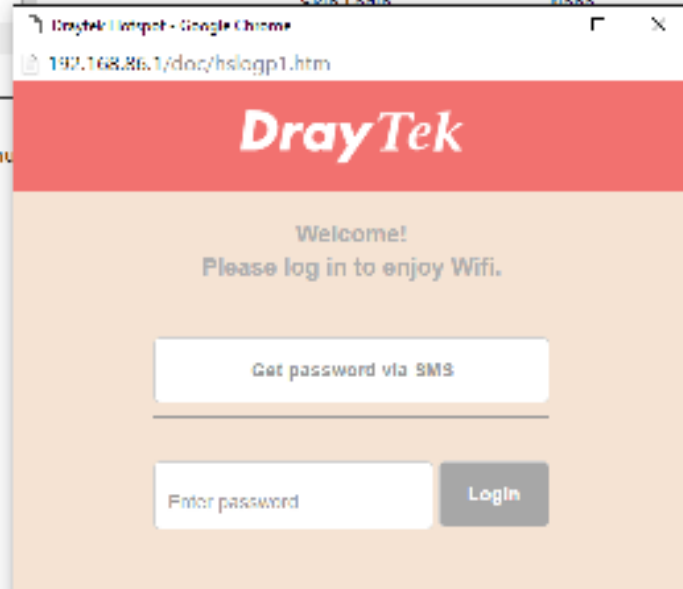
10. Now, the hotspot settings are applied to the selected interfaces. You may click **Preview** to check how the login page looks.

Hotspot Web Portal Profile

Index	Enable	Comments	Login Mode	Applied Interface	
1.	☒	SMS authentication	PIN Code Login	WI 0/0/0.4/4(2)	Preview
2.	☐		Skip Login	None	Preview
3.	☐				Preview
4.	☐				Preview

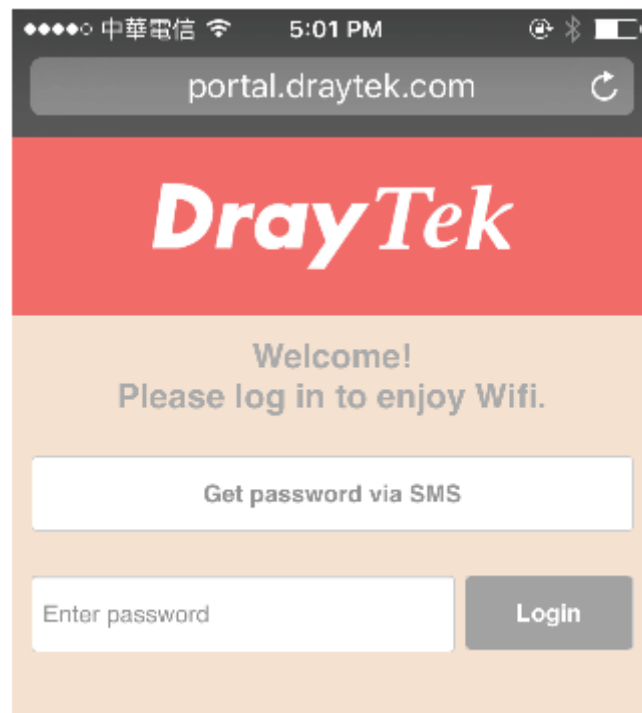
Note:

The router mu



Hotspot Client Login

11. If the client connected to the selected interface of the router and try to open a webpage, they will be redirected to hotspot login page. If they do not have a password yet, they can click on the button to get a password.





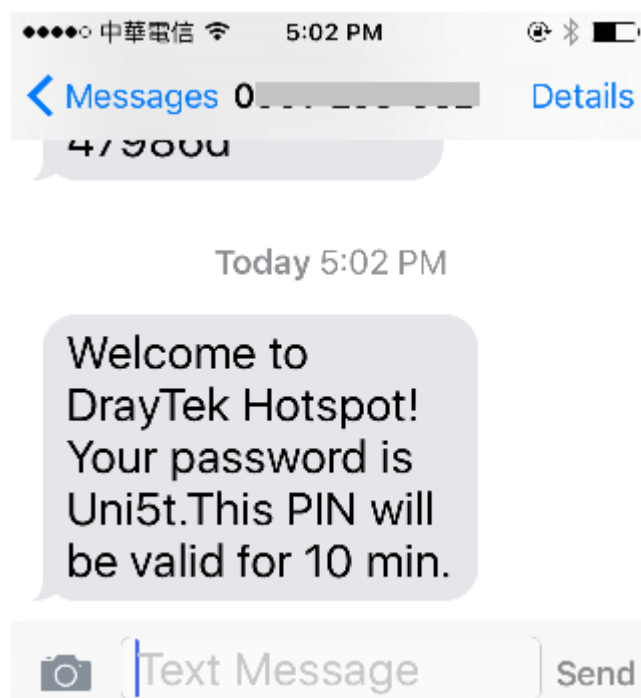
Info

- Due to security concerns, the browser might warn that it cannot verify server identity, the clients would need to tap "continue" before they can proceed to portal.draytek.com.
- The client might not be able to access "portal.draytek.com" if this domain name is resolved by a DNS server on LAN. If so, set up LAN DNS to make sure the domain name will be resolved to the router's LAN IP.

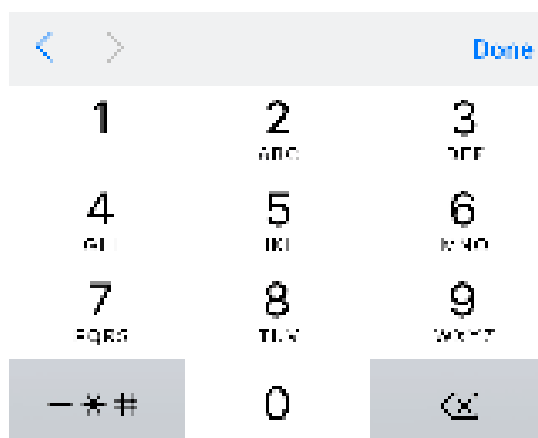
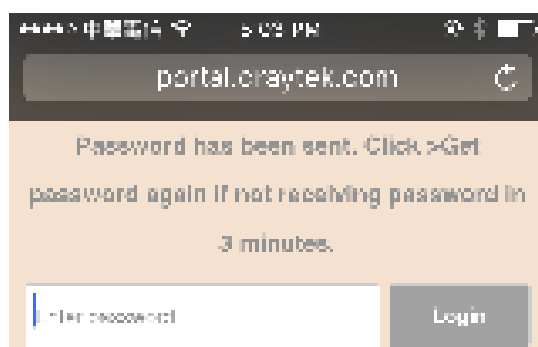
12. Enter the mobile phone number to receive the SMS message.

The screenshot shows a mobile browser interface for portal.draytek.com. At the top, the status bar displays '中華電信' (Chunghwa Telecom), signal strength, time '5:02 PM', and battery level. The address bar shows 'portal.draytek.com'. Below the address bar is a red header with the 'DrayTek' logo. The main content area has a light orange background. It starts with a back arrow icon and the text 'Password will be sent over via SMS.' Below this is a form for a phone number, with a dropdown showing '+ 886' and a text input field containing '918'. A grey button labeled 'Get password' is positioned below the phone number field. At the bottom, there is a text input field labeled 'Enter password' and a grey button labeled 'Login'.

13. The number will get a message about the password.



14. Enter the password on the login page, and click **Login**.



15. If the password is correct, the client will be redirected to the landing page, and after that, they will be able to surf the Internet.



VII-5 Central Management (AP)

Vigor2765 can manage the access points supporting AP management via Central AP Management.

AP Map

AP Map is helpful to determine the best location for VigorAP in a room. A floor plan of a room is required to be uploaded first. By dragging and dropping available VigorAP icon from the list to the floor plan, the placement with the best wireless coverage will be clearly indicated through simulated signal strength

AP Maintenance

Vigor router can execute configuration backup, configuration restoration, firmware upgrade and remote reboot for the APs managed by the router. It is very convenient for the administrator to process maintenance without accessing into the web user interface of the access point.

Load Balance for AP

The parameters configured for Load Balance can help to distribute the traffic for all of the access points registered to Vigor router. Thus, the bandwidth will not be occupied by certain access points.

AP Load Balance (Traffic overload)



Web User Interface

Central Management
AP
Status
WLAN Profile
AP Maintenance
Traffic Graph
Load Balance
External Devices

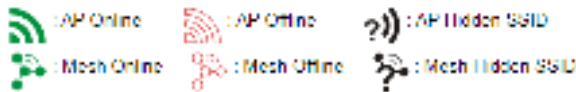
VII-5-1 Status

This page displays current status (online, offline or SSID hidden, IP address, encryption, channel, version, password and etc.) of the access points managed by Vigor router.

Central Management >> AP >> Status

Clear Refresh									
Index	Device Name	IP Address	SSID	Ch.	STA List	Uptime	Ver.	Password	
 1	VigorAP810	192.168.1.10	Daisy-Tail-A-Net-A	11	0/64	0d 00:04	1.3.2	Password	

Note:



Maximum support 20 APs

1. Display the overall mesh network information instead of the each AP in the mesh network.
2. The status of local mesh network is listed on [Mesh >> Mesh Status](#) page.
3. When AP Devices connect via an intermediary switch, please ensure that UDP:4944 port and the HTTP port of AP Devices are not blocked so that the AP status can be retrieved.

Available settings are explained as follows:

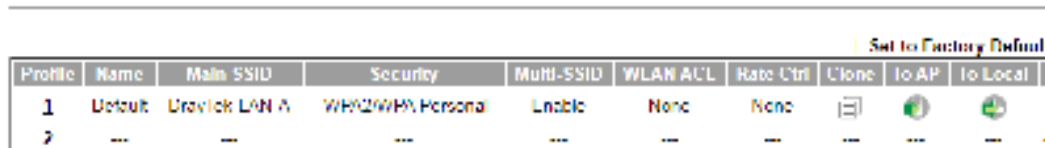
Item	Description
Index	Click the index number link for viewing the settings summary of the access point.
Device Name	The name of the AP managed by Vigor router will be displayed here.
IP Address	Display the IP address of the access point.
SSID	Display the SSID configured for the access point(s) connected to Vigor2765.
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	Vigor2765 can get related information of the access point by accessing into the web user interface of the access point. This button is used to modify the logging password of the connected access point.

VII-5-2 WLAN Profile

WLAN profile is used to apply to a selected access point. It is very convenient for the administrator to configure the setting for access point without opening the web user interface of the access point.

Central Management >> AP >> WLAN Profile



Profile	Name	Main SSID	Security	Multi-SSID	WLAN ACL	Rate Ctrl	Clone	To AP	To Local
1	Default	Urvick LAN A	WPA2/WPA Personal	Enable	None	None	☒	☒	☒
2	---	---	---	---	---	---	☐	☐	☐

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	It can copy settings from an existing WLAN profile to another WLAN profile. First, you have to check the box of the existing profile as the original profile. Second, click Clone. The following dialog will appear.  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. The new profile has been created with the settings coming from the original profile.
To AP	Click it to apply the selected wireless profile to the specified Access Point.

	 Simply choose the device you want from Existing Device field. Click >> to move the device to Selected Device field. Then, click OK. The selected WLAN profile will be applied to the selected access point immediately. Later the access point will reboot.
To Local	WLAN Profile configured in this page is specified for VigorAP connected to Vigor router. 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.

How to edit the wireless LAN profile?

1. Select the WLAN profile (index number 1 to 2) 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 Auto Provision
Administrator	admin
Password	1234
2nd Subnet	☒ Enable ☐ Disable
Management VLAN	☐ Enable Management VLAN: LAN A/VLAN ID 0 (0 ~ 4095) LAN-B/VLAN ID 0 (0 ~ 4095)

WLAN General Setting

	2.4GHz	5GHz	5GHz-2
Wireless LAN	☒ Enable ☐ Disable		
Limit Client	☐ Enable 64 (0 ~ 128, default: 64)		
Operation Mode	AP		
2.4G Mode	Mixed(11b, 11g, 11n)		
2.4G Channel	2402MHz (Channel 11)		
Airtime Fairness	☐ Enable Airtime Fairness Triggering Client Number 2 (2 ~ 128, default: 2)		
Roam Sleeping	☐ Enable Roam Sleeping Check Time for WLAN Client Sleep 15 seconds (1 ~ 60, default: 15)		
Roaming	☐ Minimum Basic Rate 1 Mbps ☒ Disable RSSI Requirement ☐ Strictly Minimum RSSI -75 dbm (-42 %) (default: -70) ☐ Minimum RSSI -60 dbm (-60 %) (default: -60) with Adjacent AP RSSI over 5 dB (default: 5) ☐ Enable Fast Roaming(WPA2002 fix) PMK Cache Period 10 minutes (10 ~ 600, default: 10)		
WMM	☐ Enable ☒ Disable		
Tx Power	100%		
Channel Width	Auto 20/40 MHz		

Note:

1. Administrator can contain only a-z A-Z 0-9 _ - ! @ # % ^ & * () { } [] ~
2. Password can contain only a-z A-Z 0-9 _ - ! @ # % ^ & * () { } [] ~
3. The setting of 5GHz-2 band only takes effect to tri-band models.
4. AP will ignore the change if you apply the unsupported channel due to different countries and models.

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
2.4GHz SSID			
Active	☒ Enable ☐ Disable		
SSID	Drag-Ick LAN A LAN A v ☐ Hide SSID		
WLAN	0 (0 inteq)		
Isolate	☐ From LAN ☐ From Member		
Security Settings			
Encryption	WPA1/WPA2/PSK v		
	Set up <u>802.1X</u> Server if 802.1X is enabled. WPA		
	WPA Algorithms ☐ TKIP ☐ AES ☒ TKIP/AES		
	Pass Phrase *****		
	Key Renewal Interval 3600 Seconds		
WEP	Setup <u>WEP</u> Key if WEP is enabled. 802.1X WEP ☐ Enable ☒ Disable		
	Access Control		
	Mode	Name v	
List	Add Delete Edit Cancel		
	Client's MAC Address: : : : : :		
	Add Delete Edit Cancel		
Bandwidth Limit			
Status	☐ Enable ☒ Disable		Auto Adjustment ☐ Enable ☒ Disable
Upload	0 Kbps	Download	0 Kbps
Station Control			
Status	☐ Enable ☒ Disable		
Connection Time	1 hour v	Reconnection Time	1 hour v
Note: SSID can contain only A-Z, a-z, 0-9, _ , @ & % .			
Back Cancel Next			
Backup ACL Cfg Backup		Upload from File: Select File Upload Restore	

- After finished the above web page configuration, click **Next** to open the following page for 5G wireless security settings.

Central Management >> AP >> WLAN Profile

5G SSID1	5G SSID2	5G SSID3	5G SSID4
5GHz SSID			
Active ☒ Enable ☐ Disable			
SSID Dragon 5G LAN A ☐ Hide SSID			
VLAN 0 (0 ~ 4095)			
Isolate ☐ From LAN ☐ From Member			
Security Settings			
Encryption Disable			
Set up RADIUS Server if RADIUS is enabled. WPA WPA Algorithms ☐ TKIP ☐ AES ☒ TKIP/AES Pass Phrase Max: 64 characters Key Renewal Interval 3600 Seconds WEP Set up WEP Key if WEP is enabled. 802.1X WEP ☐ Enable ☒ Disable			
Access Control			
Mode None			
List Client's MAC Address: : : : : : Add Delete Edit Cancel			
Bandwidth Limit			
Status ☐ Enable ☒ Disable		Auto Adjustment ☐ Enable ☒ Disable	
Upload 0 Kbps		Download 0 Kbps	
Station Control			
Status ☐ Lockable ☒ Usable			
Connection Time 1 hour		Reconnection Time 1 hour	
Note: 1. 5GHz SSID Configuration only work with VigorAP900 v1.1 and newer APM Client 2. SSID can contain only A-Z a-z 0-9 _ . < 64 characters			
Back Cancel Next			
Backup ACL Cfg : Backup Upload From File 選擇檔案 本選擇檔已檔案 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.

VII-5-3 AP Maintenance

Vigor router can execute configuration backup, configuration restoration, firmware upgrade and remote reboot for the APs managed by the router. It is very convenient for the administrator to process maintenance without accessing into the web user interface of the access point.



Info

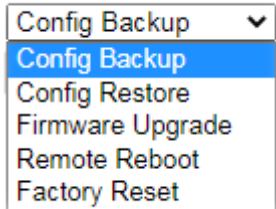
Config Backup can be performed to one AP at one time. Others functions (e.g., Config Restore, Firmware Upgrade, Remote Reboot) can be performed to more than one AP at one time by using Vigor2765.

Central Management >> AP >> AP Maintenance

AP Maintenance

The screenshot shows the 'AP Maintenance' web interface. It includes a 'Select Action' dropdown menu with 'Config Backup' selected. Below this are 'Action Type' and 'File/Path' fields. The 'Select Device' section features two lists: 'Existing Device' and 'Selected Device', with arrows for moving devices between them. At the bottom are 'OK' and 'Cancel' buttons.

Available settings are explained as follows:

Item	Description
Action	There are four actions provided by Vigor router to manage the access points.  Vigor router can backup the configuration of the selected AP, restore the configuration for the selected AP, perform the firmware upgrade of the selected AP, reboot the selected AP remotely and perform the factory reset for the selected AP.
File/Path	Specify the file and the path which will be used to perform Config Restore or Firmware Upgrade .
Select Device	Display all the available access points managed by Vigor router. Simply click << or >> to move the device(s) between Select Device and Selected Device areas.

Selected Device	Display the access points that will be applied by such function after clicking OK.

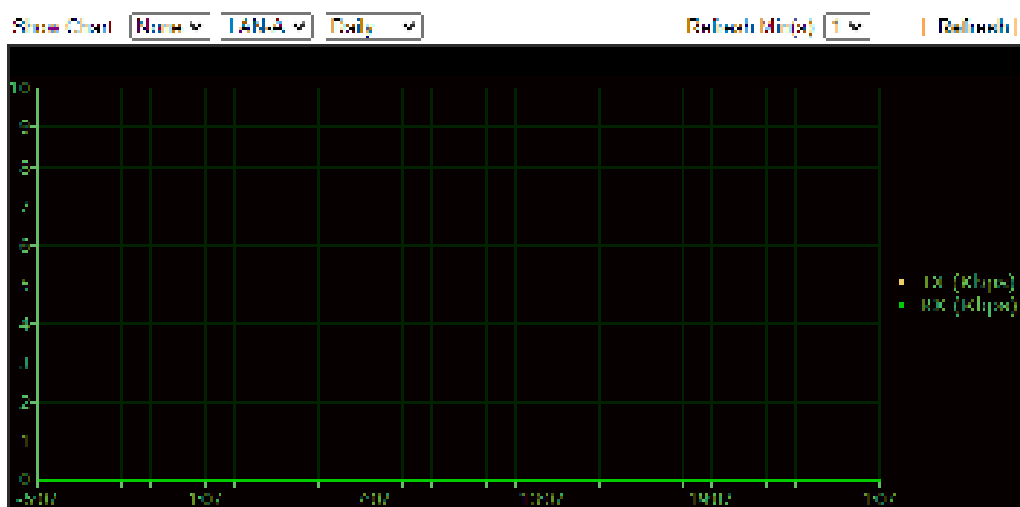
After finishing all the settings here, please click **OK** to perform the action.

VII-5-4 Traffic Graph

Click **Traffic Graph** to open the web page. Choose one of the managed Access Points, LAN-A or LAN-B, daily or weekly for viewing data transmission chart. Click **Refresh** to renew the graph at any time.

Central Management >> AP >> Traffic Graph

Enable



Note:

Enabling/Disabling AP Traffic Graph will also Enable/Disable the External Devices function.

The horizontal axis represents time; the vertical axis represents the transmission rate (in kbps).



Info

Enabling/Disabling such function will also enable/disable the External Devices function.

VII-5-5 Load Balance

The parameters configured for Load Balance can help to distribute the traffic for all of the access points registered to Vigor router. Thus, the bandwidth will not be occupied by certain access points.

Central Management >> AP >> Load Balance

AP Load Balance By Station Number or Traffic

Station Number Threshold

Wireless LAN (2.4GHz) (0-120)

Wireless LAN (5GHz) (0-128)

Wireless LAN (5GHz 2) (0-120)

Traffic Threshold

Upload Limit User defined OK kps (Default unit: K)

Download Limit User defined OK kps (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 (-100)

Choose to Apply

All APs

Note:
The maximum station number of Wireless LAN (2.4GHz) will be applied to both Wireless LAN (2.4GHz) and Wireless LAN (5GHz) if the hardware version of AP900 is less than or equal to 1.1.4.1.

OK Cancel

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. By Station Number - The operation of load balance will be executed based on the station number configured in this page. It is used to limit the allowed number for the station connecting to the access point. The purpose is to prevent lots of stations connecting to access point at the same time and causing traffic unbalanced. Please define the required station number for WLAN (2.4GHz) and WLAN (5GHz) separately. By Traffic - The operation of load balance will be executed according to the traffic configuration in this page. By Station Number or Traffic - The operation of load balance will be executed based on the station number or the traffic configuration.
Station Number Threshold	Set the number of stations as a threshold to activate AP load balance.
Traffic Threshold	Upload Limit - Use the drop down list to specify the traffic limit for uploading. Download Limit - Use the drop down list to specify the traffic

	limit for downloading.
Action When Threshold Exceeded	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. Dissociate existing station by longest idle time - When the access point is overload (e.g., reaching the limit of station number or limit of network traffic), it will terminate the network connection of the client's station which is idle for a longest time. 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.
Choose to Apply	The settings configured for Load Balance can be applied to all of AP devices or selected AP devices.

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

VII-6 Central Management (External Devices)

Vigor router can be used to connect with many types of external devices. In order to control or manage the external devices conveniently, open **External Devices** to make detailed configuration.

Central Management >> External Device

☐ External Device Syslog

☐ External Device Auto Discovery

External Devices Connected

[Refresh](#)

Below shows available devices that connected externally:

For security reason:

If you have changed the administrator password on External Device, please click the Account button to re-type 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.

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 00:00:18
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 re-type new username and password. Otherwise, the router will be unable to monitor the External Device device properly. Click the Clear button to Clear the off-line information and account information.

OK

When you finished the configuration, click **OK** to save it.



Info

Only DrayTek products can be detected by this function.

Part VIII Others



Objects Settings

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



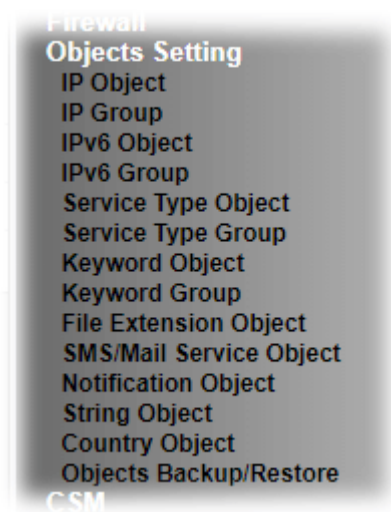
USB

USB device connected on Vigor router can be regarded as a server or WAN interface. By way of Vigor router, clients on LAN can access, write and read data stored in USB storage disk with different applications.

VIII-1 Objects Settings

This section allows the creation of objects and object groups from IP addresses, service types, keywords, file extensions, SMS and email recipients, and notification types. Once set up, these objects can be applied to firewall and content management rules.

Web User Interface



VIII-1-1 IP Object

For IPs in a range and service ports in a limited range usually will be applied in configuring router's settings, therefore we can define them with **objects** and bind them with **groups** for using conveniently. Later, we can select that object/group for applying it. For example, all the IPs in the same department can be defined with an IP object (a range of IP address)

Up to 192 IP Objects can be created.

Objects Setting >> IP Object

Create from ARP Table

Create from Hostmap Table

IP Object Profiles:

[Set to Factory Default](#)

View: All

Search

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.		

1-12 13-24 25-36 37-48 49-60 61-72

Next

Objects Backup/Restore

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 profile settings.
Search	Enter a string of the IP object that you wan to search.
Index	Profile number of the IP object.
Name	Name of the object.
Address	Displays the IP address configured for the object profile.
Objects Backup/Restore	Click it to backup or restore the IP object.

To set up a profile, click the profile number under Index column to bring up the configuration page.

Objects Setting >> IP Object

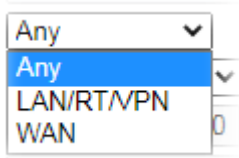
Profile Index : 1

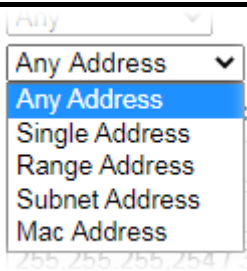
Name:	HR Department
Interface:	Any
Address Type:	Any Address
Mac Address:	00 : 00 : 00 : 00 : 00 : 00
Start IP Address:	0.0.0.0
End IP Address:	0.0.0.0
Subnet Mask:	255.255.255.254 / 31
Invert Selection:	☐

Next >>>

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Name	Name that identifies this profile. Maximum length is 15 characters.
Interface	The network interface on which the IP address or addresses are to be found.  Any - All network interfaces. LAN/ RT/VPN - All network interfaces except WAN. WAN - Only WAN interfaces.
Address Type	Type of Addresses.

	 Any Address – Object covers all IP addresses. Single Address – Object covers one IP address. Range Address – Object covers a range of IP addresses. Subnet Address – Object covers a range of IP addresses specified in subnet notation. Mac Address – Object contains a MAC address.
MAC Address	Enter MAC address of the network device, if Address Type is Mac Address.
Start IP Address	Enter beginning IP address, if Address Type is one of Single Address, Range Address and Subnet Address.
End IP Address	Enter ending IP address, if Address type is one of Single Address, Range Address and Subnet Address.
Subnet Mask	Enter subnet mask, if Address type is Subnet Mask.
Invert Selection	If selected, all addresses except the ones entered above will be used.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current IP object, click **Clear**.

Object Settings >> IP Object

[Create from ARP Table](#)

[Create from Routing Table](#)

IP Object Profiles:

View: All ▼

Index	Name	Address	Index	Name
1.	RD Department	Any	17.	
2.	Financial Dept	192.168.1.9	18.	
3.	HR Department	192.168.10.10 - 192.168.10.100	19.	
4.			20.	

VIII-1-2 IP Group

Multiple IP Objects can be placed into an IP Group.

Objects Setting => IP Group

IP Group Table:

[Set to Factory Default](#)

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

Objects Backup/Restore

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Index	Index number of the profile.
Name	Name that identifies the profile.
Objects Backup/Restore	Click it to backup or restore the IP group object.

To set up a profile, click its index to bring up the configuration page.

Objects Setting => IP Group

Profile Index : 1

Name:	Administration
Interface:	Any
Available IP Objects	Selected IP Objects (Up to 12)
3-ITR Department	1-HQ Department
	2-Financial Dept
	Add
	Remove

Available settings are explained as follows:

Item	Description
Name	Name that identifies this profile. Maximum length is 15 characters.
Interface	Select WAN, LAN or Any to filter IP objects.
Available IP Objects	All available IP objects that are associated with the selected interface.
Selected IP Objects	IP objects that have been added to this profile.

To add an IP object to the IP Group, select it under Available IP Objects, then click the >> button. To remove an IP object from the IP Group, select it under Selected IP Objects, then click the << button.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current IP group, click **Clear**.

VIII-1-3 IPv6 Object

Up to 64 IPv6 Objects can be created.

[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 / 1-64

Next

Objects Backup/Restore

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Index	Index number of the profile.
Name	Name that identifies the profile.
Objects Backup/Restore	Click it to backup or restore the IPv6 object.

To set up a profile, click the profile number under Index column to bring up the configuration page.

Object Settings IPv6 Object

Profile Index : 1

Name	2F_CHECK
Address Type	Subnet Address
Mac Address	00 : 00 : 00 : 00 : 00 : 00
Start IP Address:	1102:1 Select
End IP Address:	Select
Prefix Length:	
Invert Selection:	

Next >>

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Name	Name that identifies this profile. Maximum length is 15 characters.
Address Type	Type of Addresses. Any Address - Object covers all IPv6 addresses. Single Address - Object covers one IPv6 address. Range Address - Object covers a range of IPv6 addresses. Subnet Address - Object covers a range of IPv6 addresses specified in subnet notation. Mac Address - Object contains a MAC address.
Mac Address	Enter MAC address of the network device, if Address Type is Mac Address.
Start IP Address	Enter beginning IP address, if Address Type is one of Single Address, Range Address and Subnet Address.
End IP Address	Enter ending IP address, if Address type is one of Single Address, Range Address and Subnet Address.
Prefix Length	Enter IPv6 prefix length, if Address type is Subnet Address.
Invert Selection	If selected, all addresses except the ones entered above will be used.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the IPv6 object, click **Clear**.

VIII-1-4 IPv6 Group

Multiple **IPv6 Objects** can be placed into an **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.	

Objects Backup/Restore

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Index	Index number of the profile.
Name	Name that identifies the profile.
Objects Backup/Restore	Click it to backup or restore the IPv6 object.

To set up a profile, click the profile number under Index column to bring up the configuration page.

Objects Setting => IPv6 Group

Profile Index: 1

Name: _____	
Available IPv6 Objects	Selected IPv6 Objects (Up to 8)
OK Clear Cancel	

Available settings are explained as follows:

Item	Description
Name	Name that identifies this profile. Maximum length is 15 characters.
Available IPv6 Objects	All available IP objects that are associated with the selected interface.
Selected IPv6 Objects	IPv6 objects that have been added to this profile.

To add an IPv6 object to the IPv6 Group, select it under Available IPv6 Objects, then click the >> button. To remove an IPv6 object from the IPv6 Group, select it under Selected IPv6 Objects, then click the << button.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current IPv6 group, click **Clear**.

VIII-1-5 Service Type Object

Up to 96 Service Type Objects can be created.

[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 >>

[Objects Backup/Restore](#)

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Index	Index number of the profile.
Name	Name that identifies the profile.
Objects Backup/Restore	Click it to backup or restore the service type object.

To set up a profile, click the profile number under Index column to bring up the configuration page.

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

Profile Index : 1

Name

Protocol

Source Port

Destination Port

Any

1

1

1

65535

65535

65535

Next >>

OK

Clear

Cancel

Available settings are explained as follows:

Item	Description

Name	Name that identifies this profile. Maximum length is 15 characters.
Protocol	Protocol(s) to which this profile applies. Any - All protocols. ICMP - Internet Control Message Protocol IGMP - Internet Group Management Protocol TCP - Transmission Control Protocol UDP - User Datagram Protocol TCP/UDP - Transmission Control Protocol and User Datagram Protocol Other - Other protocols not listed above. Enter protocol number in the textbox.
Source/Destination Port	When protocol selected includes TCP or UDP, the source and destination ports can be specified. = - any port that falls within the specified range. != - any port that falls outside of the specified range. - all port numbers that are greater than the specified value. < - all port numbers that are smaller than the specified value.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current service type object, click **Clear**.

Objects Setting >> Service Type Object

Service Type Object Profiles:

Index	Name	
<u>1.</u>	www	
<u>2.</u>		
<u>3.</u>		
<u>4.</u>		

VIII-1-6 Service Type Group

Multiple **Service Type Objects** can be placed into a **Service Type Group**.

Objects **Setting** **>** **Service Type Group**

Service Type Group Table: | **Set to Factory Default** |

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

Objects **Backup/Restore**

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Index	Index number of the profile.
Name	Name that identifies the profile.
Objects Backup/ Restore	Click it to backup or restore the service type group object.

To set up a profile, click the profile number under Index column to bring up the configuration page.

Objects Setting >> Service Type Group Setup

Profile Index : 1

Name	
Available Service Type Objects 1 www	Selected Service Type Objects (Up to 5)
>> <<	
OK Clear Cancel	

Available settings are explained as follows:

Item	Description
Name	Name that identifies this profile. Maximum length is 15 characters.
Available Service Type Objects	All available service type objects.
Selected Service Type Objects	Service type objects that have been added to this profile.

To add a Service Type Object to the Service Type Group, select it under **Available Service Type Objects**, then click the >> button. To remove a Service Type Object to the Service Type Group, select it under **Selected Service Type Objects**, then click the << button.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current service type group, click **Clear**.

VIII-1-7 Keyword Object

200 Keyword Object Profiles can be created for use as blacklists or white lists in **CSM >>URL Content Filter Profile** and **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](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [13](#) [14](#) [15](#) [16](#) [17](#) [18](#) [19](#) [20](#) [21](#) [22](#) [23](#) [24](#) [25](#) [26](#) [27](#) [28](#) [29](#) [30](#) [31](#) [32](#) [Next](#)

[Objects Backup/Restore](#)

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Index	Index number of the profile.
Name	Name that identifies the profile.
Objects Backup/Restore	Click it to backup or restore the keyword object.

To set up a profile, click its index to bring up the configuration page.

Object Setup ► Keyword Object Setup

Profile Index : 1

Name	
Contents	 Limit of Contents: Max 3 Words and 63 Characters. Each word should be separated by a single space. You can replace a character with %00 %. Example: Contents: backdoor%02 virus keep%02out Results: 1. backdoor 2. virus 3. keep out

Next >>

Available settings are explained as follows:

Item	Description
Name	Name that identifies this profile. Maximum length is 15 characters.
Contents	Keywords to be matched. Enter the content for this 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. In addition, up to 3 key phrases, separated by spaces, for a total length of 63 characters can be entered. For key phrases that contain spaces, replace spaces with the sequence %20. For example, the phrase “keep out” is to be entered as “keep%20out”.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current keyword object, click **Clear**.

VIII-1-8 Keyword Group

Multiple Keyword Objects can be placed into a Keyword Group.

Keyword groups can be chosen as blacklists or white lists in **CSM >>URL / Web Content Filter Profile**.

Objects Setting => Keyword Group

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

Index	Name	Objects	Index	Name	Objects
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.		

[Objects Backup/Restore](#)

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Index	Index number of the profile.
Name	Name that identifies the profile.
Objects	Displays the keyword objects under this group.
Objects Backup/ Restore	Click it to backup or restore the keyword group object.

To set up a profile, click its index to bring up the configuration page.

Objects Setting => Keyword Group Setup

Profile Index : 1

Name:	
Available Keyword Objects	Selected Keyword Objects (Up to 16)
OK Clear Cancel	

Available settings are explained as follows:

Item	Description
Name	Name that identifies this profile. Maximum length is 15 characters.
Available Keyword Objects	All keyword objects that have not been added to this profile.
Selected Keyword Objects	Keyword objects that have been added to this profile.

To add a Service Type Object to the Service Type Group, select it under **Available Service Type Objects**, then click the >> button. To remove a Service Type Object to the Service Type Group, select it under **Selected Service Type Objects**, then click the << button.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current keyword group, click **Clear**.

VIII-1-9 File Extension Object

Up to 8 File Extension Objects can be set up for use with **CSM>>URL Content Filter**.

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

File Extension Object Profiles				Set to Factory Default	
Profile	Name	Profile	Name		
1		1			
2		2			
3		3			
4		4			

[Objects Backup/Restore](#)

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Index	Index number of the profile.
Name	Name that identifies the profile.
Objects Backup/Restore	Click it to backup or restore the file extension object.

To set up a profile, click its index to bring up the configuration page.

Objects Setting >> File Extension Object Setup

Profile Index: 1 Profile Name: | |

Categories	File Extensions
Image Select All Clear All	☐ .bmp ☐ .dib ☐ .gif ☐ .jpg ☐ .jpe ☐ .jpg2 ☐ .jpe2 ☐ .pct ☐ .pex ☐ .pic ☐ .pict ☐ .png ☐ .tif ☐ .tiff ☐ .ico
Video Select All Clear All	☐ .ast ☐ .avi ☐ .mov ☐ .mpe ☐ .mpeg ☐ .mpg ☐ .mp4 ☐ .ep ☐ .mm ☐ .wmv ☐ .3gp ☐ .3gpp ☐ .3gpp2 ☐ .3g2 ☐ .div ☐ .set
Audio Select All Clear All	☐ .aac ☐ .aiff ☐ .au ☐ .mp3 ☐ .m4a ☐ .m4p ☐ .ogg ☐ .ra ☐ .ram ☐ .wav ☐ .wma ☐ .wma2
Java Select All	☐ .class ☐ .jail ☐ .jar ☐ .jav ☐ .java ☐ .jam ☐ .js

Available settings are explained as follows:

Item	Description
Profile Name	Name that identifies this profile. Maximum length is 7 characters.
Select All	Selects all file extensions for the category.
Clear All	Deselects all file extensions for the category.

Select the file extensions you wish to be included in the profile. To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current file extension object, click **Clear**.

VIII-1-10 SMS/Mail Service Object

SMS Service Object

Up to 10 SMS Service Objects can be set up for use with **Application>>SMS Alert Service**.

[Objects Setting >> SMS / Mail Service Object](#)

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

[Objects Backup/Restore](#)

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Index	Index number of the profile.
Profile	Name that identifies the profile.
SMS Provider	The SMS provider selected for the profile.
Objects Backup/ Restore	Click it to backup or restore the SMS service object.

To set up a profile, click the **SMS Provider** tab, and then click its index to bring up the configuration page.

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

SMS Provider		Mail Server
Index	Profile Name	
1.		
2.		
3.		
4.		

Profile Index: 1

Profile Name	
Service Provider	katxmx.com.tw (TW) ✓
Connection Protocol	☒ HTTP ☐ HTTPS
Username	Max: 31 characters
Password	Max: 31 characters
Quota	10
Sending Interval	3 (seconds)

Note:

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

Available settings are explained as follows:

Item	Description
Profile Name	Name that identifies this profile. Maximum length is 31 characters.
Service Provider	Select a Service Provider from the dropdown list.
Connection Protocol	Specify HTTP or HTTPS.
Username	Username used to log in to the service. Maximum length is 31 characters.
Password	Password used to log in to the service. Maximum length is 31 characters.
Quota	Remaining number of text messages allowed to be sent. The quota value reduces by 1 every time the router sends an SMS message. When the quota reaches 0, no SMS will be sent until it is reset to greater than 0.
Sending Interval	Minimum amount of time, in seconds, to wait between sending SMS messages.
Send a Test Message	Click it to send a test e-mail according to above configuration.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the SMS service object, click **Clear**.

Objects Setting => SMS / Mail Service Object

SMS Provider	Mail Server	[Set to Factory Default]	
Index	Profile Name	SMS Provider	
1.	Line_down	katxmx.com.tw (TW)	
2.			
3.			
4.			
5.			

Customized SMS Service

The router offers an extensive list of preset SMS service providers for your convenience. However, if your service provider is not among the list of supported service providers, simply use Indexes 9 and 10 to create a customized SMS service profile.

Object Setting - SMS / Mail Service Object

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

Objects Backup/Restore

To set up a customized profile, click the SMS Provider tab, and then click one of the 2 indexes (9 and 10) to bring up the configuration page.

Objects Setting => SMS / Mail Service Object

Profile Index: 9	
Profile Name	Custom 1
Service Provider	Max: 255 characters
Please contact with your SMS provide to get the exact URL String eg: bulk sms center net 5567/exp?auth=msisdn&end_sms=212 02&username=444&id=444 &password=123456789&id=123456789&id=123456789&id=123456789&id=123456789&id=123456789	
Server Response	Max: 32 characters
Username	Max: 31 characters
Password	Max: 31 characters
Queue	10
Sending Interval	3 (seconds)

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.

Page 10/10

[Send a Test Message](#)

Available settings are explained as follows:

Item	Description
Profile Name	Display-only profile name, which is Custom 1 for Index 9 and Custom 2 for Index 10.
Service Provider	Enter an identifier for the service provider. Maximum length is 23 characters.

Entry box	Enter the URL for the SMS service. Maximum length is 255 characters. Contact the service provider for the appropriate URL to use.
Server Response	Enter the API text defined by the SMS provider. It allows Vigor router to acknowledge that the SMS server has received the request coming from the SMS server.
Username	Username used to log in to the service. Maximum length is 31 characters.
Password	Password used to log in to the service. Maximum length is 31 characters.
Quota	Remaining number of text messages allowed to be sent. The quota value reduces by 1 every time the router sends an SMS message. When the quota reaches 0, no SMS will be sent until it is reset to greater than 0.
Sending Interval	Minimum amount of time, in seconds, to wait between sending SMS messages.
Send a Test Message	Click it to send a test e-mail according to above configuration.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the SMS service object, click **Clear**.

Mail Service Object

Up to 10 **Mail Service Objects** can be set up for use with **Application>>SMS/Mail Alert Service**.

[Objects Setting => SMS / Mail Service Object](#)

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

[Objects Backup/Restore](#)

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profile settings.
Index	Index number of the profile.
Profile	Name that identifies the profile.
Objects Backup/Restore	Click it to backup or restore the mail service object.

To set up a profile, click the Mail Server tab, and then click its index to bring up the configuration page.

Objects Setting >> SMS / Mail Service Object

Profile Index: 1

Profile Name	Mail_Notify
SMTP Server	192.168.1.90
SMTP Port	25
Sender Address	camo_@draytek.com
☐ Use SSL	
☒ Authentication	
Username	john
Password	*****
Sending Interval	0 (seconds)

Note:

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

OK Clear Cancel Send a Test E-mail

Available settings are explained as follows:

Item	Description
Profile Name	Name that identifies this profile. Maximum length is 31 characters.
SMTP Server	IP address of the SMTP server.
SMTP Port	Port number of the SMTP server.
Sender Address	E-mail address of the sender.
Use SSL	Check this box to use SMTPS (SMTP over SSL) to communicate with the SMTP server. Note that the de facto port used for SMTPS is 465.
Authentication	Select to send username and password to SMTP server for authentication. Username - Username for authentication. Maximum length is 31 characters. Password - Password for authentication. Maximum length is 31 characters.
Sending Interval	Minimum amount of time, in seconds, to wait between sending e-mail messages.
Send a Test E-mail	Click it to send a test e-mail according to above configuration.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the mail service object, click **Clear**.

VIII-1-11 Notification Object

Up to 8 Notification Objects can be set up for use in **Application>>SMS Alert Service** and **Application>>Mail Alert Service**.

[Objects Setting](#) => [Notification Object](#)

[Set to Factory Default](#)

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

[Objects Backup/Restore](#)

To set up a profile, click its index to bring up the configuration page.

[Objects Setting](#) => [Notification Object](#)

Profile Index: 1

Profile Name		
Category	Status	
WAN	☐ Disconnected	☐ Reconnected
VPN Tunnel	☐ Disconnected	☐ Reconnected
Temperature Alert	☐ USB Out of Range	
WAN Budget	☐ Limit Reached	
Security	☐ Web Login	
	☐ Telnet Login	
	☐ SSH Login	
	☐ TRUSS Login	
	☐ FTP User Login	
	☐ Config Changed (from WebUI and CLI)	

Available settings are explained as follows:

Item	Description
Profile Name	Name that identifies this profile. Maximum length is 31 characters.
Category	Areas to be monitored.
Status	Select the states to be monitored. For example, the check box of Disconnected under the category of WAN is checked. Once the profile is enabled, the Vigor router system will send out a notification to the recipient via SMS when the WAN connection is down.

To save changes on the page, click OK. To discard changes, click Cancel. To blank out all settings in the notification object, click Clear.

VIII-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	
1	testtest_087	☐

Add

Available settings are explained as follows:

Item	Description
Index	Click it to open the following page for modifying an existed string object. String (Max.255 chars.) OKClearCancel
String	Display the name of a string profile.
Clear	Choose the string that you want to remove. Then check the box and click Clear to delete the selected string profile.
Add	Click it to create a new string object profile.

Below shows an example to apply string object (in Route Policy):

Routing >> Route Policy

Index: 1

☒ Enable

Comment

Details

Criteria

Protocol

Any

Source

Any

Destination

Domain Name

SelectDelete

Destination Port

Send via If Criteria Matched

Interface

Gateway

Packet Forwarding to WAN/LAN via

String Object - Google Chrome

192.168.1.1/doc/strobjsl.htm

Objects Setting >> String Object

Index	String
1	testtest_087

OKCancel

VIII-1-13 Country Object

The country object profile can determine which country/countries shall be blocked by the Vigor router's Firewall.

[Object 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	

[Objects Backup/Restore](#)

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).

[Routing >> Route Policy](#)

Index: 1

☒ Enable

Comment: [Delete](#)

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	Telecom
Available Country 1-Afghanistan 2-Aland Islands 3-Albania 4-Algeria 5-American Samoa 6-Andorra 7-Angola 8-Anguilla 9-Antarctica	Selected Country (Up to 16) 222 Taiwan

Next >>

Note:

The maximum number of Selected Country is 16

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Name	Enter a name for such profile. The maximum length of the name you can set is 15 characters.
Available Country / Selected Country	Select any country from Available Country. Click >> to move the selected country and place on Selected Country. 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
1.	Index1	17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	

VIII-1-14 Objects Backup/Restore

The objects settings can be backup as a file. The backup file can be imported to the device to restore the configuration in the future if required.

Backup

☐ Select All
☐ IP Object
☐ IP Group
☐ IPv6 Object
☐ IPv6 Group
☐ Service Type Object
☐ Service Type Group
☐ Keyword Object
☐ Keyword Group
☐ File Extension Object
☐ SMS/MMS Service Object
☐ Notification Object
☐ Ring Object
☐ Country Object
☒ Backup the current IP Objects with a CSV file
☐ Download the default CSV template to edit

Restore

上傳檔案到系統

Notice:

For better compatibility, it's suggested to edit IP Objects with the provided default CSV template.

Available settings are explained as follows:

Item	Description
Backup	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. 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. Select All - Check the box to select all of the items listed below. 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. 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. Download - Download the CSV file from Vigor router and store in your hard disk.
Restore IP Object	Select – Click it to specify a predefined CSV file. Restore – Import the selected CSV file onto Vigor router.

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 Setting >> SMS / Mail Service Object

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

[Objects Backup/Restore](#)

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 Setting >> SMS / Mail Service Object

Profile Index: 1

Profile Name	Test number	
Service Provider	kddnet.com.tw (TW)	
Connection Protocol	☒ HTTP ☐ HTTPS	
Username	abc0020	
Password	*****	
Quota	10	
Sending Interval	3	(=minutes)

Note:

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

- After finished the settings, click **OK** to return to previous page. Now you have finished the configuration of the SMS Provider profile setting.

Objects Setting >> SMS / Mail Service Object

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

Objects Backup/Restore

- Open **Object Settings>>Notification Object** to configure the event conditions of the notification.

Objects Setting >> Notification Object

Set to Factory Default		
Index	Profile Name	Settings
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		

Objects Backup/Restore

- 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

Category	Status
WAN	☐ Disconnected ☐ Reconnected
VPN Tunnel	☐ Disconnected ☐ Reconnected
Temperature Alert	☐ Out of Range
WAN Budget	☐ Limit Reached
Security	☐ Web Log in ☐ Telnet Log-In ☐ SSH Log in ☐ TR069 Log-In ☐ FTP User Log in ☐ Config Changed(From WebUI and CLI)

OK Clear Cancel

- After finished the settings, click **OK** to return to previous page. You have finished the configuration of the notification object profile setting.

Object Setting => Notification Object

| Set to Factory Default |

Index	Profile Name	Settings
1	WAN Notify	WAN
2		
3		
4		
5		
6		
7		
8		

Object Backup/Restore

- 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	Enable	SMS Provider	Recipient Number	Notify Profile	Schedule(1-12)
1	☒	1 Local number	09 02223456	1 WAN Notify	None
2	☐	1 Local number		1 WAN Notify	None
3	☐	1 Local number		1 WAN Notify	None
4	☐	1 Local number		1 WAN Notify	None
5	☐	1 Local number		1 WAN Notify	None
6	☐	1 Local number		1 WAN Notify	None
7	☐	1 Local number		1 WAN Notify	None
8	☐	1 Local number		1 WAN Notify	None
9	☐	1 Local number		1 WAN Notify	None
10	☐	1 Local number		1 WAN Notify	None

Note:

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

OK

Cancel

- Click **OK** to save the settings. Later, if one of the WAN connections fails in your router, the system will send out SMS to the phone number specified. If the router has only one WAN interface, the system will send out SMS to the phone number while reconnecting the WAN interface successfully.

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	Custom 1
Service Provider	clicktel
Please contact with your SMS provide to get the exact URL string eg: bulk sms.com.cn:8555/soap/submit/sms/send_sms/2/2.0?username=***&password=***&srcid=***&to=***&msgid=***&dest=***&message=***&msg=***	
Server Response	Max 32 characters
Username	tan123
Password	*****
Quota	10
Sending Interval	3 (seconds)

Note:

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

OK Clear Cancel

VIII-2 USB Application

USB devices connected to the Vigor router can function as storage servers, WAN interfaces, network printers or thermometers.

After setting the configuration in USB Application, a USB storage device can be accessed using either the FTP or SMB protocol from LAN clients with the IP address of the Vigor router and the username and password entered in **USB Application>>USB User Management**.

	
Info	USB modems that are supported by the router are listed in 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



VIII-2-1 USB General Settings

This page allows you to configure the file sharing feature of the Vigor router, where USB mass storage devices such as thumb drives and hard drives can be made accessible to LAN clients. Currently, only FAT16 and FAT32 file systems are supported by the Vigor router, so verify that the USB drive contains these file systems. FAT32 is recommended because of its long filename support, which FAT16 lacks.

[USB Application](#) >> [USB General Settings](#)

USB General Settings

General Settings	
Simultaneous FTP Connections	5 (Maximum 6)
Default Charset	English v
SMB File Sharing Service (Network Neighborhood)	
☐ Enable ☒ Disable	
Access Mode	
☒ LAN Only ☐ LAN And WAN	
NetBios Name Service	
Workgroup Name	WORKGROUP
Host Name	Vigor
Printer Server	
☐ Enable ☒ Disable	

Note:

1. If character set is set to "English", only English long filename is supported.
2. Multi-session FTP download will be banned by Router FTP server. If your FTP client has a multi-connection mechanism, such as FileZilla, you should limit client connections to 1 to improve performance.
3. A workgroup name must be different from the host name. The workgroup name can have up to 15 characters and the host name can have up to 15 characters. Names cannot contain any of the following: \, /, <, >, |, \, /, <, >, |, \, /, <, >, |.

OK

Available settings are explained as follows:

Item	Description
General Settings	Simultaneous FTP Connections - Enter the maximum number of simultaneous FTP sessions allowed. The router allows up to 6 simultaneous sessions. Default Charset - Select the character set for file and directory names. Currently, the Vigor router supports four

	character sets. The default charset is English.
SMB File Sharing Service	Click Enable to enable SMB service (file sharing).
Access Mode	LAN Only - Only users on the LAN can connect access the shared USB disk. LAN And WAN - Both LAN and WAN users can access SMB server of the router.
NetBios Name Service	For SMB file sharing service, you need to specify a workgroup name and a host name. The two names cannot be identical, and neither can contain any of the following characters: ; : " < > * + = \ ? Workgroup Name –Enter the workgroup name. Maximum allowed length is 15 characters. Host Name –Enter the NetBIOS hostname for the router. Maximum allowed length is 23 characters.
Printer Server	Enable - Select to allow the Vigor router to act as a print server for printers connected the USB.

Select **OK** to save changes on the page.

VIII-2-2 USB User Management

This page allows you to set up profiles for FTP/SMB users. Any user who wants to access the USB storage disk must authenticate using a username and password that have been configured on this page. Please connect a USB storage device before adding or modifying settings on this page, or else an error message will appear requesting you to do so before allowing you to proceed.

USB Application >> USB User Management

USB User Management
[Set to Factory Default](#)

Index	Enable	Username	Home Folder	File Access Rule	Directory Access Rule
1	☐				
2	☐				
3	☐				
4	☐				
5	☐				
6	☐				
7	☐				
8	☐				
9	☐				
10	☐				
11	☐				
12	☐				
13	☐				
14	☐				
15	☐				

Click index number to access into configuration page.

Profile Index: 1

☐ Enable	
Username	Max: 11 characters
Password	Max: 11 characters
Confirm Password	
Home Folder	
Access Rule	
File	☐ Read ☐ Write ☐ Delete
Directory	☐ List ☐ Create ☐ Remove

Note:

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

Available settings are explained as follows:

Item	Description
Enable	Check to activate this profile (account) for FTP service and / or SMB service. Later, the user can use the username specified in this page to login into FTP server.
Username	Enter the username for this user profile. Maximum allowed length of the username is 11 characters. Note: Anonymous user access is not supported. Note: “Admin” cannot be used as a username, as it is reserved for access to web pages on the Vigor router, and for FTP firmware upgrade. Note: Ensure that the FTP client does not use passive FTP mode as it is not supported by the Vigor router.
Password	Enter the password for this user profile. Maximum allowed length of the password is 11 characters.
Confirm Password	Enter the password again to confirm.
Home Folder	Enter the folder which will be the root folder for FTP and SMB sessions established using the credentials of this user profile. Only folders and files inside this selected root folder are accessible to the user. In addition, if the user types “/” here, the user can access into all of the disk folders and files in USB storage disk. To browse the list of folders available for selection, or to create a new folder, click the  icon.

	 Note: If the USB storage device is write-protected, new folders cannot be created. Only existing folders can be selected. Note: Only folders directly under the root can be selected as the home folder.
Access Rule	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. File - Check the items (Read, Write and Delete) for such profile. Directory -Check the items (List, Create and Remove) for such profile.

To save changes on this page, ensure that a USB storage device is connected, and click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current IP object, click **Clear**.

VIII-2-3 File Explorer

File Explorer offers an easy way for users to view and manage the content of USB storage disk connected on Vigor router.

USB Application >> File Explorer

USB Disk Connection Status: **Not Connected**

Refresh

Note:

1. File Explorer cannot be used, if USB disk is disconnected.
2. The folder cannot be deleted when it is not empty.

After inserting a USB, the following page will be shown on the screen.

USB Application >> File Explorer

USB Disk Connection Status: **Connected**

Refresh

File Explorer

 Current Path: /

Name	Size	Delete	Rename
??2014_2016			
System Volume Information			
C?2014_2016			
??2016			
C?2016			
USB DISK	1 KB		

 Upload File

Select a file:

Note:

1. File Explorer cannot be used, if USB disk is disconnected.
2. The folder cannot be deleted when it is not empty.

Available settings are explained as follows:

Item	Description
 Refresh	Click this icon to refresh the list of files and folders.
 Back	Click this icon to return to the parent folder.
 Create	Click this icon to add a new folder.
Current Path	Shows current folder.
Upload	To upload a file to the USB storage device, click the Browse... button to bring up the file selection dialog box. Select the file you wish to upload, and click the Upload button to initiate the upload process.

VIII-2-4 USB Device Status

This page allows monitoring of the status of USB devices (disk, modem, printer, and sensor) connected to the Vigor router. To maintain the data integrity of a USB disk that is connected to the router, always click **Disconnect USB Disk** before unplugging the disk from the router.

USB Application > USB Device Status

Disk	Modem	Printer	Sensor	Refresh

USB Mass Storage Device Status

Connection Status: **No Disk Connected** Disconnect USB Disk

Disk Capacity: 1 MB

Free Capacity: 1 MB Refresh

USB Disk Users Connected

Index	Service	IP Address(Port)	Username

Available settings are explained as follows:

Item	Description
Connection Status	Shows whether a USB disk is connected or not. If there is no USB device connected to the Vigor router, “No Disk Connected” will be displayed.
Disk Capacity	Shows the total capacity of the USB storage disk.
Free Capacity	Shows the free space on the USB storage disk. Click Refresh at any time to get the most up-to-date free capacity.
USB Disk Users Connected	Shows the clients that are connected to the SMB/FTP server. Index - The profile index used by the LAN client to establish the connection. Service - Shows whether the connection is using FTP or SMB. IP Address - Shows the client’s IP address. Username - Shows the username used to establish the connection.
Disconnect USB Disk	Before unplugging the USB storage device from the router, make sure you click this first to ensure that all data has been written to the disk and all open files are closed.

After a USB storage device has been connected, the **Connection Status** will be updated within a few seconds.

USD Application => Temperature Sensor Setting

Temperature Chart	Temperature Sensor Settings
Display Settings	
Temperature Calibration	0.00
Temperature Unit	☒ Celsius ☐ Fahrenheit
Alarm Settings	
☐ Enable Syslog Alarm	
Upper temperature limit	30.00
Lower temperature limit	10.00

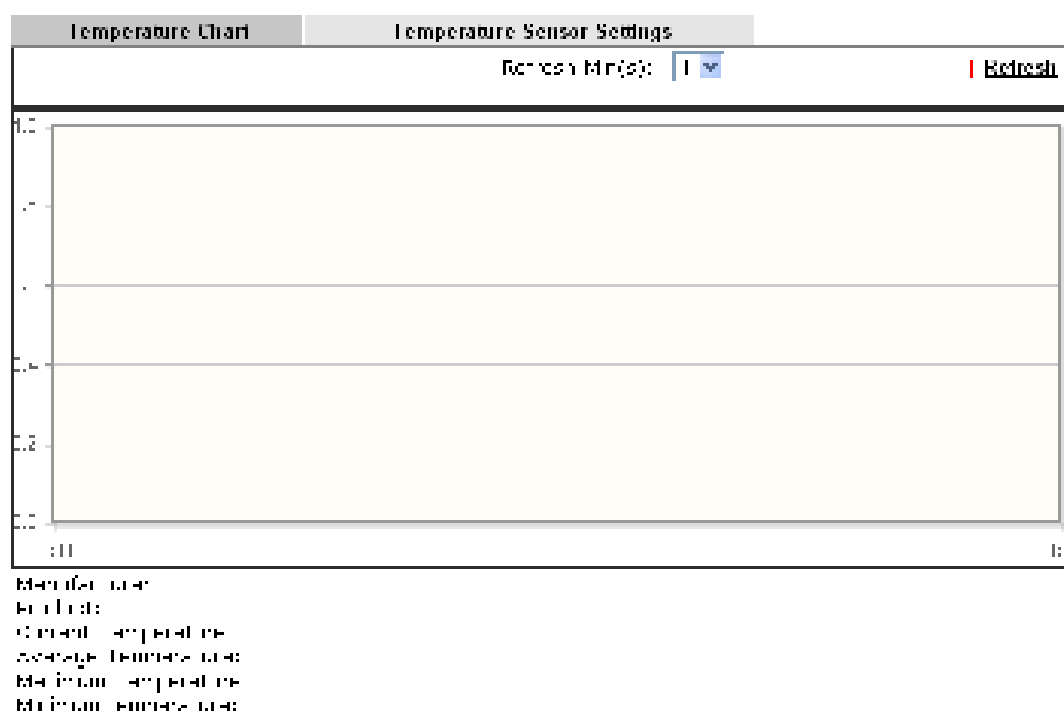
Note:
Set 1) Notification Object, 2) SMS / Mail Service Object, 3) SMS / Mail Alert Service to make Vigor router send alert when the temperature reaches the limit.

Available settings are explained as follows:

Item	Description
Display Settings	Temperature Calibration - Enter the difference between the actual temperature and the temperature as reported by the thermometer. Temperature Unit - Select the temperature scale to be used.
Alarm Settings	Enable Syslog Alarm - Select to enable recording of the temperature in Syslog. Upper temperature limit/Lower temperature limit - Enter the upper and lower temperature limits. If the temperature falls outside of this range, an alert will be sent.

Temperature Chart

Below shows an example of temperature graph:



VIII-2-6 Modem Support List

This page lists the brands and models of USB modems that are supported by the Vigor router. This list is subject to change between different versions of firmware as support for new modems are added.

USB Application >> Modem Support List

The following compatibility test lists 3G/4G/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@shytek.com or consult your dealer for further information.

Brand	Model	LTE	Access Mode	Status
4G system	XEPlug P3		PPP	Y
ASUS	ASUS T500		PPP	Y
Aiko	Aiko 70E		PPP	Y
	Aiko 83D		PPP	Y
Alcatel	Alcatel L100V		DHCP	Y
	Alcatel L100V		PPP	Y
	Alcatel L800		DHCP	Y
	Alcatel W100		DHCP	Y
	Alcatel W100		PPP	Y
	Alcatel W800		DHCP	N
	Alcatel X080S		PPP	Y
	Alcatel X030		PPP	Y

VIII-2-7 SMB Client Support List

This page shows a list of SMB clients on various platforms, and their levels of compatibility with the Vigor router as determined by our in-house testing. This list is subject to change as support for SMB clients are added or improved.

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	+
Microsoft® Windows® Vista™	Built-in	++
Microsoft® Windows® 7	built-in	-
Microsoft® Windows® 8	built-in	+
Microsoft® Windows® 10	built-in	-
Mac OS® 10.6.5	built-in	-
Mac OS® 10.11.1	built-in	-
Ubuntu 14.04	built-in	-
Android™	Android™	-
Android™	ES File Explorer™	++
Android™	FileExpert	-
Android™	File Manager	++
Android™	Swift™ Files	-

Application Notes

A-1 How can I get the files from USB storage device connecting to Vigor router?

Files on USB storage device can be reviewed by opening **USB Application>>File Explorer**. If it is necessary for you to delete, copy files on the device or write, paste files to the device, it must be done through SMB server or FTP server.

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

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

USB Application >> USB Disk Status

USB Mass Storage Device Status

Connection Status: **Disk Connected**

Disconnect USB Disk

Write Protect Status: No

Disk Capacity: 5000 MB

USB Disk Users Connected

Refresh

Index	Service	IP Address(Port)	Username

Note: If the write protect switch of this disk is turned on, the 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: 5 (Maximum 5)

Default Charset: English

SMB File Sharing Service (Network Neighborhood)

☒ Enable ☐ Disable

Access Mode

☒ LAN Only ☐ LAN And WAN

NetBIOS Name Service

Workgroup Name: WORKGROUP

Host Name: Vigor

Printer Server

☐ Enable ☒ Disable

Note:

1. If character set is set to "English", only English long file name is supported.

2. Multi session FTP download will be banned by Router FTP server. If your FTP client has a multi connection mechanism, such as FileZilla, you should limit client connections to 1 to improve performance.

3. A workgroup name must be different from the host name. The workgroup name can have up to 15 characters and the host name can have up to 15 characters. Names cannot contain any of the following: \ / : * > ? [] ,

OK

3. Setup a user account for the FTP service by using **USB Application >>USB User Management**. Click index #1 link. In the example below, we have set up a new account with the username "user1", and granted "Read", "Write" and "List" permissions to it.

USB Application >> USB User Management

Profile Index: 1

☒ Profile	
Username	user1
Password	*****
Confirm Password	*****
Home Folder	
Access Rule	
File	☒ Read ☒ Write ☐ Delete
Directory	☒ List ☐ Create ☐ Remove

Notes:
The folder name can only contain the following characters: A-Z a-z 0-9 % ' () ~ * ! , ; and space.

OK Clear Cancel

4. Click **OK** to save the configuration.
5. To verify that the FTP service is running properly, open a browser window and enter ftp://192.168.1.1 as the destination. Replace 192.168.1.1 with the actual IP address of the router. When prompted to enter the login credentials, enter the username "user1" to login.

Log On

Enter the user name and password to log on to the system.

IP Address: 192.168.1.1

User Name: user1

Password: *****

After logging on, you can see the system log, Executive and other files.

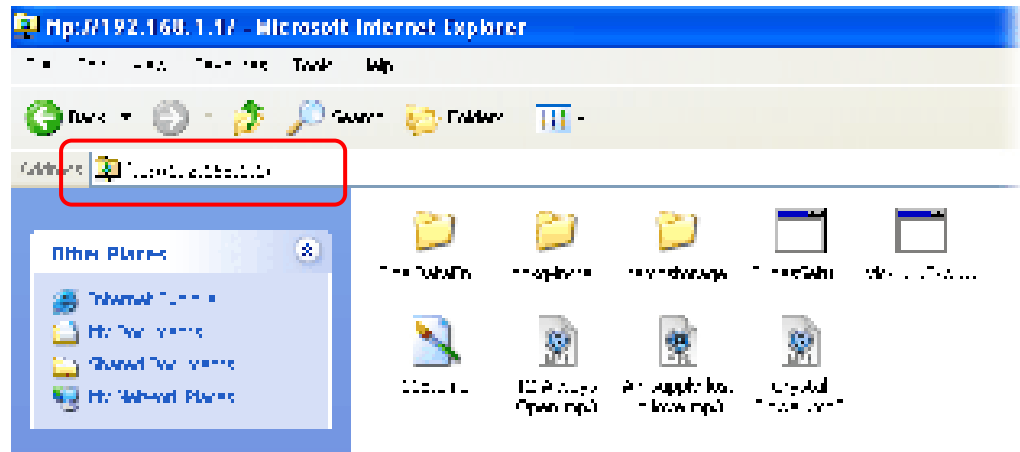
The driver will attempt to connect to the system before sending data to the system. To protect the security of your information, a data transfer folder (user1) is created.

Warning: About Log On Folder.

☐ Log on with key ☒ Log on with key

Log On Cancel

- When the following screen appears, you have successfully connected to the FTP server and verified that it is running properly.



- If you check **USB Application >> USB Disk Status** on browser, you will see the FTP session initiated by user1.

[USB Application >> USB Disk Status](#)

USB Mass Storage Device Status

Connection Status: **Link Connected**

[Disconnect USB Disk](#)

Write Protect Status: **No**

Disk Capacity: 5000 MB

USB Disk Users Connected

[Refresh](#)

Index	Service	IP Address(Port)	Username	
1	FTP	192.168.1.100(21)	user1	Close

Now, users in LAN of Vigor2765 can access into the USB storage device by typing ftp://192.168.1.1 on any browser. They can add or remove files / directories, depending on the Access Rule for FTP account settings in **USB Application >>USB User Management**.

Part IX Troubleshooting



Troubleshooting

This part will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration

IX-1 Diagnostics

This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

If all above stages are done and the router still cannot run normally, it is the time for you to contact your dealer or DrayTek technical support for advanced help.

Web User Interface

This section contains utilities that can assist you in analyzing issues and failures during the setup and operation of the router.

System Maintenance

Diagnostics

Dial-out Triggering

Routing Table

ARP Cache Table

IPv6 Neighbour Table

DHCP Table

NAT Sessions Table

DNS Cache Table

Ping Diagnosis

Data Flow Monitor

Traffic Graph

Trace Route

Syslog Explorer

IPv6 TSPC Status

DSL Status

DoS Flood Table

Route Policy Diagnosis

IX-1-1 Dial-out Triggering

This page shows the packet header that is transmitted when a WAN connection (such as a PPPoE connection) is initiated.

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

Decoded Format:

00.00.00.00 -> 00.00.00.00

Protocol: 0x00

Available settings are explained as follows:

Item	Description
HEX Format	Shows the dial-out triggered packet header in hexadecimal format.
Decoded Format	Shows the dial-out triggered packet header in human-readable format.

Refresh	Click it to reload the page.

IX-1-2 Routing Table

Click **Diagnostics** and click **Routing Table** to open the web page.

[Diagnostics](#) >> [View Routing Table](#)

IPv4 Routing Table					Refresh
Key	Destination	Gateway	Interface		
G	192.168.18.0/24	255.255.255.255	v4a-192.168.1.2	LAN1	
C	192.168.1.0/24	255.255.255.0	directly connected	LAN1	
G	0.0.0.0/0	255.255.255.255	v4a-192.168.1.1	LAN1	

Key
C: Connected R: Static R: RIP -: default -: private

IPv6 Routing Table					Show Detail	Refresh
Destination	Interface	Flags	Metric	Next Hop		
FE80::/64	LAN1	U	256	::		
FE80::/64	LAN1	U	256	::		

Flag
U: Route UP D: Default Route G: Use Next Hop S: Static Route R: RIPv6

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

IX-1-3 ARP Cache Table

Click **Diagnostics** and click **ARP Cache Table** to view the content of the ARP (Address Resolution Protocol) cache held in the router. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.

Diagnostics

View ARP Cache Table

LAN

WAN

Show

All LANs

and

All VLANs

Ethernet ARP Cache Table

All VLANs

Clear

Refresh

IP Address	MAC Address	VLAN	Host ID	Interface	View	Port
192.168.1.8	aa-bb-cc-11-22-33	VLAN1		Ether1	---	P1
192.168.1.10	dd-ee-ff-44-55-66	VLAN3		Ether1		P2
		VLAN4				
		VLAN5				
		VLAN6				
		VLAN7				

Show Comment

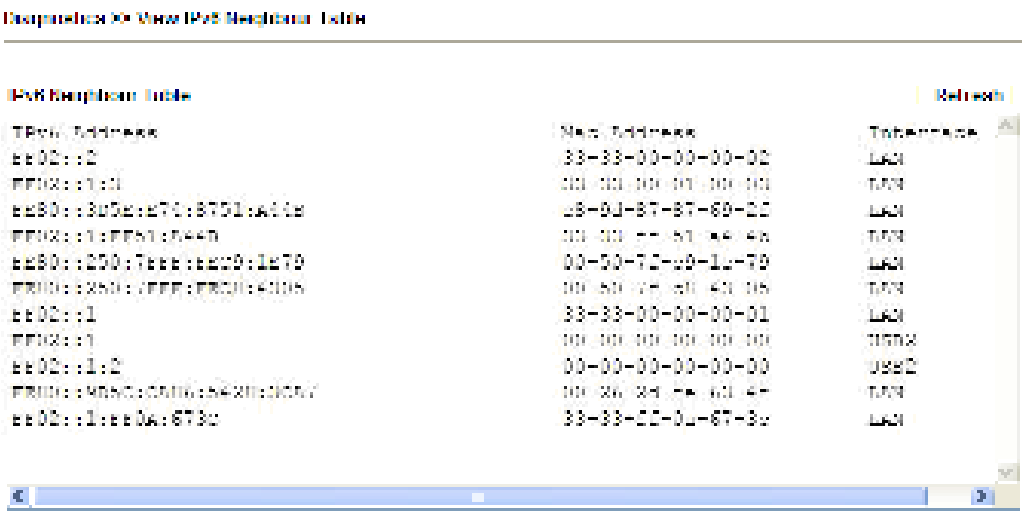
Available settings are explained as follows:

Item	Description
Show	Select the LAN(s) and VLAN(s) to display ARP table information. By default, information on all LANs and VLANs is displayed.
Refresh	Click it to reload the page with the most up-to-date information.

IX-1-4 IPv6 Neighbour Table

This page displays the mapping between Ethernet hardware addresses (MAC addresses) and IPv6 addresses. This information is helpful in diagnosing network problems, such as IP address conflicts.

Click **Diagnostics** and click **IPv6 Neighbour Table** to open the web page.



Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

IX-1-5 DHCP Table

This page 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](#)

IPv4 Address Assignment Table

State: All LANs

Dynamic IP Assignment Table		Static IP Assignment Table		☐ Show Comment Refresh	
Index	IP Address	MAC Address	Leased Time	Host IP	

[LAN1	> DHCP Server On		IP Pool: 192.168.1.10 ~ 192.168.1.200]		
1	192.168.1.18	68-18-7F-22-11-44	22:18:48		

IPv6 Address Assignment Table

[Refresh](#)

Index	IPv6 Address	LAID	Link Layer Address	Leased Time

Available settings are explained as follows:

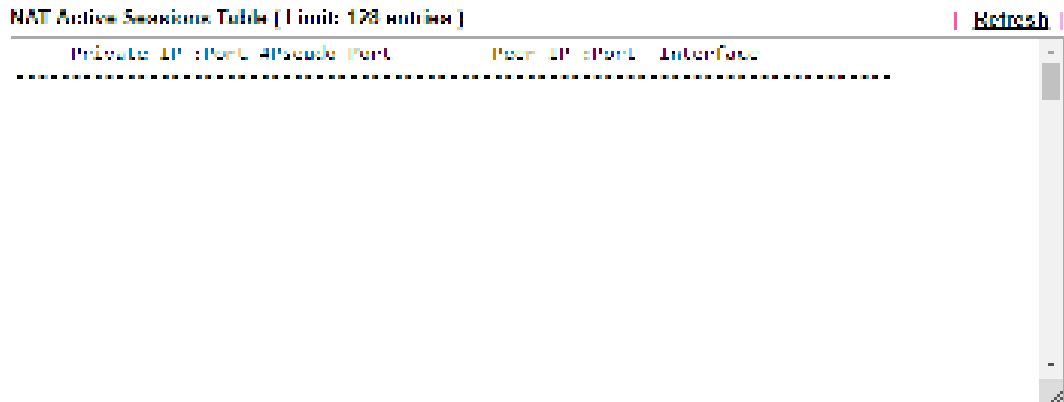
Item	Description
Index	Shows the index of the DHCP entry.
IP Address	Shows the IP address assigned by the router to the MAC address.
MAC Address	Shows the MAC address of this DHCP entry.
Leased Time	Shows the remaining time of the DHCP lease of the device.
HOST ID	Shows the host ID of this network device.
Refresh	Click to reload this page with the most up-to-date information.

IX-1-6 NAT Sessions Table

This screen shows the 128 newest entries in the NAT sessions table.

Click **Diagnostics** and click **NAT Sessions Table** to open the list page.

[Diagnostics](#) >> [NAT Sessions Table](#)



Private IP :Port #Pseudo Port	Peer IP :Port	Interface

Available settings are explained as follows:

Item	Description
Private IP:	Shows the IP address of the LAN host.
Port #	Shows the port number used on the LAN host for this NAT session.
Pseudo Port	Shows the external port number used on the WAN interface for this NAT session.
Peer IP:	Shows the remote host's IP address.
Port	Shows the port number used on the remote host for this NAT session.
Interface	Shows the WAN interface used for this NAT session.
Refresh	Click to reload this page with the most up-to-date information.

IX-1-7 DNS Cache Table

The router can function as a DNS server which allows LAN clients to look up DNS information by sending DNS requests to the router. Such DNS information is temporarily cached on the router and can be viewed on this page.

Click **Diagnostics** and click **DNS Cache Table** to open the web page.

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)

Notes:

An entry of which TTL shows "Static" is a domain name created in LAN DNS.

☐

When an entry's TTL is larger than

0

 s, this entry will be deleted from the table.

OK

Available settings are explained as follows:

Item	Description
Clear	Click to clear all cached DNS lookup entries.
Refresh	Click it to reload the page.
When an entry's TTL is larger than...	When this box is checked, DNS entries whose TTL (time to live, in seconds) exceeds the valued specified here will be deleted from the router's cache automatically. Be sure to click OK after making changes to have them saved.

IX-1-8 Ping Diagnosis

Click **Diagnostics** and click **Ping Diagnosis** to open the web page.

Diagnostics >> Ping Diagnosis

Ping Diagnosis

IPv4 IPv6

Ping through: Auto

Ping to: Host IP

Source IP: Auto

IP Address:

Run

Result

Clear

Note:

1. If you want to ping a LAN PC or you don't want to specify which WAN to ping through, please select "Auto" in Ping Through.
2. If you select "Auto" in Source IP, we will fill Source IP according to the interface you ping through.

or

Diagnostics >> Ping Diagnosis

Ping Diagnosis

IPv4 IPv6

Ping through: Auto

Ping IPv6 Address: Auto

WAN1

WAN2

WAN3

Run

Result

Clear

Note:

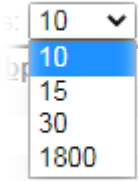
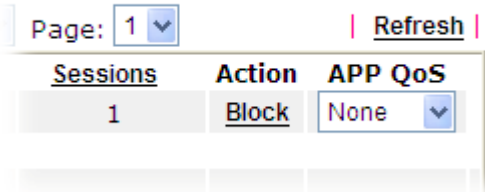
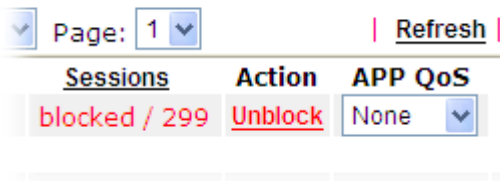
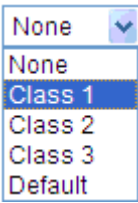
1. If you want to ping a LAN PC or you don't want to specify which WAN to ping through, please select "Auto" in Ping Through.
2. If you select "Auto" in Source IP, we will fill Source IP according to the interface you ping through.

Available settings are explained as follows:

Item	Description
IPv4 /IPv6	Choose the interface for such function. Select the protocol to perform the ping operation.
Ping through	Select a WAN interface from drop down list to through which you want to perform the ping operation, or choose Auto to be let the router select the WAN interface.

Ping to	Select the type of target to which you wish to ping.
IP Address	Enter the IP address of the Host/IP that you want to ping.
Ping IPv6 Address	Enter the IPv6 address that you want to ping.
Run	Click this button to initiate the ping process. The result will be displayed on the screen.
Clear	Click this link to clear the ping result.

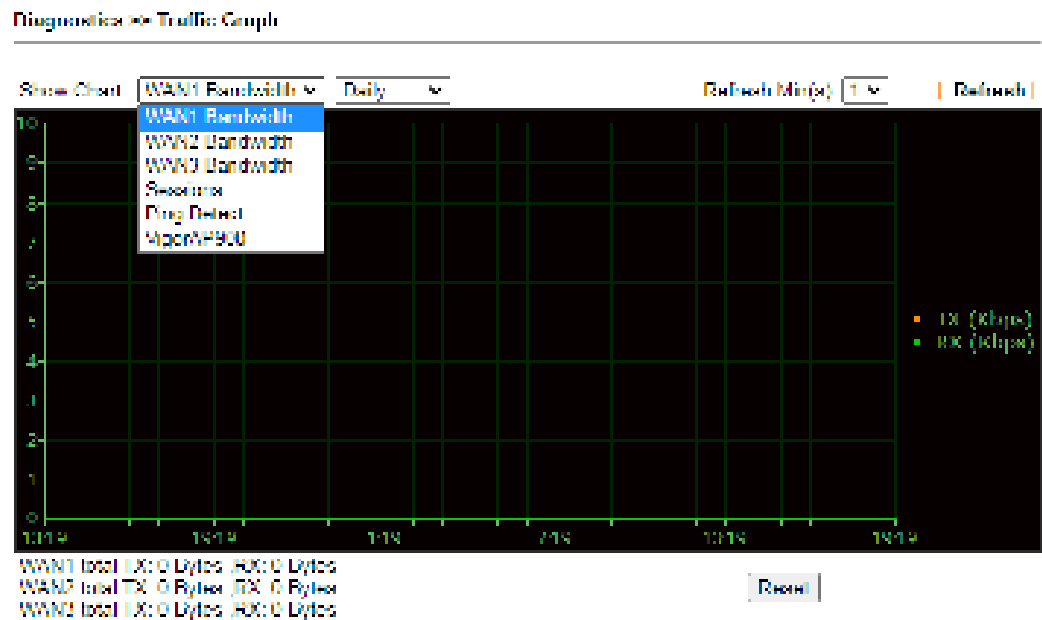
Item	Description
Enable Data Flow Monitor	Check this box to enable this function.

Refresh Seconds	Select the desired refresh time interval from the drop-down list. The page will then be refreshed with updated information at the selected interval. 
Refresh	Click to refresh this page manually.
Index	Shows the index of the data flow.
IP Address	Shows the IP address of the monitored device.
TX rate (kbps)	Shows the transmission speed of the monitored device.
RX rate (kbps)	Shows the receiving speed of the monitored device.
Sessions	Shows the number of session that you specified on the Limit Session web page.
Action	Block - can prevent specified PC accessing into Internet within 5 minutes.  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. 
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.

IX-1-10 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to open the web page. Choose WAN1/WAN2/WAN3 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. Click **Reset** to zero the accumulated RX/TX (received and transmitted) data of WAN. Click **Refresh** to renew the graph at any time.



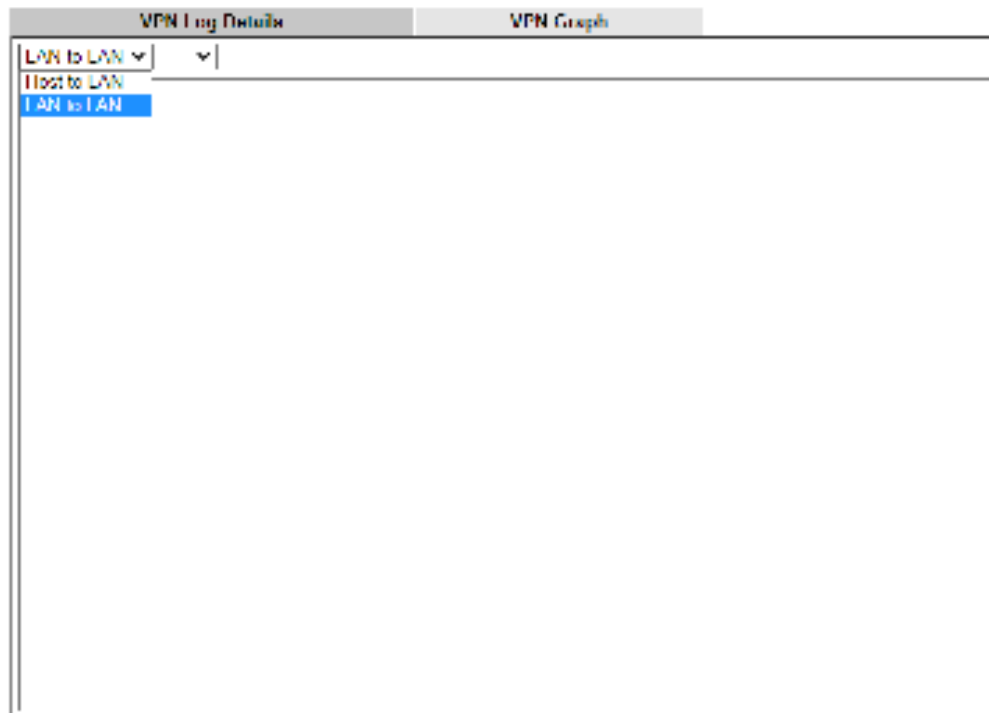
The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1/WAN2/WAN3 Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

For Sessions chart, the numbers displayed on vertical axis represent the numbers of the NAT sessions during the past.

VIII-1-11 VPN Graph

Click **Diagnostics** and click **VPN Graph** to open the web page.

Diagnostics >> VPN Graph



and

Diagnostics >> VPN Graph



IX-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

Auto

Protocol

ICMP

Host / IP Address:

Run

Result

Clear

or

Diagnostics >> Trace Route

Trace Route

☐ IPv4

☒ IPv6

Trace Host / IP Address:

Run

Result

Clear

Available settings are explained as follows:

Item	Description
IPv4 / IPv6	Select the IP version used to perform the trace route.
Trace through	Select the WAN interface used to perform the trace route.
Protocol	Select either UDP or ICMP used to perform the trace route.

Host/IP Address	Enter the hostname or the IP address of trace route destination.
Trace Host/IP Address	Enter the hostname or the IPv6 address of trace route destination.
Run	Click this button to start the trace.
Clear	Click to clear the trace route result.

IX-1-13 Syslog Explorer

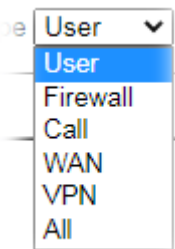
This page displays syslog information in real time. There are two options for displaying syslog information: Web Syslog and USB Syslog.

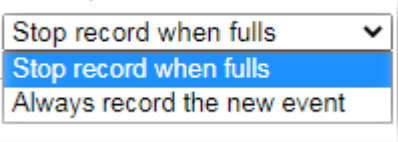
For Web Syslog

This page displays User/Firewall/call/WAN/VPN Syslog events and their time of occurrence. To enable Web Syslog, check the **Enable Web Syslog** checkbox, specify the type of Syslog events to view, and select the display mode. The log messages will start appearing as events matching the selected type occur.

Diagnostics >> Syslog Explorer

Available settings are explained as follows:

Item	Description
Enable Web Syslog	Check this box to enable Web Syslog.
Syslog Type	Select the type of Syslog info to monitor. 
Export	Click to save the data as a file.
Refresh	Click to refresh this page manually.
Clear	Click to purge Syslog entries from the Web Syslog buffer.
Display Mode	Two display modes are available.

	 Stop record when fulls – When the Web Syslog buffer is full, no further logging will be performed. Always record the new event – Events are recorded in a FIFO manner. As the buffer gets full, oldest events are purged to make room for new events.
Time	Displays the time when the event occurred.
Message	Displays the event information.

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 within the event syslog file size is over 100K.			
Time	Log Type	Page 1/14	Log Type: 1/14
Time	Log Type	Message	

Available settings are explained as follows:

Item	Description
Time	Displays the time of the event occurred.
Log Type	Displays the type of the record.
Message	Displays the information for each event.

IX-1-14 IPv6 TSPC Status

IPv6 TSPC (Tunnel Setup Protocol Client) status page could help you diagnose issues with IPv6 connections that utilize TSP.

If TSPC is configured properly, the router will display the following when the router has connected to the tunnel broker successfully.

Diagnostics >> IPv6 TSPC Status

[illegible]

Available settings are explained as follows:

Item	Description
Refresh	Click to refresh the page to show the latest status.
WAN1 ~ WAN3	Select the tab that corresponds to the WAN connection that you wish to view the IPv6 TSPC status.

IX-1-15 DSL Status

This page shows the DSL status for debugging or troubleshooting by DrayTek support staff.

Diagnostics >> DSL Status

General		Time Information		Refresh	
ATU-R Information					
Type:	VDSL2				
Hardware:	Zamor A				
Firmware:	001 001 000 001 001 017				
Power Mgmt. Mode:	DPA - G997 - RPA - NA				
Line State:	TRAINING				
Running Mode:					
Vendor ID:	76004452 41590000				
ATU-C Information					
Vendor ID:	00000000 00000000 [-----]				
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	

IX-1-16 DoS Flood Table

This page shows IP addresses that are currently engaging in DoS flood as detected by the DoS Flooding Defense mechanism. It provides useful information to network engineers (e.g., MIS engineers) to diagnose the network environment to identify potentially malicious network traffic and entities. Identified IP addresses and the destination ports used in SYN, UDP, and ICMP Flood attacks will be shown on the respective tab pages.

IP addresses that are suspected to be attacking the network can be blocked by clicking the **Block** button on the SYN Flood, UDP Flood and ICMP Flood tab pages.

Diagnosics >> DoS Flood Table

IPv4

SYN Flood

UDP Flood

ICMP Flood

Refresh

Tracking IP	Destination Port	
192.168.1.100	80	Block
192.168.1.100	40000(🚫)	Block

IPv6

SYN Flood

UDP Flood

ICMP Flood

Refresh

Tracking IP	Destination Port

📘

Info

The icon - (🚫) - means there is something wrong (e.g., attacking the system) with that IP address.

IX-1-17 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

ICMP

▼

Src IP

Specify an IP

▼

192.168.1.2

Dst IP

Specify an IP

▼

Dst Port

Any 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

選擇檔案

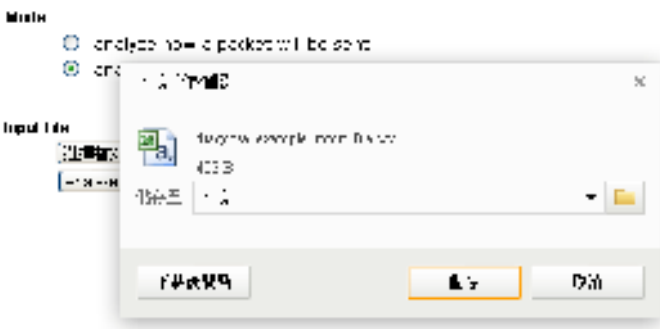
未選擇任何檔案

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

IX-2 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

1. Check the power line and WLAN/LAN cable connections.
Refer to “I-2 Hardware Installation” for details.
2. Turn on the router. Make sure the **ACT LED** blink once per second and the correspondent **LAN LED** is bright.



3. If not, it means that there is something wrong with the hardware status. Simply back to “I-2 Hardware Installation” to execute the hardware installation again. And then, try again.

IX-3 Checking If the Network Connection Settings on Your Computer Is OK or Not

Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is still failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows



Info

The example is based on Windows 7. As to the examples for other operation systems, please refer to the similar steps or find support notes in www.DrayTek.com.

1. Open **All Programs>>Getting Started>>Control Panel**. Click **Network and Sharing Center**.

Fonts

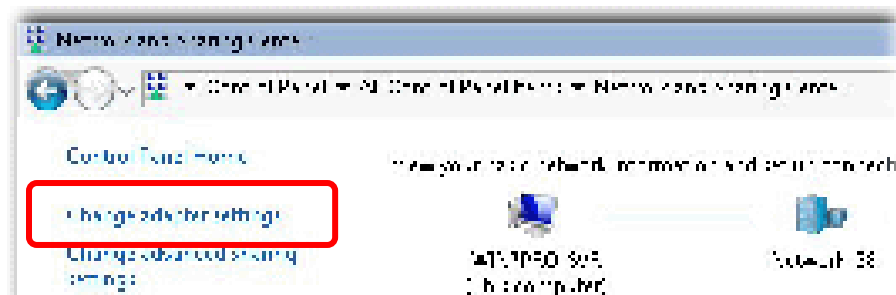
Java

Network and Sharing Center

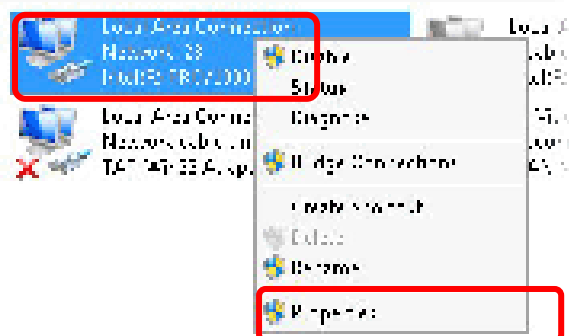
Personalization

Recovery

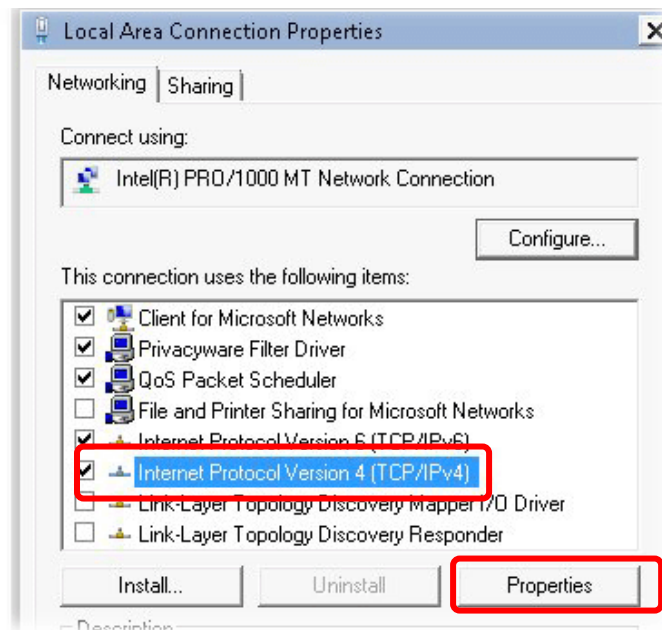
2. In the following window, click **Change adapter settings**.



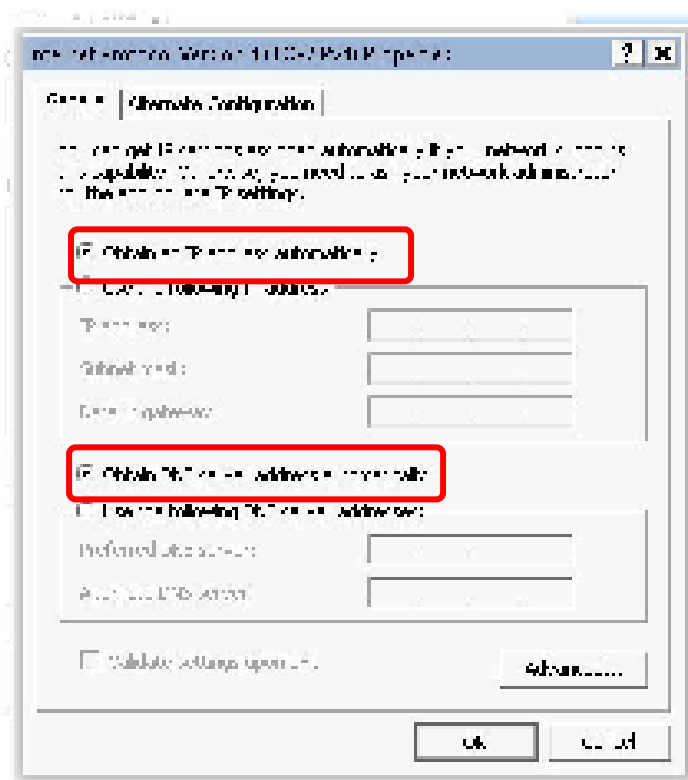
3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



4. Select **Internet Protocol Version 4 (TCP/IP)** and then click **Properties**.

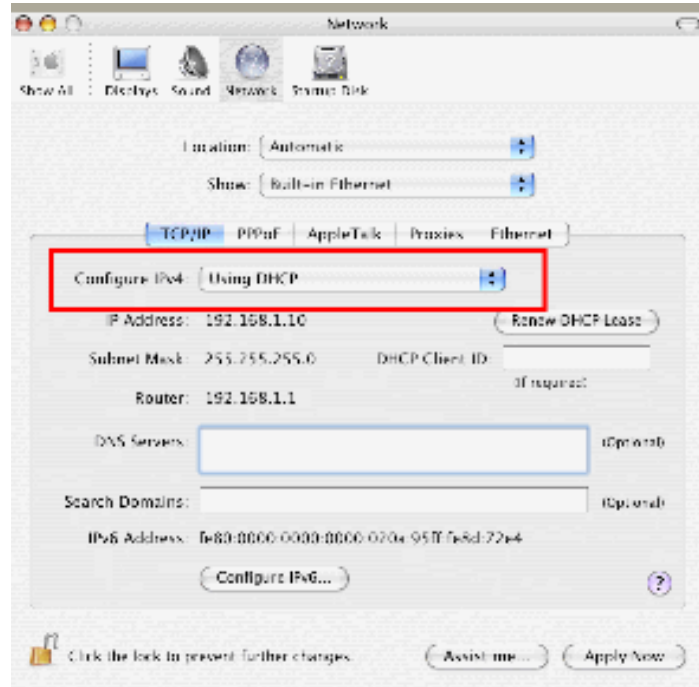


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



For Mac OS

1. Double click on the current used Mac OS on the desktop.
2. Open the **Application** folder and get into **Network**.
3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.



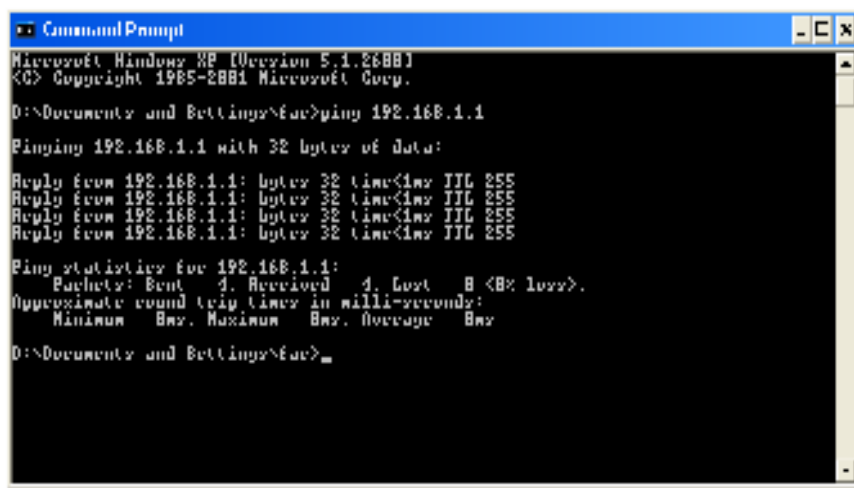
IX-4 Pinging the Router from Your Computer

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use “ping” command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section VIII-3).

Please follow the steps below to ping the router correctly.

For Windows

1. Open the **Command Prompt** window (from **Start menu> Run**).
2. Enter **cmd**. The DOS command dialog will appear.



```
Command Prompt
Microsoft Windows [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\far>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\far>
```

3. Enter **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. Enter **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 ttty1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$
```

IX-5 Checking If the ISP Settings are OK or Not

If WAN connection cannot be up, check if the LEDs (according to the LED explanations listed on section I-1) are correct or not. If the LEDs are off, please:

- Change the **Physical Type** from **Auto negotiation** to other values (e.g., 100M full duplex).
- Next, change the physical type of modem (e.g., DSL) offered by ISP with the same value configured in Vigor router. Check if the LEDs on Vigor router are on or not.
- If not, please install an additional switch for connecting both Vigor router and the modem offered by ISP. Then, check if the LEDs on Vigor router are on or not.
- If the problem of LEDs cannot be solved by the above measures, please contact with the nearest reseller, or send an e-mail to DrayTek FAE for technical support.
- Check if the settings offered by ISP are configured well or not.

When the LEDs are on and correct, yet the WAN connection still cannot be up, please:

- Open **WAN >> Internet Access** page and then check whether the ISP settings are set correctly. Click **Details Page** of WAN1~WAN3 to review the settings that you configured previously.

WAN >> Internet Access

Internet Access

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

DHCP Client Option

IX-6 Problems for 3G/4G Network Connection

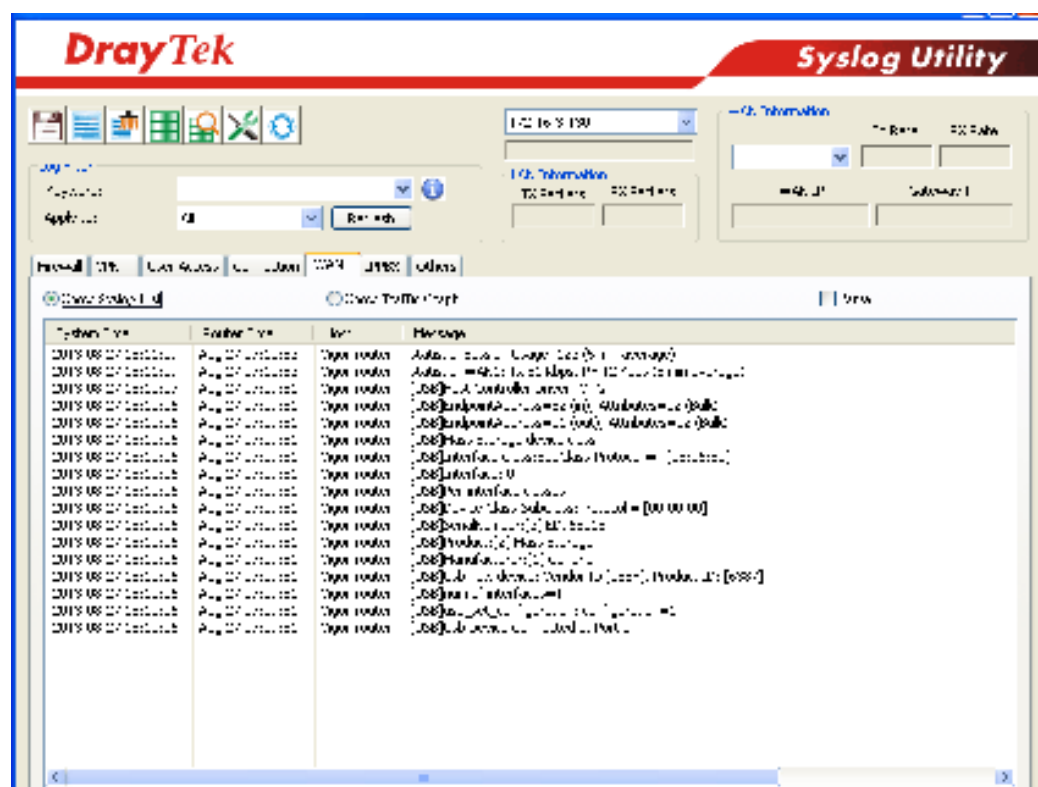
When you have trouble in using 3G/4G network transmission, please check the following:

Check if USB LED lights on or off

You have to wait about 15 seconds after inserting 3G/4G USB Modem into your Vigor2765. 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 Vigor2765.

USB LED lights on but the network connection does not work

Check the PIN Code of SIM card is disabled or not. Please use the utility of 3G/4G USB Modem to disable PIN code and try again. If it still fails, it might be the compliance problem of system. Please open DrayTek Syslog Tool to capture the connection information (WAN Log) and send the page (similar to the following graphic) to the service center of DrayTek.



Transmission Rate is not fast enough

Please connect your Notebook with 3G/4G USB Modem to test the connection speed to verify if the problem is caused by Vigor2765. In addition, please refer to the manual of 3G/4G USB Modem for LED Status to make sure if the modem connects to Internet via HSDPA mode. If you want to use the modem indoors, please put it on the place near the window to obtain better signal receiving.

IX-7 Backing to Factory Default Setting If Necessary

Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware. Such function is available in **Admin Mode** only.

**Info**

After pressing factory default setting, you will loose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null.

Software Reset

You can reset the router to factory default via Web page. Such function is available in **Admin Mode** only.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **Reboot Now**. After few seconds, the router will return all the settings to the factory settings.

System Maintenance » Reboot System

Reboot System

Do you want to reboot your router ?

☒ Using current configuration

☐ Using factory default configuration

Reboot Now

Auto Reboot Time Schedule

Schedule Profile : None

None

None

None

Note:

Action and Duration Time settings will be ignored.

OK

Cancel

Hardware Reset

While the router is running (ACT LED blinking), press the **Factory Reset** button and hold for more than 5 seconds. When you see the **ACT** LED blinks rapidly, please release the button. Then, the router will restart with the default configuration.



After restore the factory default setting, you can configure the settings for the router again to fit your personal request.

IX-8 Contacting DrayTek

If the router still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@DrayTek.com.

Part X Telnet Commands

Accessing Telnet of Vigor2765

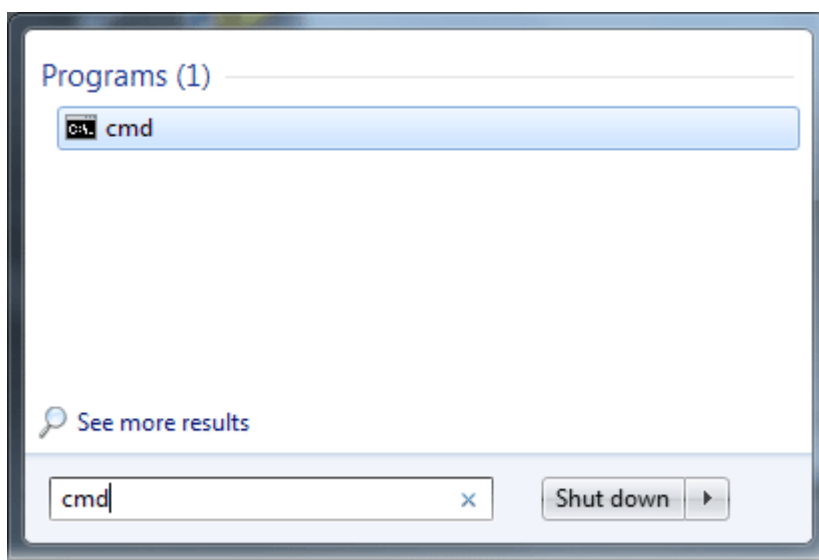
This chapter also gives you a general description for accessing telnet and describes the firmware versions for the routers explained in this manual.



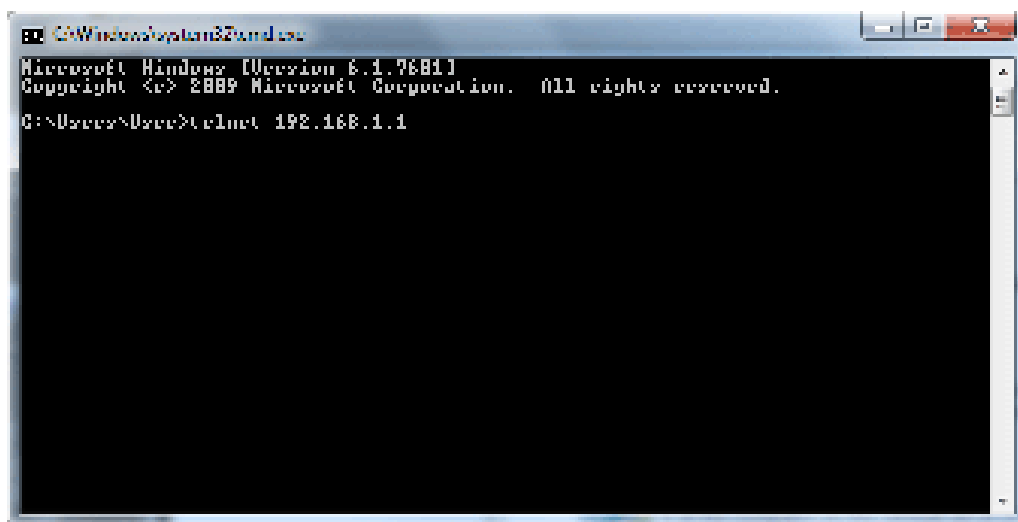
Info

For Windows 7 user, please make sure the Windows Features of Telnet Client has been turned on under Control Panel>>Programs.

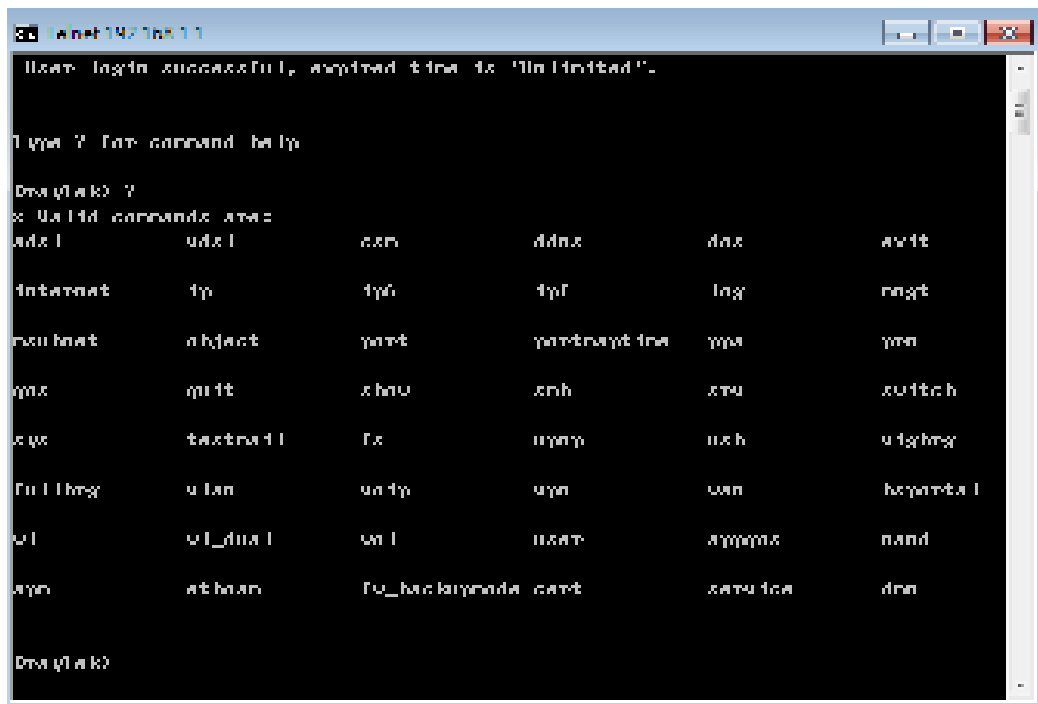
Enter **cmd** and press Enter. The Telnet terminal will be open later.



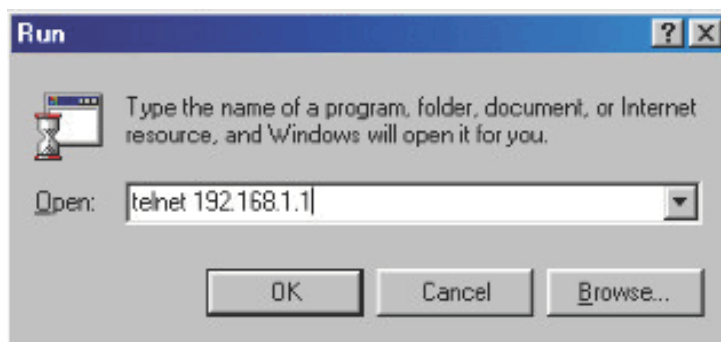
In the following window, type **Telnet 192.168.1.1** as below and press Enter. Note that the IP address in the example is the default address of the router. If you have changed the default, enter the current IP address of the router.



Next, enter admin/admin for Account/Password. Then, enter ?. 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*]

Syntax	Description
auto	It means auto detection of ADSL transmission packet.
percent	It means to specify the percentage of ADSL transmission packet. Available range is 10-100.

Example

```
> adsl txpct auto
% tx percentage : 80
> adsl txpct 75
% tx percentage : 75
```

Telnet Command: adsl status

This command is used to display current status of ADSL setting.

Syntax

adsl status

Example

```
> adsl status
----- ATU-R Info (hw: annex A, f/w: annex A) -----
Running Mode      :                State      : TRAINING
DS Actual Rate    :          0 bps   US Actual Rate    :          0 bps
DS Attainable Rate :          0 bps   US Attainable Rate :          0 bps
DS Path Mode      :          Fast   US Path Mode      :          Fast
DS Interleave Depth :          0     US Interleave Depth :          0
NE Current Attenuation :          0 dB   Cur SNR Margin    :          0 dB
DS actual PSD     :          0. 0 dB   US actual PSD     :          0. 0 dB
NE Rcvd Cells     :          0     NE Xmitted Cells    :          0
NE CRC Count      :          0     FE CRC Count       :          0
NE ES Count       :          0     FE ES Count        :          0
Xdsl Reset Times  :          0     Xdsl Link Times   :          0
ITU Version[0]    : b5004946   ITU Version[1]      : 544e0000
ADSL Firmware Version : 06-06-01-07-00-01
Power Management Mode : DSL_G997_PMS_NA
Test Mode         : DISABLE
----- ATU-C Info -----
Far Current Attenuation :          0 dB   Far SNR Margin    :          0 dB
CO ITU Version[0]      : 00000000   CO ITU Version[1] : 00000000
DSLAM CHIPSET VENDOR   : < ----- >
>
```

Telnet Command: adsl ppp

This command can set the Internet Access mode for the router.

Syntax

adsl ppp [? | pvc_no vci vpi Encap Proto modu acqIP idle [Username Password]

Syntax Description

Parameter	Description
?	Display the command syntax of “adsl ppp”.
pvc_no	It means the PVC number and the adjustable range is from 0 (Channel-1) to 7(Channel-8).
Encap	Different numbers represent different modes. 0 : VC_MUX, 1: LLC/SNAP, 2: LLC_Bridge, 3: LLC_Route, 4: VCMUX_Bridge 5: VCMUX_Route, 6: IPoE.
Proto	It means the protocol used to connect Internet. Different numbers represent different protocols. 0: PPPoA, 1: PPPoE, 2: MPoA.
Modu	0: T1.413, 2: G.dmt, 4: Multi, 5: ADSL2, 7: ADSL2_AnnexM 8: ADSL2+ 14: ADSL2+_AnnexM.
acqIP	It means the way to acquire IP address. 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.

adsl bridge [*pvc_no/ status/ save/ enable/ disable*] [*on/ off/ clear/ tag tag_no*] [*service type*] [*px ...*]

Syntax Description

Parameter	Description
<i>pvc_no</i>	It means <i>pvc</i> number and must be between 0(Channel 1) to 7(Channel 8).
<i>status</i>	It means to shown the whole bridge status.
<i>save</i>	It means to save the configuration to flash.
<i>enable</i>	It means to enable the Multi-VLAN function.
<i>disable</i>	It means to disable the Multi-VLAN function.
<i>on/ off</i>	It means to turn on/off bridge mode for the specific channel.
<i>clear</i>	It means to turn off and clear all the PVC settings.
<i>tag tag_no</i>	No tag: -1 Available number for tag: 0-4095
<i>pri pri_no</i>	The number 0 to 7 can be set to indicate the priority. "7" is the highest.
<i>service type</i>	Two number can be set: 0: for Normal (all the applications will be processed with the same PVC). 1: for the IGMP with different PVC which is used for special ISP.
<i>px...</i>	It means the number of LAN port (x=2-4). Port 1 is locked for NAT.

Example

```

> adsl bridge 4 on p2 p3
PVC Bridge p1 p2 p3 p4 Service Type Tag Pri

```

```
-----  
4    ON      0    0    1    0    Normal    -1 (OFF)    0  
PVC 0 & 1 can't set for bridge mode.  
Please use 'save' to save config.
```

Telnet Command: adsl drivermode

This command is useful for laboratory to measure largest power of data transmission. Please follow the steps below to set adsl drivermode.

1. Please connect dsl line to the DSLAM.
2. Waiting for dsl SHOWTIME.
3. Drop the dsl line.
4. Now, it is on continuous sending mode, and adsl2/2+ led is always ON.
5. Use 'adsl reboot' to restart dsl to normal mode.

Telnet Command: adsl reboot

This command can wake up the idle router.

Example

```
> adsl reboot  
% Adsl is Rebooting...
```

Telnet Command: adsl oamlb

This command is used to test if the connection between CPE and CO is OK or not.

adsl oamlb [*n*][*type*]

adsl oamlb chklink [*on/off*]

adsl oamlb [*log_on/log_off*]

Syntax Description

Parameter	Description
<i>n</i>	It means the total number of transmitted packets.
<i>type</i>	It means the protocol that you can use. 1 - for F4 Seg-to-Seg (VP level) 2 - for F4 End-to-End (VP level) 4 - for F5 Seg-to-Seg (VC level) 5 - for F5 End-to-End (VC level)
<i>chklink</i>	Check the DSL connection.
<i>Log_on/log_off</i>	Enable or disable the OAM log for debug.

Example

```
> adsl oamlb chklink on
OAM checking dsl link is ON.
> adsl oamlb F5 4
Tx cnt=0
Rx Cnt=0
>
```

Telnet Command: adsl vcilimit

This command can cancel the limit for vci value.

Some ISP might set the vci value under 32. In such case, we can cancel such limit manually by using this command. Do not set the number greater than 254.

adsl vcilimit [*n*]

Syntax Description

Parameter	Description
<i>n</i>	The number shall be between 1 - 254.

Example

```
> adsl vcilimit 33
change VCI limitation from 32 to 33.
```

Telnet Command: adsl annex

This command can display the annex interface of this router.

Example

```
> adsl annex
% hardware is annex B.
% modem code is annex B; built at 01/15,07:34.
```

Telnet Command: adsl automode

This command is used to add or remove ADSL modes (such as ANNEXL, ANNEXM and ANNEXJ) supported by Multimode.

adsl automode [*add*/*remove*/*set*/*default*/*show*] [*adsl_mode*]

Syntax Description

Parameter	Description
<i>add</i>	Add ADSL mode.
<i>remove</i>	Remove ADSL mode.
<i>set</i>	Use default settings plus the new added ADSL mode.
<i>default</i>	Use default settings.
<i>show</i>	Display current setting.
<i>adsl_mode</i>	There are three modes to be choose, ANNEXL, ANNEXM and ANNEXJ.

Example

```
> 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.

adsl showbins [*startbin endbin* | *up*]

Syntax Description

Parameter	Description
<i>startbin</i>	The number is between 0 ~ 4092.
<i>endbin</i>	The number is between 4 ~ 4095.
<i>up</i>	Show upstream information.

Example

```
> adsl showbins 2 30
DOWNSTREAM :
-----
Bin  SNR  Gain Bi - Bin  SNR  Gain Bi - Bin  SNR  Gain Bi - Bin  SNR  Gain Bi
```

dB .1dB ts				dB .1dB ts				dB .1dB ts				dB .1dB ts			
-----				-----				-----				-----			
-----				-----				-----				-----			
Bin	SNR	Gain	Bi -	Bin	SNR	Gain	Bi -	Bin	SNR	Gain	Bi -	Bin	SNR	Gain	Bi
	dB	.1dB	ts		dB	.1dB	ts		dB	.1dB	ts		dB	.1dB	ts
>															

Telnet Command: adsl optn

This command allows you to configure DSL line feature. This feature is depended on modem firmware. For G.Vector feature, modem firmware needs to support VDSL2 G.Vector.

adsl optn FUNC [*us/ ds/ bi* [*value/ on/ off*]]

Syntax Description

Parameter	Description
<i>FUNC</i>	Available functions include: 'trellis', 'bitswap', 'sra', 'retx', 'aelem', 'status', 'g.vector', 'default'. default: Set all features back to default settings.
<i>us/ ds/ bi</i>	us: means "upstream" ds: means "downstream" bi: means "bidirection"
<i>value</i>	The values for different functions change slightly. bitswap=0-2, sra=0,2,3,4.
<i>on/ off</i>	Type "on" for enabling such function. Type "off" for disabling such function. Functions of 'aelem' and 'g.vector' are only on/off.

Example

```
> adsl optn status
trellis      [US] =      ON, [DS] =      ON.
bitswap      [US] =      0, [DS] =      0.
              [0: default (ON), 1: ON, 2: OFF]
sra          [US] =      0, [DS] =      0.
              [0: default (=3), 2: OFF, 3: ON , 4: DYNAMIC_SOS]
retx         [US] =      ON, [DS] =      ON.
aelem        ON
G.Vector     ON
```

Telnet Command: adsl savecfg

This command can save the configuration into FLASH with a file format of cfg.

Example

```
> adsl savecfg
% Xdsl Cfg Save OK!
```

Telnet Command: adsl vendorid

This command allows you to configure user-defined CPE vendor ID.

adsl vendorid [*status/ on/ off/ set vid0 vid1*]

Syntax Description

Parameter	Description
<i>status</i>	Display current status of user-defined vendor ID.
<i>on</i>	Enable the user-defined function.
<i>off</i>	Disable the user-defined function.
<i>set vid0 vid1</i>	It means to set user-defined vendor ID with vid0 and vid1. The vendor ID shall be set with HEX format, ex: 00fe7244: 79612f21.

Example

```
> adsl vendorid status
% User define CPE Vendor ID is OFF
% vid0:vid1 = 0x00fe7244:79612f21
> adsl vendorid on set vid0 vid1
% User define CPE Vendor ID is ON
```

Telnet Command: adsl atm

This command can set QoS parameter for ATM.

adsl atm pcr [*pvc_no*][*PCR*][*max*][*status*]

adsl atm scr [*pvc_no*][*SCR*][*status*]

adsl atm mbs [*pvc_no*][*MBS*][*status*]

adsl atm status

Syntax Description

Parameter	Description
<i>pvc_no</i>	It means <i>pvc</i> number and must be between 0(Channel 1) to 7(Channel 8).
<i>PCR</i>	It means Peak Cell Rate for upstream. The range for the number is "1" to "2539".
<i>max</i>	Get the highest speed for the upstream.
<i>SCR</i>	Mean Sustainable Cell Rate. The range for the number is "1" to "2539".
<i>MBS</i>	Maximum Burst Size. The range for the number is "1" to "2539".
<i>status</i>	Display PCR/SCR/MBS setting.

Example

```
> adsl atm pcr 1 200 max
% PCR is 0 for pvc 1.
> adsl atm pcr status
pvc    channel      PCR
-----
0       1           0
1       2           0
2       3           0
3       4           0
4       5           0
5       6           0
```

6	7	0
7	8	0
8	9	0
9	10	0

Telnet Command: adsl pvcbinding

This command can configure PVC to PVC binding. Such command is available only for PPPoE and MPoA 1483 Bridge mode.

adsl pvcbinding [*pvc_x pvc_y* | *status* | *-1*]

Syntax Description

Parameter	Description
<i>pvc_x</i>	The PVC number for the source.
<i>pvc_y</i>	The PVC number that the source PVC will be bound to.
<i>status</i>	Display a table for PVC binding group.
<i>-1</i>	It means to clear specific PVC binding.

Example

```
> adsl pvcbinding 3 5
set done. bind pvc3 to pvc5.
```

The above example means PVC3 has been bound to PVC5.

```
> adsl pvcbinding 3 -1
clear pvc-1 binding
```

The above example means the PVC3 binding group has been removed.

Telnet Command: adsl inventory

This command is used to display information about CO or CPE.

Syntax

adsl inventory [*co* | *cpe*]

Syntax Description

Parameter	Description
<i>co</i>	It means DSLAM (Digital Subscriber Line Access Multiplexer) or CO (Central Office).
<i>cpe</i>	It means CPE (Customer Premise Equipment).

Example

```
> adsl inventory co
DrayTek> adsl inventory co
xDSL inventory info only available in showtime.
DrayTek> adsl inventory cpe
G.994 vendor ID           : 0XB5004946544E0000
  G.994.1 country code    : 0XB500
  G.994.1 provider code   : IFTN
```

```

G.994.1 vendor info      : 0X000
System vendor ID         : 0XFE00445241590000
  System country code    : 0XFE00
  System provider code   : DRAY
  System vendor info     : 0X000
Version number           : 8B0F07
Version number(16 octets) : 0X3842304630370000000000000000000000
Self-test result         : PASS
Transmission mode capability : 0X50004000C010007
DrayTek>
>

```

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         : 0 bps US Actual Rate : 0 bps
DS Attainable Rate     : 0 bps US Attainable Rate : 0 bps
DS Path Mode           : Fast US Path Mode : Fast
DS Interleave Depth    : 0 US Interleave Depth : 0
NE Current Attenuation : 0 dB Cur SNR Margin : 0 dB
DS actual PSD          : 0. 0 dB US actual PSD : 0. 0
dB
NE CRC Count           : 0 FE CRC Count : 0
NE ES Count            : 0 FE ES Count : 0
Xdsl Reset Times       : 0 Xdsl Link Times : 0
ITU Version[0]         : b5004946 ITU Version[1] : 544e0000
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 : 0 dB 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.
<i>tcpmessage</i>	DSL debug tool mode is on.
<i>tcpmessage_off</i>	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
<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

```
> 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
<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

```
> 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
<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

```
> vdsl inventory co
xDSL inventory info only available in showtime.
> vdsl inventory cpe
G.994 vendor ID           : 0XB5004946544E0000
  G.994.1 country code    : 0XB500
  G.994.1 provider code   : IFTN
  G.994.1 vendor info     : 0X000
System vendor ID         : 0XFE00445241590000
  System country code     : 0XFE00
  System provider code    : DRAY
  System vendor info      : 0X000
Version number           : 8B0F07
Version number(16 octets) : 0X38423046303700000000000000000000
Self-test result         : PASS
Transmission mode capability : 0X50004000C010007
>
```

Telnet Command: csm appe prof

Commands under CSM allow you to set CSM profile to define policy profiles for different policy of IM (Instant Messenger)/P2P (Peer to Peer) application.

“csm appe prof “ is used to configure the APP Enforcement Profile name. Such profile will be applied in **Default Rule of Firewall>>General Setup** for filtering.

Syntax

```
csm appe prof -i INDEX [-v | -n NAME] setdefault]
```

Syntax Description

Parameter	Description
<i>INDEX</i>	Specify the index number of CSM profile, from 1 to 32.
- v	View the configuration of the CSM profile.
- n	Set a name for the CSM profile.
<i>NAME</i>	Specify a name for the CSM profile, less then 15 characters.
<i>setdefault</i>	Reset to default settings.

Example

```
> csm appe prof -i 1 -n games
The name of APPE Profile 1 was setted.
```

Telnet Command: csm appe set

It is used to configure group settings for IM/P2P/Protocol and Others in APP Enforcement Profile.

Syntax

```
csm appe set -i INDEX [-v GROUP] -e AP_IDX | -d AP_IDX] -a AP_IDX [ACTION]]
```

Syntax Description

Parameter	Description
<i>INDEX</i>	Specify the index number of CSM profile, from 1 to 32.
- v	View the IM/P2P/Protocol and Others configuration of the CSM profile.
-e	Enable to block specific application.
-d	Disable to block specific application.
-a	Set the action of specific application
<i>GROUP</i>	Specify the category of the application. Available options are: IM, P2P, Protocol and Others.
<i>AP_IDX</i>	Each application has independent index number for identification in CLI command. Specify the index number of the application here. If you have no idea of the inex number, do the following (Take IM as an example): Type “csm appe set -l 1 -v IM”, the system will list all of the index numbers of the applications categorized under IM.
<i>ACTION</i>	Specify the action of the application, 0 or 1.

	0: Block. All of the applications meet the CSM rule will be blocked. 1: Pass. All of the applications meet the CSM rule will be passed.

Example

```
>csm appe set -i 1 -a 1 1
Profile 1 - : <NULL> action set to Pass.
>
```

Telnet Command: csm appe show

It is used to display group (IM/P2P/Protocol and Others) information APP Enforcement Profile.

Syntax

csm appe show [-a/-i/-p/-t/-m]

Syntax Description

Parameter	Description
-a	View the configuration status for All groups.
-i	View the configuration status of IM group.
-p	View the configuration status of P2P group.
-t	View the configuration status of protocol group.
-m	View the configuration status of Others group.

Example

```
>csm appe show -t

      Type      Index      Name      Version  Advance
Advanced Option: (M)essage, (F)ile Transfer, (G)ame, (C)onference, and (O)ther
Activities
-----
      PROTOCOL      52      DB2
      PROTOCOL      53      DNS
      PROTOCOL      54      FTP
      PROTOCOL      55      HTTP      1.1
      PROTOCOL      56      IMAP      4.1
      PROTOCOL      57      IMAP STARTTLS      4.1
      PROTOCOL      58      IRC      2.4.0      .....
```

Telnet Command: csm appe config

It is used to display the configuration status (enabled or disabled) for IM/P2P/Protocol/Other applications.

Syntax

csm appe config -v INDEX [-i/-p/-t/-m]

Syntax Description

Parameter	Description

INDEX	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	Hotspot Shield	Disable	
OTHERS	TUNNEL	82	MS Teredo	Disable	
OTHERS	TUNNEL	83	PGPNet	Disable	
OTHERS	TUNNEL	84	Ping Tunnel	Disable	
.					
.					
.					

Total 66 APPs					
>					

Telnet Command: csm appe interface

It is used to configure APPE signature download interface.

Syntax

csm appe interface [*AUTO/ WAN#*]

Syntax Description

Parameter	Description
<i>AUTO</i>	Vigor router specifies WAN interface automatically.
<i>WAN</i>	Specify the WAN interface for signature downloading.

Example

```

> csm appe interface wan1
Download interface is set as "WAN1" now.

> csm appe interface auto
Download interface is set as "auto-selected" now.

```

Telnet Command: csm appe email

It is used to set notification e-mail for APPE signature based on the settings configured in **System Maintenance>>SysLog/Mail Alert Setup** (in which, the box of **APPE Signature** is checked under **Enable E-Mail Alert**).

Syntax

csm appe email [-e/ -d/ -s]

Syntax Description

Parameter	Description
-e	Enable notification e-mail mechanism.
-d	Disable notification e-mail mechanism.
-s	Send an example e-mail.

Example

```
> csm appe email -e
Enable APPE email.
```

Telnet Command: csm ucf

It is used to configure settings for URL control filter profile.

csm ucf show

csm ucf setdefault

csm ucf msg MSG

csm ucf obj INDEX [-n PROFILE_NAME | -l [P| B| A] | uac | wf]

csm ucf obj INDEX -n PROFILE_NAME

csm ucf obj INDEX -p VALUE

csm ucf obj INDEX -l P| B| A

csm ucf obj INDEX uac

csm ucf obj INDEX wf

Syntax Description

Parameter	Description
<i>show</i>	Display all of the profiles.
<i>setdefault</i>	Return to default settings for all of the profile.
<i>msg</i> MSG	Set the administration message. MSG means the content (less than 255 characters) of the message itself.
<i>obj</i>	Specify the object for the profile.
INDEX	Specify the index number of CSM profile, from 1 to 8.
-n	Set the profile name.
PROFILE_NAME	Specify the name of the profile (less than 16 characters)
-p	Set the priority (defined by the number specified in VALUE) for the profile.
VALUE	Number 0 to 3 represent different conditions. 0: It means Bundle: Pass. 1: It means Bundle: Block. 2: It means Either: URL Access Control First. 3: It means Either: Web Feature First.
-l	It means the log type of the profile. They are: P: Pass,

	B: Block, A: All,
<i>MSG</i>	Specify the Administration Message, less then 255 characters
<i>uac</i>	Set URL Access Control part.
<i>wf</i>	Set Web Feature part.

Example

```
> csm ucf obj 1 -n game -l B
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
Action:[pass]
[ ]Prevent web access from IP address.
  No  Obj NO.    Object Name
  ----
  No  Grp NO.    Group Name
  ----
```

Telnet Command: **csm ucf obj INDEX uac**

It means to configure the settings regarding to URL Access Control (uac).

csm ucf obj INDEX uac -v

csm ucf obj INDEX uac -e

csm ucf obj INDEX uac -d

csm ucf obj INDEX uac -a P| B

csm ucf obj INDEX uac -i E| D

csm ucf obj INDEX uac -o KEY_WORD_Object_Index

csm ucf obj INDEX uac -g KEY_WORD_Group_Index

Syntax Description

Parameter	Description
<i>INDEX</i>	Specify the index number of CSM profile, from 1 to 8.
- v	View the protocol configuration of the CSM profile.
-e	Enable the function of URL Access Control.
-d	Disable the function of URL Access Control.
-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.
<i>KEY_WORD_Object_Index</i>	Specify the index number of the object profile.
-g	Set the keyword group.
<i>KEY_WORD_Group_Index</i>	Specify the index number of the group profile.

Example

```
> csm ucf obj 1 uac -i E
Log:[block]
Priority Select : [Either : Url Access Control First]
-----
URL Access Control
[ ]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
Log:[block]
Priority Select : [Either : Url Access Control First]
-----
URL Access Control
[ ]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: **csn ucf obj INDEX wf**

It means to configure the settings regarding to Web Feature (wf).

csn ucf obj INDEX wf -v

csn ucf obj INDEX wf -e

csn ucf obj INDEX wf -d

csn ucf obj INDEX wf -a P|B

csn ucf obj INDEX wf -s WEB_FEATURE

csn ucf obj INDEX wf -u WEB_FEATURE

csn ucf obj INDEX wf -f File_Extension_Object_index

Syntax Description

Parameter	Description
<i>INDEX</i>	Specify the index number of CSM profile, from 1 to 8.
<i>-v</i>	View the protocol configuration of the CSM profile.
<i>-e</i>	Enable the restriction of web feature.
<i>-d</i>	Disable the restriction of web feature.
<i>-a</i>	Set the action of web feature, P or B. B: Block. The web access meets the web feature will be blocked. P: Pass. The web access meets the web feature will be passed.
<i>-s</i>	Enable the the Web Feature configuration. Features available for configuration are: c: Cookie p: Proxy u: Upload
<i>-u</i>	Cancel the web feature configuration.
<i>-f</i>	Set the file extension object index number.
<i>File_Extension_Object_index</i>	Type the index number (1 to 8) for the file extension object.

Example

```
> csn ucf obj 1 wf -s c
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
Action:[block]
[v] Prevent web access from IP address.
  No  Obj NO.    Object Name
---
 
  No  Grp NO.    Group Name
---

[ ]Enable Restrict Web Feature
Action:[pass]
```

File Extension Object Index : [0]	Profile Name : []
[V] Cookie [] Proxy [] Upload	

Telnet Command: csm wcf

It means to configure the settings regarding to web control filter (wcf).

csm wcf show

csm wcf look

csm wcf cache

csm wcf server WCF_SERVER

csm wcf msg MSG

csm wcf setdefault

csm wcf obj INDEX -v

csm wcf obj INDEX -a P| B

csm wcf obj INDEX -n PROFILE_NAME

csm wcf obj INDEX -l N| P| B| A

csm wcf obj INDEX -o KEY_WORD Object Index

csm wcf obj INDEX -g KEY_WORD Group Index

csm wcf obj INDEX -w E| D| P| B

csm wcf obj INDEX -s CATEGORY| WEB_GROUP

csm wcf obj INDEX -u CATEGORY| WEB_GROUP

Syntax Description

Parameter	Description
<i>show</i>	Display the web content filter profiles.
<i>Look</i>	Display the license information of WCF.
<i>Cache</i>	Set the cache level for the profile.
<i>Server WCF_SERVER</i>	Set web content filter server.
<i>Msg MSG</i>	Set the administration message. MSG means the content (less than 255 characters) of the message itself.
<i>setdefault</i>	Return to default settings for all of the profile.
<i>obj</i>	Specify the object profile.
<i>INDEX</i>	Specify the index number of web content filter profile, from 1 to 8.
<i>- v</i>	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>	Set the profile name.
<i>PROFILE_NAME</i>	Specify the name of the profile (less than 16 characters)
<i>-l</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>	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 WCF INDEX
csm dnsf UCF INDEX
csm dnsf cachetime <CACHE_TIME>
csm dnsf blockpage show/ on/ off
csm dnsf profile_show
csm dnsf profile_edit INDEX
csm dnsf profile_edit INDEX -n PROFILE_NAME
csm dnsf profile_edit INDEX -l N| P| B| A
csm dnsf profile_edit INDEX -w WCF_PROFILE
csm dnsf profile_edit INDEX -u UCF_PROFILE
csm dnsf profile_edit INDEX -c CACHE_TIME
```

csm dnsf profile_setdefault

csm dnsf local_bw e/ d/ p/ b/ a/ g/ o/ s/ c

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>WCF INDEX</i>	Specify a WCF profile (1 to 8) 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>UCF INDEX</i>	Specify a UCF profile (1 to 8) as the base of DNS filtering. Type a number to indicate the index number of UCF profile (1 is first profile, 2 is second profile, and so on ...).
<i>cachetime</i> <CACHE_TIME>	CACHE_TIME: It means to set the time for cache to live (available values are 1 to 24; 1 is one hour, 2 is two hours, and so on ...) for DNS filter. OFF is no cache ; AUTO is using TTL from pkt.
<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>-l N P B A</i>	Specify the log type of the profile. P: Pass. B: Block. A: All. N: None.
<i>-w WCF_PROFILE</i>	WCF_PROFILE: 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.
<i>profile_setdefault</i>	Reset to factory default setting.
<i>local_bw e/ d/ p/ b/ a/ g/ o/ s/ c</i>	Set the Black/White List of DNS Filter Local Setting. e: Enable the function of black/white list. d: Disable the function of black/white list. p: Set the action as "Pass". b: Set the action as "Block".

	a <0/1/2/3/4> <value>: Set the address type. 0=mask, 1=single, 2=any, 3=range, 4=group and objects g: item_number group_index: Select the group index (for the address type set with 4, group and objects) item_number=1 or 2 (group 1 or group 2) group_index=1 to 192 o item_number object_index: Select the object index (for the address type set with 4, group and objects) item_number=1 or 2 (object 1 or object 2) object_index=1 to 32 s: Show the config setting. c: Clear the config setting and reset to factory default settings.

Example

```
> csm dnsf profile_edit 1
Profile Index: 1
Profile Name:[]

Log:[block]

WCF Profile Index: 0

UCF Profile Index: 0
> csm dnsf profile_setdefault
setdefault!!!
> csm dnsf profile_setdefault
setdefault!!!
>csm dnsf cachetime 20
dns cache time set up!!!
> csm dnsf local_bw e
Enable the Block and White List.
> csm dnsf local_bw a 1 192.168.1.11
Address Type: 0:mask, 1:single, 2:any, 3:range, 4:object and group
Set the [SINGLE] Address type
> csm dnsf local_bw s
Show Block/White List information for DNS Filter Local Setting
Block/White List:[ENABLE]
Action:[PASS]
Address type:[SINGLE]
Start ip address:[192.168.1.11]
End/Mask ip address:[0.0.0.0]
Group 1:[0]
Group 2:[0]
Object 1:[0]
Object 2:[0]
```

Telnet Command: ddns enable

Enable/disable the DDNS service.

Syntax Description

Parameter	Description
<i>Enable</i> <0/ 1>	Enable or disable DDNS service. 1: enable. 0: disable.

Example

```
> ddns enable 1
Enable Dynamic DNS Setup
```

>

Telnet Command: ddns set

This command allows users to set Dynamica DNS account.

Syntax

ddns set *option* *<value>*

Syntax Description

Parameter	Description
<i>-i <value></i>	It means index number of Dynamic DNS Account. <value>=1-6
<i>-E <value></i>	It means to enable /disable Dynamic DNS Account. <value>=0-1 0: Disable 1: Enable
<i>-W <value></i>	It means to specify WAN Interface. <value>=1-4 1: WAN1 First 2: WAN1 Only 3: WAN2 First 4: WAN2 Only example: To set WAN Interface: WAN1 First
<i>-L <value></i>	It means to type Login Name. [value]: limit up to 64 characters
<i>-P <value></i>	It means to type Password. [value]: limit up to 24 characters
<i>-C <value></i>	It means to enable /disable Wildcards. <value>=0-1 0: Disable 1: Enable
<i>-B <value></i>	It means to enable / disable Backup MX. <value>=0-1 0: Disable 1: Enable
<i>-M <value></i>	It means to type Mail Extender. [value]: limit up to 60 characters
<i>-R <value></i>	It means to type Determine Real WAN IP. <value>=0-1 0: WAN IP, 1: Internet IP
<i>-S <value></i>	It means to specify Service Provider. If user want to set User-Defined page, value must select 1. <value>= 1-19 1: User-Defined 2: 3322 DDNS (www.3322.org) 3: ChangeIP.com (www.changeip.com) 4: ddns.com.cn (www.ddns.com.cn) 5: DtDNS (www.dtdns.com) 6: dyn.com (www.dyn.com) 7: DynAccess (www.dynaccess.com) 8: dynami.co.za (www.dynami.co.za) 9: freedns.afraid.org (freedns.afraid.org) 10: NO-IP.COM Free (www.no-ip.com) 11: opendns.com (www.opendns.com) 12: OVH (www.ovh.com) 13: Strato (www.strato.eu) 14: TwoDNS (www.twodns.de) 15: TZO (www.tzo.com) 16: ubddns.org (ubddns.org) 17: Viettel DDNS (vddns.vn) 18: vigorddns.com (www.vigorddns.com) 19: ZoneEdit DDNS (dynamic.zoneedit.com)

<i>T</i> <value>	It means to type Service Type. <value>= 1-3 1: Dynamic 2: Custom 3: Static
<i>-D</i> <Host Name> <sub Domain Name>	It means to type Domain Name. i.e: Account index 1 setting Domain Name for Dynamic Service Type >> ddns set -i 1 -T 1 -D "host ddns.com.cn" i.e: Account index 2 setting Domain Name for Custom Service Type >> ddns set -i 2 -T 2 -D "domain name" i.e: Account index 3 setting Domain Name for Static Service Type >> ddns set -i 3 -T 3 -D "domain name"
<i>-H</i> <value>	It means to type User-Defined Provider Host. <value>= limit up to 64 characters
<i>-A</i> <value>	It means to type User-Defined Service API. <value>= limit up to 256 characters
<i>-a</i> <value>	It means to type User-Defined Auth Type. <value>=0-1 0: basic 1: URL
<i>-N</i> <value>	It means to type User-Defined Connection Type. <value>=0-1 0: Http 1: Https
<i>-O</i> <value>	It means to type User-Defined Server Response. <value>: limit up to 32 characters

Example

```
> ddns set -i 1 -S 6 -T 1 -D "hostname dnsalias.net" -L user1 -P pwd1
> Save OK
```

Telnet Command: ddns log

Displays the DDNS log.

Example

```
>ddns log
>
```

Telnet Command: ddns time

Sets and displays the DDNS time.

ddns time <update in minutes>

Syntax Description

Parameter	Description
<i>Update in minutes</i>	Type the value as DDNS time. The range is from 1 to 14400.

Example

```
> ddns time
ddns time <update in minutes>
Valid: 1 ~ 14400
%Now: 14400
```

```
> ddns time 1000
ddns time <update in minutes>
Valid: 1 ~ 14400
%Now: 1000
```

Telnet Command: ddns forceupdate

This command will update DDNS automatically.

Example

```
> ddns forceupdate
Now updating DDNS ...
Please check result by using command "ddns log"
```

Telnet Command: ddns setdefault

This command will return DDS with factory default settings.

Example

```
> ddns setdefault
> Set to Factory Default.
```

Telnet Command: ddns show

This command allows users to check the content of selected DDNS account.

Syntax

ddns show -i <value>

Syntax Description

Parameter	Description
-i <value>	Display the content of selected DDNS account by entering the index number of the account. <value>=1-6

Example

```
> ddns show -i 1
-----
Index: 1
[ ] Enable Dynamic DNS Account
WAN Interface: WAN1 First
Service Provider: dyn.com (www.dyn.com)
Service Type: Dynamic
Domain Name: [].[]
Login Name:
[ ] Wildcards
[ ] Backup MX
Mail Extender:
Determine Real WAN IP: WAN IP

>
```

Telnet Command: dos

This command allows users to configure the settings for DoS defense system.

dos [-V | D | A]

dos [-s ATTACK_F [THRESHOLD][TIMEOUT]]

dos [-a | e [ATTACK_F][ATTACK_0] | d [ATTACK_F][ATTACK_0]]

dos -o <LOG_TYPE> | p <LOG_TYPE> | l <LOG_TYPE>

dos -P <add4/ remove4> <type> <value> | <add6/ remove6> <type> <value> | <show> | remove4 all | remove6 all>

dos -B <add4/ remove4> <type> <value> | <add6/ remove6> <type> <value> | <show> | remove4 all | remove6 all>

dos -f <0/ 1/ show>

dos -i <1/ 2/ 3/ 4/ show>

Syntax Description

Parameter	Description
-V	View the configuration of DoS defense system.
-D	Deactivate the DoS defense system.
-A	Activate the DoS defense system.
-s	Enable the defense function for a specific attack and set its parameter(s).
ATTACK_F	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.
TIMEOUT	It means the time (seconds) that a flooding attack will be blocked. Set a value larger than 5.
-a	Enable the defense function for all attacks listed in ATTACK_0.
-e	Enable defense function for a specific attack(s).
ATTACK_0	Specify a name of the following attacks: ip_option, tcp_flag, land, teardrop, smurf, pingofdeath, traceroute, icmp_frag, syn_frag, unknow_proto, fraggle.
-d	Disable the defense function for a specific attack(s).
-P <add4/ remove4> <type> <value> <add6/ remove6> <type> <value> <show> remove4 all remove6 all>	Add or remove the IPv4/IPv6 address in the white passing IP list. add4/remove4: Add /remove an IPv4/IPv6 address to/from the whitelist. add6/remove6: Add/remove an IPv6 address to/from the whitelist. Type: Two types, -i and -c. In which, "-i" means the IPv4 address and "-c" means the country object. Value: Enter the IP address for -i; enter the index number of the country object profile. Show: Display the whitelist.
-B <add4/ remove4> <type> <value> <add6/ remove6> <type> <value> <show> remove4 all remove6 all>	Add or remove the IPv4/IPv6 address in the black blocking IP list. add4/remove4: Add /remove an IPv4/IPv6 address to/from the blacklist. add6/remove6: Add/remove an IPv6 address to/from the blacklist. Type: Two types, -i and -c. In which, "-i" means the IPv4 address and "-c" means the country object. Value: Enter the IP address for -i; enter the index number of the country object profile.

	Show: Display the blacklist.
<i>dos -o <LOG_TYPE></i>	Enable/Disable dos defense log. <LOG_TYPE>: Enter 0 or 1. 0: Disable 1: Enable
<i>dos -p <LOG_TYPE></i>	Enable/Disable spoofing defense log. <LOG_TYPE>: Enter 0 or 1. 0: Disable 1: Enable
<i>dos -l <LOG_TYPE></i>	Enable/Disable dos defense black/white list log. <LOG_TYPE>: Enter 0 to 3. 0: None 1: White list 2: Black List 3: All
<i>dos -f <0/ 1/ show></i>	Set priority of Whitelist/Blacklist. 0:WhiteList 1:BlackList
<i>dos -i <1/ 2/ 3/ 4/ show></i>	Set Whitelist/Blacklist log sending time interval(seconds). 1:30 2:60 3:180 4:300

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>
> dos -P add4 -i 192.168.5.89
Add IP in Passing IP List success.
> dos -P show
DoS White Passing IP List:
      Type      IPv4      Type      IPv6
1. IP      192.168.5.89    IP      ::
2. IP      0.0.0.0        IP      ::
3. IP      0.0.0.0        IP      ::
4. IP      0.0.0.0        IP      ::
..
..
```

Telnet Command: exit

Type this command will leave telnet window.

Telnet Command: Internet

This command allows you to configure detailed settings for WAN connection.

Syntax

internet *-W n -M n [-<command> <parameter> | ...]*

Syntax Description

Parameter	Description

-W n	W means to set WAN interface. 1=WAN1, 2=WAN2,... Default is WAN1.
-M n	M means to set Internet Access Mode (Mandatory) and n means different modes (represented by 0 - 3) n=0: Offline n=1: PPPoE n=2: Dynamic IP n=3: Static IP n=4: PPTP with Dynamic IP, n=5: PPTP with Static IP, n=6: L2TP with Dynamic IP n=7: L2TP with Static IP n=A: 3G/4G USB Modem(PPP mode), n=B: 3G/4G USB Modem(DHCP mode)
<command><parameter>[...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-S <isp name>	Set ISP Name (max. 23 characters).
-P <on/off>	Enable PPPoE Service.
-u <username>	Set username (max. 49 characters) for Internet accessing.
-p <password>	Set password (max. 49 characters) for Internet accessing.
-a n	It means to set PPP Authentication Type and n means different types (represented by 0-1). n=0: PAP/CHAP (this is default setting) n=1: PAP Only
-r <0/ 1>	It means to enable / disable the function of PPPoE pass-through. 0: disable 1: enable
-t n	Set connection duration and n means different conditions. n=-1: Always-on n=1 - 999: Idle time for offline (default 180 seconds)
-i <ip address>	It means that <i>PPPoE server</i> will assign an IP address specified here for CPE (PPPoE client). If you type 0.0.0.0 as the <ip address>, ISP will assign suitable IP address for you. However, if you type an IP address here, the router will use that one as a fixed IP.
-w <ip address>	It means to assign WAN IP address for such connection. Please type an IP address here for WAN port.
-n <netmask>	It means to assign netmask for WAN connection. You have to type 255.255.255.xxx (x is changeable) as the netmask for WAN port.
-g <gateway>	Assign gateway IP for such WAN connection.
-V	View Internet Access profile.
-C <sim pin code>	Set (PPP mode) SIM PIN code (max. 15 characters).
-O <init string>	Set (PPP mode) Modem Initial String (max. 47 characters).
-T <init string2>	Set (PPP mode) Modem Initial String2 (max. 47 characters)
-D <dial string>	Set (PPP mode) Modem Dial String (max. 31 characters).
-v <service name>	Set (PPP mode) Service Name (max. 23 characters).
-m <ppp username>	Set (PPP mode) PPP Username (max. 63 characters).
-o <ppp password>	Set (PPP mode) PPP Password (max. 62 characters).

<i>-e n</i>	Set (PPP mode) PPP Authentication Type. n= 0: PAP/CHAP (default), 1: PAP Only
<i>-q n</i>	(PPP mode) Index(1-15) in Schedule Setup-One
<i>-x n</i>	(PPP mode) Index(1-15) in Schedule Setup-Two
<i>-y n</i>	(PPP mode) Index(1-15) in Schedule Setup-Three
<i>-z n</i>	(PPP mode) Index(1-15) in Schedule Setup-Four
<i>-Q <mode></i>	Set (PPP mode or DHCP mode) WAN Connection Detection Mode. <mode> 0: ARP Detect; 1: Ping Detect
<i>-I <ping ip></i>	Set (PPP mode or DHCP mode) WAN Connection Detection Ping IP. <ping ip>= ppp.qqq.rrr.sss: WAN Connection Detection Ping IP
<i>-L n</i>	Set (PPP mode) WAN Connection Detection TTL (1-255) value.
<i>-R n</i>	Set (PPP mode) WAN Connection Detection Echo Interval secondes. n= 3 to 60.
<i>-E <sim pin code></i>	Set (DHCP mode) SIM PIN code (max. 19 characters).
<i>-G <mode></i>	Set (DHCP mode) Network Mode. <mode> 0: 4G/3G/2G; 1: 4G Only; 2: 3G Only; 3: 2G Only
<i>-N <apn name></i>	Set (DHCP mode) APN Name (max. 47 characters)
<i>-U n</i>	(DHCP mode) MTU(1000-1440)
<i>j <on/off></i>	Enable/disable the separate account for ADSL.
<i>k <username></i>	Set the ADSL account username if the separate account for ADSL is enabled.
<i>l <password></i>	Set the ADSL account password if the separate account for ADSL is enabled.

Example

```
>internet -M 1 -S tcom -u username -p password -a 0 -t -1 -i 0.0.0.0
WAN1 Internet Mode set to PPPoE/PPPoA
WAN1 ISP Name set to tcom
WAN1 Username set to username
WAN1 Password set successful
WAN1 PPP Authentication Type set to PAP/CHAP
WAN1 Idle timeout set to always-on
WAN1 Gateway IP set to 0.0.0.0
> internet -V
WAN1 Internet Mode:PPPoE
ISP Name: tcom
Username: username
Authentication: PAP/CHAP
Idle Timeout: -1
WAN IP: Dynamic IP
> internet -W 1 -M 1 -u link1 -p link1 -a 0
```

```
You are going to watching and setting in WAN 1
WAN1 Internet Mode set to PPPoE/PPPoA
WAN1 Username set to link1
WAN1 Password set successful
WAN1 PPP Authentication Type set to PAP/CHAP
>
```

Telnet Command: ip pubsubnet

This command allows users to enable or disable the IP routing subnet for your router.

Syntax

ip pubsubnet *<Enable/ Disable>*

Syntax Description

Parameter	Description
<i>Enable</i>	Enable the function.
<i>Disable</i>	Disable the function.

Example

```
> ip 2ndsubnet enable
public subnet enabled!
```

Telnet Command: ip pubaddr

This command allows to set the **IP routed subnet** for the router.

Syntax

ip pubaddr ?

ip pubaddr *<public subnet IP address>*

Syntax Description

Parameter	Description
<i>?</i>	Display an IP address which allows users set as the public subnet IP address.
<i>public subnet IP address</i>	Specify an IP address. The system will set the one that you specified as the public subnet IP address.

Example

```
> ip pubaddr ?
% ip addr <public subnet IP address>
% Now: 192.168.0.1

> ip pubaddr 192.168.2.5
% Set public subnet IP address done !!!
```

Telnet Command: ip pubmask

This command allows users to set the mask for IP routed subnet of your router.

Syntax

ip pubmask ?

ip pubmask <public subnet mask>

Syntax Description

Parameter	Description
?	Display an IP address which allows users set as the public subnet mask.
public subnet IP address	Specify a subnet mask. The system will set the one that you specified as the public subnet mask.

Example

```
> ip pubmask ?
% ip pubmask <public subnet mask>
% Now: 255.255.255.0

> ip pubmask 255.255.0.0
% Set public subnet mask done !!!
```

Telnet Command: ip addr

This command allows users to set/add a specified LAN IP your router.

Syntax

ip addr [IP address]

Syntax Description

Parameter	Description
IP address	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 net mask]

Syntax Description

Parameter	Description
<i>IP netmask</i>	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/ 5/ status>

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/ status</i>	0: disable to accept illegal source mac address 1: enable to accept illegal source mac address 2: disable to accept illegal dest mac address 3: enable to accept illegal dest mac address 4: Decline VRRP mac into arp table 5: Accept VRRP mac into arp table status: display the setting status.
<i>Time</i>	Available settings will be 10, 20, 30,...2550 seconds.

Example

```
> ip arp status
[ARP Table]
  Index IP Address      MAC Address      Netbios Name      Interface  VLAN
  Port
    1   192.168.1.5      00-05-5D-E4-D8-EE      LAN1
VLAN0   P1
```

```
>
```

Telnet Command: ip dhcpc

This command is available for WAN DHCP.

Syntax

ip dhcpc *option*

ip dhcpc *option -h/l*

ip dhcpc *option -d [idx]*

ip dhcpc *option -e [1 or 0] -w [wan unumber] -c [option number] -v [option value]*

ip dhcpc *option -e [1 or 0] -w [wan unumber] -c [option number] -x "[option value]"*

ip dhcpc *option -e [1 or 0] -w [wan unumber] -c [option number] -a [option value]*

ip dhcpc *option -u [idx unumber]*

ip dhcpc *release [wan number]*

ip dhcpc *renew [wan number]*

ip dhcpc *status*

Syntax Description

Parameter	Description
<i>option</i>	It is an optional setting for DHCP server. -h: display usage -l: list all custom set DHCP options -d: delete custom dhcp client option by index number -e: enable/disable option feature, 1:enable, 0:disable -w: set WAN number (e.g., 1=WAN1) -c: set option number: 0-255 -v: set option value by string -x: set option value by raw byte (hex) -u: update by index number
<i>release</i>	It means to release current WAN IP address.
<i>renew</i>	It means to renew the WAN IP address and obtain another new one.
<i>status</i>	It displays current status of DHCP client.

Example

```
>ip dhcpc status
I/F#3 DHCP Client Status:

DHCP Server IP      : 172.16.3.7
WAN Ipm             : 172.16.3.40
WAN Netmask         : 255.255.255.0
WAN Gateway         : 172.16.3.1
Primary DNS         : 168.95.192.1
Secondary DNS       : 0.0.0.0
Leased Time         : 259200
Leased Time T1      : 129600
```

Leased Time T2	: 226800
Leased Elapsed	: 259194
Leased Elapsed T1	: 129594
Leased Elapsed T2	: 226794

Telnet Command: ip ping

This command allows users to ping IP address of WAN1/WAN2 for verifying if the WAN connection is OK or not.

Syntax

ip ping [*IP address*] [*AUTO/ WAN1 / WAN2 / PVC3/ PVC4/ PVC5*] [*Source IP address*]

Syntax Description

Parameter	Description
<i>IP address</i>	It means the WAN IP address.
<i>AUTO/ WAN1 / WAN2 / PVC3/ PVC4/ PVC5</i>	It means the WAN interface that the above IP address passes through.

Example

```
>ip ping 172.16.3.229 WAN1
Pinging 172.16.3.229 with 64 bytes of Data:
Receive reply from 172.16.3.229, time=0ms
Receive reply from 172.16.3.229, time=0ms
Receive reply from 172.16.3.229, time=0ms
Packets: Sent = 5, Received = 5, Lost = 0 <0% loss>
```

Telnet Command: ip tracert

This command allows users to trace the routes from the router to the host.

ip tracert [*Host/ IP address*] [*WAN1/ WAN2/ WAN3*] [*Udp/ Icmp*]

Syntax Description

Parameter	Description
<i>IP address</i>	The target IP address.
<i>WAN1/ WAN2/ WAN3</i>	It means the WAN port that the above IP address passes through.
<i>Udp/ Icmp</i>	The UDP or ICMP.

Example

```
>ip tracert 22.128.2.62 WAN1
Traceroute to 22.128.2.62, 30 hops max
1  172.16.3.7  10ms
2  172.16.1.2  10ms
3  Request Time out.
4  168.95.90.6650ms
5  211.22.38.134  50ms
6  220.128.2.6250ms
Trace complete
```

Telnet Command: ip telnet

This command allows users to access specified device by telnet.

Syntax

ip telnet [*IP address*][*Port*]

Syntax Description

Parameter	Description
<i>IP address</i>	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 LAN1 and 2 means IP Routed.

Example

```
> ip rip 1
%% Set RIP LAN1.
```

Telnet Command: ip wanrip

This command allows users to set the RIP (routing information protocol) of WAN IP.

Syntax

ip wanrip [*ifno*] *-e* [*0/ 1*]

Syntax Description

Parameter	Description
<i>ifno</i>	It means the connection interface. 1: WAN1,2: WAN2, 3: PVC3,4: PVC4,5: PVC5 Note: PVC3 -PVC5 are virtual WANs.
<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
> ip wanrip 5 -e 1
> ip wanrip ?
Valid ex:ip wanrip <ifno> -e <0/1>
<ifno> 1: WAN1,2: WAN2
       3: PVC3,4: PVC4,5: PVC5
-e <0/1> 0: disable, 1: enable
Now status:
WAN[1] Rip Protocol disable
WAN[2] Rip Protocol disable
WAN[3] Rip Protocol disable
WAN[4] Rip Protocol disable
WAN[5] Rip Protocol enable
>
```

Telnet Command: ip route

This command allows users to set static route.

Syntax

ip route *add* [*dst*] [*netmask*][*gateway*][*ifno*][*rtype*]

ip route *del* [*dst*] [*netmask*][*rtype*]

ip route *status*

ip route *cnc*

ip route *default* [*wan1/wan2/off/?*]

ip route *clean* [*1/0*]

Syntax Description

Parameter	Description
<i>add</i>	It means to add an IP address as static route.
<i>del</i>	It means to delete specified IP address.
<i>status</i>	It means current status of static route.
<i>dst</i>	It means the IP address of the destination.
<i>netmask</i>	It means the netmask of the specified IP address.
<i>gateway</i>	It means the gateway of the connected router.
<i>ifno</i>	It means the connection interface.

	3=WAN1, 4=WAN2, 5=WAN3, 6=WAN4
<i>rtype</i>	It means the type of the route. default : default route; static: static route.
cnc	It means current IP range for CNC Network.
default	Set WAN1/WAN2/off as current default route.
clean	Clean all of the route settings. 1: Enable the function. 0: Disable the function.

Example

```
> ip route add 172.16.2.0 255.255.255.0 172.16.2.4 3 static
> ip route status
```

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

```
C~      192.168.9.0/    255.255.255.0 is directly connected, DMZ
C~      192.168.1.0/    255.255.255.0 is directly connected, LAN1
S       172.16.2.0/    255.255.255.0 via 172.16.2.4, WAN1
```

Telnet Command: ip igmp_proxy

This command allows users to enable/disable igmp proxy server.

Syntax

ip igmp_proxy set

ip igmp_proxy reset

ip igmp_proxy wan

ip igmp_proxy query

ip igmp_proxy ppp [0/ 1]

ip igmp_proxy status

ip igmp_proxy version [v2/ v3/ auto/ show]

ip igmp_proxy syslog [0/ 1]

Syntax Description

Parameter	Description
<i>set</i>	It means to enable proxy server.
<i>reset</i>	It means to disable proxy server.
<i>wan</i>	It means to specify WAN interface for IGMP service.
<i>query</i>	It means to set IGMP general query interval. The default value is 125000 ms.
<i>ppp</i>	0 - No need to set IGMP with PPP header. 1 - Set IGMP with PPP header.
<i>status</i>	It means to display current status for proxy server.
<i>version <v2/ v3/ auto/ show></i>	It means to set IGMP version fixed on v2 or v3.
<i>syslog [0/ 1]</i>	It means to set IGMP syslog. 0: disable 1: enable

Example

```
> 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
> ip igmp_proxy set
% ip igmp_proxy [set|reset|wan|status], IGMP Proxy is ON
> ip igmp_proxy status
%% ip igmp_proxy [set|reset|wan|status], IGMP Proxy is ON
%%% igmp_proxy WAN:
    239.255.255.250    state=1
    239.255.255.250    timer=0
```

Telnet Command: ip igmp_snoop

This command is used to enable/disable igmp snoop server.

Syntax

ip igmp_snoop enable

ip igmp_snoop disable

ip igmp_snoop status

ip igmp_snoop txquery [on| off] [v2| v3]

ip igmp_snoop chkleave [on| off]

ip igmp_snoop separate [on| off]

ip igmp_snoop acceptlist [type] [index]

Syntax Description

Parameter	Description
<i>enable</i>	It means to enable proxy server.
<i>disable</i>	It means to disable proxy server.
<i>status</i>	It means to display current status for proxy server.
<i>txquery [on off] [v2 v3]</i>	It means to send out IGMP QUERY to LAN periodically. On: enable Off: disable v2: version v2 v3: version v3
<i>chkleave [on off]</i>	It means to check the leave status. On: enable the IGMP snoop leave checking function. Off: it will drop LEAVE if still clients on the same group.
<i>separate [on off]</i>	It means to set IGMP packets being separated by NAT/Bridge. On: The packets will be separated. Off: The packets will not be separated by NAT/Bridge.
<i>acceptlist [type] [index]</i>	It means to set the accept list for IGMP snoop. Type: 1/2/3. In which, 1 means Disable, 1 means IP object, and 2 means IP group. index: 0 means Disable; 0-192 for ip object; 0-32 for ip group.

Example

```
> ip igmp_snoop enable
% ip igmp snooping [enable|disable|status], IGMP Snooping is Enabled.
>
```

Telnet Command: ip igmp_fl

This command is used to enable/disable igmp fast leave.

Syntax

ip igmp_fl enable

ip igmp_fl disable

ip igmp_fl status

Syntax Description

Parameter	Description
<i>enable</i>	Enable IGMP fast leave.
<i>disable</i>	Disable IGMP fast leave.
<i>status</i>	Display current status of IGMP Fast Leave.

Example

```
> ip igmp_fl enable
%% ip igmp_fl [enable|disable|status], IGMP Fast Leave is Enabled.
>
```

Telnet Command: ip session

This command allows users to set maximum session limit number for the specified IP; set message for exceeding session limit and set how many seconds the IP session block works.

ip session on

ip session off

ip session default [num]

ip session default p2p [num]

ip session status

ip session show

ip session timer [num]

ip session [block/unblock][IP]

ip session [add/del][IP1-IP2][num][p2pnum]

Syntax Description

Parameter	Description
<i>on</i>	Turn on session limit for each IP.
<i>off</i>	Turn off session limit for each IP.
<i>default [num]</i>	Set the default number of session num limit.
<i>Default p2p [num]</i>	Set the default number of session num limit for p2p.
<i>status</i>	Display the current settings.
<i>show</i>	Display all session limit settings in the IP range.
<i>timer [num]</i>	Set when the IP session block works. The unit is second.
<i>[block/unblock][IP]</i>	Block/unblock the specified IP address. Block: The IP cannot access Internet through the router. Unblock: The specified IP can access Internet through the router.
<i>add</i>	Add the session limits in an IP range.
<i>del</i>	Delete the session limits in an IP range.
<i>IP1-IP2</i>	It means the range of IP address specified for this command.
<i>num</i>	It means the number of the session limits, e.g., 100.

<i>p2pnum</i>	It means the number of the session limits, e.g., 50 for P2P.

Example

```
> ip session default 100
> ip session add 192.168.1.5-192.168.1.100 100 50
> ip session on
> ip session status

IP range:
  192.168.1.5 - 192.168.1.100 : 100
Current ip session limit is turn on

Current default session number is 100
```

Telnet Command: ip bandwidth

This command allows users to set maximum bandwidth limit number for the specified IP.

ip bandwidth on

ip bandwidth off

ip bandwidth default [tx_rate][rx_rate]

ip bandwidth status

ip bandwidth routing <on/off>

ip bandwidth schedule <s1> <s2> <s3> <s4>

ip bandwidth show

ip bandwidth [add/del] [IP1-IP2][tx][rx][shared]

Syntax Description

Parameter	Description
<i>on</i>	Turn on the IP bandwidth limit.
<i>off</i>	Turn off the IP bandwidth limit.
<i>default [tx_rate][rx_rate]</i>	Set default tx and rx rate of bandwidth limit. The range is from 0 - 65535 Kpbs.
<i>status</i>	Display the current settings.
<i>routing <on/off></i>	It means to apply to IP Routed Subnet. On: apply to Off: not apply to
<i>schedule <s1> <s2> <s3> <s4></i>	It means to set schedule profile (1 to 4). S1 - S4: Up to four profile can be set. Available schedule profiles from 0 to 16.
<i>show</i>	Display all the bandwidth limits settings within the IP range.
<i>add</i>	Add the bandwidth within the IP range.
<i>del</i>	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>	Set transmission rate for bandwidth limit.
<i>rx</i>	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 dataflowmonitor

This command allows users to set data flow monitor.

Syntax

ip dataflowmonitor *on*

ip dataflowmonitor *off*

ip dataflowmonitor *status*

Syntax Description

Parameter	Description
<i>on</i>	It means to enable the Data Flow Monitor function.
<i>off</i>	It means to disable the Data Flow Monitor function.
<i>show</i>	It means to display current status of Data Flow Monitor function.

Example

```
> ip dataflowmonitor status
Data Flow Monitor: Off
```

Telnet Command: ip bindmac

This command allows users to set IP-MAC binding for LAN host.

ip bindmac *on*

ip bindmac *off*

ip bindmac *strict_on*

ip bindmac *strict_off*

ip bindmac *subnet* <all/ set LAN_Index/ unset LAN_Index/ clear/ show>

ip bindmac *add* <IP><MAC><omment>

ip bindmac *del* <IP/ all>

ip bindmac *show*

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>strict_off</i>	It means to turn off the IP bindmac policy.
<i>subnet <all/ set LAN_Index/ unset LAN_Index/ clear/ show></i>	It means to set LAN subnet to bind strict mode.
<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 Enter the IP address for binding with specified MAC address.
<i>MAC</i>	It means to Enter 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/ do main]	Specify the destination IP mode. Any: No need to specify an IP address for any IP address will be treated as destination IP address. ip_range: Indicates a range of IP addresses. ip_subnet: Indicates the IP subnet. domain: Indicates the domain name.
-3 [any/ range]	Specify the destination port mode. Range: Indicate a range of port number.

	Any: It means any port number can be used as destination port.
-G [default/ specific]	Specify the gateway mode.
-L [default/ specific]	Specify the failover gateway mode.
-s [value]	Indicate the source IP start. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.1.0)
-S [value]	Indicate the source IP end. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.1.100)
-d [value]	Indicate the destination IP start. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.2.0)
-D [value]	Indicate the destination IP end. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.2.100)
-p [value]	Indicate the destination port start. Value: Type a number (1 ~ 65535) as the port start (e.g., 1000).
-P [value]	Indicate the destination port end. Value: Type a number (1 ~ 65535) as the port end (e.g., 2000).
-y [value]	Indicate the priority of the policy route profile. Value: Type a number (0 ~ 250). The default value is “150”.
-I [value]	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
-g [value]	Indicate the gateway IP address. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.3.1)
-I [value]	Indicate the failover IP address. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.4.1)
-t [value]	It means “protocol”. Value: Available settings include “TCP”, “UDP”, “TCP/UDP”, “ICMP” and “Any”.
-n [0/ 1]	Indicates the function of “Force NAT”. 0: Disable the function. 1: Enable the function.
-a [0/ 1]	Indicates to enable the function of failover. 0: Disable the function. 1: Enable the function.
-f [value]	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
-b [value]	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	
-s [value]	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).
-d [value]	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.
-p [value]	It means “destination port”. Value: Specify a number or type Any (indicating any number).
-t [value]	It means “protocol”. Value: Available settings include “ICMP”, “TCP”, “UDP” and “Any”.

Example

```
> ip policy_rt diagnose -s 192.168.1.100 -d any -p any -t ICMP

-----
      Matched Route  (Priority)
-----
* No_Match

-----
      Matched Policy (Priority)
-----
* Policy_1 (200)

* Conclusion:The packet was dropped because the send-to interface
of the mat
ched policy "policy 1" was inactive and there was no failover setting
> ip policy_rt -i -1 -o add -1 range -s 192.168.1.10 -S 192.168.1.20 -2
ip_range -d 202.211.100.10 -D 202.211.100.20 -g 202.211.100.1 -I WAN2
```

Telnet Command: ip lanDNSRes

This command is used to set LAN DNS profiles. With such feature, the user can configure some services (such as ftp, www or database) with domain name which is easy to be accessed.

Syntax

ip lanDNSRes [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
[<command> <parameter> ..]	The available commands with parameters are listed below. [..] means that you can type in several commands in one line.
-a <IP Address>	It is used to configure IP address mapping (IPv4/IPv6 Address or multiple subnet addresses). IP Address: type the IP address (e.g., 192.168.1.56).

-c <CNAME>	It is used to set CNAME. CNAME: Enter a string.
-d <address mapping index number>	It means to delete index number with address mapping configured. address mapping index number : type the index number which represents the address mapping profile.
-e <0/ 1>	It means to enable or disable the function of LAN DNS or DNS Forwarding Profile. 0: disable 1: enable
-i <profile setting index number>	It means to create LAN DNS profile with specified domain name. profile setting index number : type the index number which represents the profile with domain name configured.
-l	It means to list detailed information of profile configuration. > ip lanDNSRes -l % % Idx: 7 % State: Enable % Profile: DrayTekFTP % Domain Name: ftp.draytek.com % ----- Address Mapping Table ----- % Idx ReplyOnlySameSubnet IP Address % 1 Yes 172.16.2.10 % 2 Yes 172.16.3.10 % 3 Yes 172.16.4.10
-n <domain name>	Set domain name.
-p <profile name>	Set profile name for LAN DNS.
-r	Reset the settings for selected profile.
-R	It means to set to factory default setting.
-s <0/1>	0:reply all 1:reply only same subnet packet
-z	update LAN DNS config to DNS Cache

Example

```

> ip lanDNSRes -i 1 -n ftp.drayTek.com
% Configure Set1's DomainName:ftp.drayTek.com
> ip lanDNSRes -i 1 -a 172.16.2.10 -s 1
% Configure Set1's IP:172.16.2.10
% Configure Set1's Idx:1 ReplyOnlySameSubnet:Yes
> ip lanDNSRes -i 1 -a 172.16.3.10 -s 1
% Configure Set1's IP:172.16.3.10
% Configure Set1's Idx:2 ReplyOnlySameSubnet:Yes
> ip lanDNSRes -i 1 -a 172.16.4.10 -s 1
% Configure Set1's IP:172.16.4.10
% Configure Set1's Idx:3 ReplyOnlySameSubnet:Yes
> ip lanDNSRes -l
% Idx: 7
% State: Enable
% Profile: DrayTekFTP
% Domain Name: ftp.draytek.com
% ----- Address Mapping Table -----
% Idx ReplyOnlySameSubnet IP Address
% 1 Yes 172.16.2.10
% 2 Yes 172.16.3.10
% 3 Yes 172.16.4.10

```


>

Telnet Command: ip dnsforward

This command is used to set LAN DNS profile for conditional DNS forwarding.

ip dnsforward [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-a <IP Address/ Domain Name>	Set forwarded DNS server IP Address or domain name. <IP Address/Domain Name>: Enter an IP address or the domain name.
-d <DNS server mapping index number>	Delete the selected LAN DNS profile. <DNS server mapping index number>: Enter the index number.
-e <0/ 1>	0: disable such function. 1: enable such function.
-i <profile setting index number>	Type the index number of the profile. <profile setting index number>: Enter the index number.
-l	List the content of LAN DNS profile (including domain name, IP address and message).
-n <domain name>	Set domain name.
-p <profile name>	Set profile name for LAN DNS.
-r	Reset the settings for selected profile.

Example

```
> ip dnsforward -i 1 -n ftp.drayTek.com
% Configure Set1's DomainName:ftp.drayTek.com
> ip dnsforward -i 1 -a 172.16.1.1
% Configure Set1's IP:172.16.1.1
> ip dnsforward -i 1 -l
% Idx: 1
% State: Disable
% Profile: test
% Domain Name: ftp.drayTek.com
% DNS Server IP: 172.16.1.1
>
```

Telnet Command: ip spoofdef

This command is used to enable/disable the IP Spoofing Defense.

Syntax

ip spoofdef <WAN/ LAN><0/ 1>

Syntax Description

Parameter	Description
<WAN/ LAN>	It means to block IP packet from WAN/LAN with inconsistent source IP address.

<0/ 1>	0: Disable the function. 1: Enable the funciton.

Example

```
> ip spoofdef WAN 1
Setting saved:
>
```

Telnet Command: ip6 addr

This command allows users to set the IPv6 address for your router.

Syntax

```
ip6 addr -s <prefix> <prefix-length> <LAN1/ .. LAN4/ WAN1/ WAN2/ USB/ VPN1/ .. VPN32>
ip6 addr -d <prefix> <prefix-length> <LAN1/ .. LAN4/ WAN1/ WAN2/ USB/ VPN1/ .. VPN32>
ip6 addr -a <LAN1/ .. LAN4/ WAN1/ WAN2/ USB/ VPN1/ .. VPN32> -u
ip6 addr -v <LAN1/ .. LAN4/ WAN1/ WAN2/ USB>
ip6 addr -t <old-prefix> <old-prefix-length> <new-prefix> <new-prefix-length>
< LAN1/ .. LAN4/ WAN1/ WAN2/ USB>
ip6 addr -o <1/ 2>
ip6 addr -o 3 <prefix> <prefix-length> <WAN1/ WAN2/ USB>
ip6 addr -l <prefix> <prefix-length> <LAN1/ .. LAN8>
ip6 addr <-p/ -b> <prefix> <prefix-length> <WAN1/ WAN2/ USB>
ip6 addr -x <LAN1/ .. LAN4>
ip6 addr -c <LAN1/ .. LAN4>
ip6 addr -e <type> < LAN1/ .. LAN4>
```

Syntax Description

Parameter	Description
-s <prefix> <prefix-length> <LAN1/ .. LAN4/ WAN1/ WAN2/ USB/ VPN1/ .. V PN32>	It means to add a static ipv6 address. <prefix>: It means to enter the prefix number of IPv6 address. <prefix-length>: It means to enter a fixed value as the length of the prefix. <LAN1/ .. LAN4/ WAN1/ WAN2/ USB/ VPN1/ .. VPN32>: It means to specify LAN/WAN/USB/VPN interface for such address.
-d <prefix> <prefix-length> <LAN1/ .. LAN4/ WAN1/ WAN2/ USB/ VPN1/ .. V PN32>	It means to delete an ipv6 address. <prefix>: It means to enter the prefix number of IPv6 address. <prefix-length>: It means to enter a fixed value as the length of the prefix. < LAN1/ .. LAN4/ WAN1/ WAN2/ USB/ VPN1/ .. VPN32>: It means to specify LAN/WAN/USB/VPN interface for such address.
-a <LAN1/ .. LAN4/ WAN1/ WAN2/ USB/ VPN1/ .. V PN32> -u	It means to show current address(es) status. <LAN1/ .. LAN4/ WAN1/ WAN2/ USB/ VPN1/ .. VPN32>: It means to specify LAN/WAN/USB/VPN interface. <-u>: It means to show unicast address only.
-v <LAN1/ .. LAN4/ WAN1/ WAN2/ USB>	It means to show prefix list status.
-t <old-prefix> <old-prefix-leng th> <new-prefix>	It means to update WAN static IPv6 address table. <old-prefix>: It means to enter the prefix number of IPv6 address.

<code><new-prefix-length></code> <code>< LAN1/ ..LAN4/</code> <code>WAN1/ WAN2/ USB></code>	<code><old prefix-length></code> : It means to enter a fixed value as the length of the prefix. <code><new-prefix></code> : It means to enter the prefix number of IPv6 address. <code><new-prefix-length></code> : It means to enter a fixed value as the length of the prefix. <code><LAN1/..LAN4/WAN1/WAN2/USB></code> : It means to specify LAN/WAN/USB interface for such address.
<code>-o <1/ 2></code>	<code><1></code> : It means to show old prefix list. <code><2></code> : It means to send old prefix option by RA.
<code>-o <3> <prefix></code> <code><prefix-length></code> <code><WAN1/ WAN2/ USB></code>	<code><3></code> : It means to set old prefix. <code><prefix></code> : It means to enter the prefix number of IPv6 address. <code><prefix-length></code> : It means to enter a fixed value as the length of the prefix. <code><WAN1/WAN2/USB></code> : It means to specify a WAN/USB interface for such address.
<code>-l <prefix> <prefix-length> <</code> <code>LAN1/ ..LAN4></code>	It means to add a ULA. <code><prefix></code> : It means to enter the prefix number of IPv6 address. <code><prefix-length></code> : It means to enter a fixed value as the length of the prefix. <code><LAN1/..LAN4></code> : It means to specify a LAN interface for such address.
<code>-p/ -b <prefix></code> <code><prefix-length></code> <code><WAN1/ WAN2/ USB></code>	It means to add/delete an prefix to/from prefix list. p: Add a prefix to a prefix list. b: Delete a prefix from a prefix list. <code><prefix></code> : It means to enter the prefix number of IPv6 address. <code><prefix-length></code> : It means to enter a fixed value as the length of the prefix. <code><WAN1/WAN2/USB></code> : It means to specify a WAN/USB interface for such address.
<code>-x <LAN1/ ..LAN4></code>	It means to generate a ULA automatically. <code><LAN1/..LAN4></code> : It means to specify a LAN interface.
<code>-c <LAN1/ ..LAN4></code>	It means to delete a ULA . <code><LAN1/..LAN4></code> : It means to specify a LAN interface.
<code>-e <type> <LAN1/ ..LAN4></code>	It means to set ULA type. <code><type></code> : 0, disable; 1, static; 2, auto <code><LAN1/..LAN4></code> : It means to specify a LAN interface.

Example

```

> ip6 addr -a
LAN
Unicast Address:
FE80::250:7FFF:FE00:0/64 (Link)
Multicast Address:
FF02::2
FF02::1:FF00:0
FF02::1

```

Telnet Command: ip6 dhcp req_opt

This command is used to configure option-request settings for DHCPv6 client.

ip6 dhcp req_opt `<LAN1/ .../ LAN4/ WAN1/ WAN2/ USB>` [`-<command>` `<parameter>` | ...]

Syntax Description

Parameter	Description
<i>req_opt</i>	It means option-request.
<i>LAN1 ... LAN4 WAN1 WAN2 USB</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>-l</i>	It means to ask NIS name.
<i>-p</i>	It means to ask NISP.
<i>-P</i>	It means to ask NISP name.
<i>-b</i>	It means to ask BCMCS.
<i>-B</i>	It means to ask BCMCS name.
<i>-r</i>	It means to ask refresh time.
<i>Parameter</i>	1: the parameter related to the request will be displayed. 0: the parameter related to the request will not be displayed.

Example

```
> ip6 dhcp req_opt WAN2 -S 1
> ip6 dhcp req_opt WAN2 -r 1
> ip6 dhcp req_opt WAN2 -a
% Interface WAN2 is set to request following DHCPv6 options:
%   sip name
>
```

Telnet Command: ip6 dhcp client

This command allows you to use DHCPv6 protocol to obtain IPv6 address from server.

ip6 dhcp client <WAN1| WAN2| USB> [-<command> <parameter>| ...]

Syntax Description

Parameter	Description
<i>client</i>	It means the dhcp client settings.
<i>[<command> <parameter> ...]</i>	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
<i>-a</i>	It means to show current DHCPv6 status.
<i>-p <IAID></i>	It means to request identity association ID for Prefix Delegation.
<i>-n <IAID></i>	It means to request identity association ID for Non-temporary Address.

<code>-t <time></code>	It means to set solicit interval. <time>: 0 ~ 7 seconds (default value is 0).
<code>-c <parameter></code>	It means to send rapid commit to server. 1: Enable 0: Disable
<code>-i <parameter></code>	It means to send information request to server. 1: Enable 0: Disable
<code>-e <parameter></code>	It means to enable or disable the DHCPv6 client. 1: Enable 0: Disable
<code>-m <parameter></code>	It means to enable/disable server DUID set by Link layer and time. 1: Enable 0: Disable
<code>-d</code>	It means to display the client DUID.
<code>-A <parameter></code>	It means to set authentication protocol. 0: Undefine 2: delayed protocol
<code>-R <parameter></code>	It means to set realm value (max: 31 characters) in delayed protocol. <parameter>: Enter a string.
<code>-S <parameter></code>	It means to set shared secret (max: 31 characters) in delayed protocol. <parameter>: Enter a string.
<code>-K <parameter></code>	It means to set key ID (1~65535) in delayed protocol. <parameter>: Enter a number.

Example

```
> ip6 dhcp client WAN2 -p

This setting will take effect after rebooting.

Please use "sys reboot" command to reboot the router.
```

Telnet Command: ip6 dhcp server

This command allows you to configure DHCPv6 server.

ip6 dhcp server [`-<command>` `<parameter>`]/ ...]

Syntax Description

Parameter	Description
<code>server</code>	It means the dhcp server settings.
<code>[<command> <parameter> ...]</code>	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
<code>-a</code>	It means to show current DHCPv6 status.
<code>-b</code>	It means to show current DHCPv6 IP assignment table.
<code>-n <name></code>	It means to set a pool name.
<code>-c <parameter></code>	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
-t <time>	It means to set prefer lifetime.
-y <time>	It means to set valid lifetime.
-u <time>	It means to set T1 time.
-o <time>	It means to set T2 time.
-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.
-R	It means to send reconfigure packet to the client.
-r <0/ 1>	It means to disable (0) or enable (1) the auto range.
-N <0/ 1>	It means to disable (0) or enable (1) the random address allocation.
-d <addr>	It means to set the first DNS IPv6 address. <addr> : Enter an IPv6 address.
-D <addr>	It means to set the second DNS IPv6 address. <addr> : Enter an IPv6 address.
-m <1/ 0>	It means to enable(1) or disable (0) the server DUID set by Link Layer and Time.
-q <name>	It means to set DNS domain search list. <name>: Enter a name.
-z <0/ 1>	It means to disable (0) or enable (1) the DHCP PD.
pdadd <suffix> <prefix_len> <client linklocal><client DUID>	It means to add PD node.
pddel <PD index>	It means to delete PD node. <PD index>: Enter a number.
-A <parameter>	It means to set authentication protocol. <parameter>: Enter 0, 2 or 3. 0: Undefine 2: delayed protocol 3: Reconfigure key
-M <parameter>	It means to set realm value (max: 31 characters) in delayed protocol. <parameter>: Enter a string.
-S <parameter>	It means to set shared secret (max: 31 characters) in delayed protocol. <parameter>: Enter a string.
-K <parameter>	It means to set key ID (1-65535) in delayed protocol. <parameter>: Enter a number.

Example

```
> ip6 dhcp server LAN1 pdadd 11:22:33 64 fe80::e202:1bff:fe65:4084
000100011d2ce39a00e06f25c839
%      Add to PD list success!
%% PD status : invalid, no prefix available.
```

Telnet Command: ip6 internet

This command allows you to configure settings for accessing Internet.

Syntax

ip6 internet *-W n -M n [-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
<i>-W n</i>	W means to set WAN interface and n means different selections. Default is WAN1. n=1: WAN1 n=2: WAN2 n=3: WAN3 . . n=X: WANx
<i>-M n</i>	M means to set Internet Access Mode (Mandatory) and n means different modes (represented by 0 - 5) n= 0: Offline, n=1: PPP, n=2: TSPC, n=3: AICCU, n=4: DHCPv6, n=5: Static n=6: 6in4-Static n=7: 6rd
<i>[<command> <parameter> ...]</i>	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
<i>For 6rd</i>	
<i>-C n</i>	Set 6rd Connection Mode. n = 0: Auto n = 1: Static.
<i>-s [server]</i>	Set 6rd IPv4 Border Relay. server= IPv4 address
<i>-m n</i>	Set 6rd IPv4 address mask length. n=1 to 32.
<i>-p [prefix]</i>	Set 6rd IPv6 prefix. prefix= IPv6 address
<i>-l n</i>	Set 6rd IPv6 prefix length. n=1 to 64.
<i>For 6in4</i>	
<i>-s [server]</i>	Set 6in4 Remote Endpoint IPv4 Address. server= IPv4 address
<i>-l [IPv6 Addr]</i>	Set 6in4 IPv6 Address. IPv6 Addr= IPv6 address.
<i>-P n</i>	Set 6in4 IPv6 WAN prefix length. n=1 to 64. (Default number is 64)
<i>-p [prefix]</i>	Set 6in4 LAN Routed Prefix. prefix= IPv6 address
<i>-l n</i>	Set 6in4 LAN Routed Prefix length. n=1 to 64. (Default number is 64)

-T n	Set 6in4 Tunnel TTL. n=1 to 255. (Default number is 255)
<i>For TSPC/ AICCU</i>	
-u [username]	Set Username (max. 63 characters).
-P [password]	Set Password (max. 63 characters).
-s [server]	Set Tunnel Server IP. server= IPv4 Address or URL (max. 63 characters).
<i>For AICCU</i>	
-p [prefix]	Set Subnet Prefix (AICCU). prefix=IPv6 address.
-l n	Subnet Prefix length (AICCU) n=1 to 64. (Default number is 64).
-o [0/ 1]	Set AICCU always on. On = 1, Off = 0.
-f [Tunnel ID]	Set AICCU tunnel ID. Tunnel ID= the number (e.g., T345678) offered by tunnel broker.
<i>For Static</i>	
-w [addr]	Set Default Gateway. Addr= IPv6 address.
<i>For others</i>	
-d <server>	Set 1st DNS Server IP server= IPv6 Address.
-D <server>	Set 2nd DNS Server IP. server= IPv6 Address.
-t <dhcp/ ra/ none>	Set ipv6 PPP WAN test mode for DHCP or RA.
-V	View IPv6 Internet Access Profile.
-k	Dial the Tunnel on the WAN.
-j	Drop the Tunnel on the WAN.
-r n	Set Prefix State Machine RA timeout. n=any value (default is 15), (unit: second)
-c n	Set Prefix State Machine DHCPv6 Client timeout. n=any value (default is 15), (unit: second)
-q [value]	Set WAN detection mode. 0: NS Detect. 1: Ping Detect. 2: Always On.
-z [value]	Set Ping Detect TTL. value= 0 ~ 255.
-x [host name/ IPv6 address]	Set Ping Detect Host (hostname or IPv6 address).
-I [interval]	Set ipv6 connection interval. Interval = 1500-60000 (unit:10ms).
-b [0/ 1]	Enable DNSv6 based on DHCPv6. 0= off 1= on

Example


```
> ip6 internet -W 1 -M 2 -u userid -p passwd -s broker.freenet6.net
This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
>
```

Telnet Command: ip6 neigh

This command allows you to display IPv6 neighbour table.

Syntax

ip6 neigh -s [*inet6_addr*] [*eth_addr*] [*LAN1/ LAN2/ .../ LAN4/ WAN1/ WAN2/ USB*]

ip6 neigh -d [*inet6_addr*] [*LAN1/ LAN2/ .../ LAN4/ WAN1/ WAN2/ USB*]

ip6 neigh -a [*inet6_addr*] [-N *LAN1/ LAN2/ .../ LAN4/ WAN1/ WAN2/ USB*]

Syntax Description

Parameter	Description
-s < <i>inet6_addr</i> > < <i>eth_addr</i> > < <i>LAN1/ ..LAN4/ WAN1/ WAN2/ USB</i> >	It means to add a neighbour. < <i>inet6_addr</i> >: Enter an IPv6 address. < <i>eth_addr</i> >: Enter a submask address. < <i>LAN1/ ..LAN4/ WAN1/ WAN2/ USB</i> >: Specify an interface for the neighbor.
-d < <i>inet6_addr</i> > < <i>LAN1/ ..LAN4/ WAN1/ WAN2/ USB</i> >	It means to delete a neighbour. < <i>inet6_addr</i> >: Enter an IPv6 address. < <i>LAN1/ ..LAN4/ WAN1/ WAN2/ USB</i> >: Specify an interface for the neighbor.
-a < <i>inet6_addr</i> > <-N <i>LAN1/ ..LAN4/ WAN1/ WAN2/ USB</i> >	It means to show neighbour status. < <i>inet6_addr</i> >: Enter an IPv6 address. < <i>LAN1/ ..LAN4/ WAN1/ WAN2/ USB</i> >: Specify an interface for the neighbor.

Example

```
> ip6 neigh -s 2001:2222:3333::1111 00:50:7F:11:ac:22:LAN2
% Neighbour 2001:2222:3333::1111 successfully added!
> ip6 neigh -a
```

I/F	ADDR	MAC	STATE
LAN1	2001:2222:3333::1111		FAILED
LAN1	::		NONE
>			NONE

Telnet Command: ip6 pneighbor

This command allows you to add a proxy neighbour.

Syntax

ip6 pneighbor -s *inet6_addr* [*LAN1*| *LAN2*| ...| *LAN4*| *WAN1*| *WAN2*| *USB*]

ip6 pneighbor -d *inet6_addr* [*LAN1*| *LAN2*| ...| *LAN4*| *WAN1*| *WAN2*| *USB*]

ip6 pneighbor -a [*inet6_addr*] [-N *LAN1*| *LAN2*| ...| *LAN4*| *WAN1*| *WAN2*| *USB*]

Syntax Description

Parameter	Description
-s < <i>inet6_addr</i> > < <i>LAN1</i> /.. <i>LAN4</i> <i>WAN1</i> / <i>WAN2</i> / <i>USB</i> >	It means to add a proxy neighbour. < <i>inet6_addr</i> >: Enter an IPv6 address. < <i>LAN1</i> /.. <i>LAN4</i> <i>WAN1</i> / <i>WAN2</i> / <i>USB</i> >: Specify an interface for the proxy neighbor.
-d < <i>inet6_addr</i> > < <i>LAN1</i> /.. <i>LAN4</i> <i>WAN1</i> / <i>WAN2</i> / <i>USB</i> >	It means to delete a proxy neighbour. < <i>inet6_addr</i> >: Enter an IPv6 address. < <i>LAN1</i> /.. <i>LAN4</i> <i>WAN1</i> / <i>WAN2</i> / <i>USB</i> >: Specify an interface for the proxy neighbor.
-a < <i>inet6_addr</i> > < <i>LAN1</i> /.. <i>LAN4</i> <i>WAN1</i> / <i>WAN2</i> / <i>USB</i> >	It means to show proxy neighbour status. < <i>inet6_addr</i> >: Enter an IPv6 address. < <i>LAN1</i> /.. <i>LAN4</i> <i>WAN1</i> / <i>WAN2</i> / <i>USB</i> >: 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 IPv6 route policy.

Syntax

ip6 route -s <*prefix*> <*prefix-length*> <*gateway*> <*LAN1*| *LAN2*| ...| *LAN4*| *WAN1*| *WAN2*| *USB*| *VPN1*| ...| *VPN32*> [-D]

ip6 route -d <*prefix*> <*prefix-length*>

ip6 route -a <*LAN1*| *LAN2*| ...| *LAN4*| *WAN1*| *WAN2*| *USB*| *VPN1*| ...| *VPN32*>]

Syntax Description

Parameter	Description
-s < <i>prefix</i> > < <i>prefix-length</i> > < <i>gateway</i> > < <i>LAN1</i> /.. <i>LAN4</i> / <i>WAN1</i> / <i>WAN2</i> / <i>USB</i> / <i>VPN1</i> /.. <i>VPN32</i> > <-D>	It means to add a route. < <i>prefix</i> >: It means to enter the prefix number of IPv6 address. < <i>prefix length</i> >: It means to enter a fixed value as the length of the prefix. < <i>gateway</i> >: It means to enter the gateway of the router. < <i>LAN1</i> /.. <i>LAN4</i> / <i>WAN1</i> / <i>WAN2</i> / <i>USB</i> / <i>VPN1</i> /.. <i>VPN32</i> >: It means to specify LAN or WAN or VPN interface for such address. <-D>: It means that such route will be treated as the default route.

<code>-d <prefix> <prefix-length></code>	It means to delete a route. <prefix>: It means to enter the prefix number of IPv6 address. <prefix length>: It means to enter a fixed value as the length of the prefix.
<code>-a <LAN1/..LAN4/ WAN1/ WAN2/ USB/ VPN1/..VPN32></code>	It means to show the route status. <LAN1/..LAN4/WAN1/WAN2/USB/VPN1/..VPN32>: It means to specify LAN or WAN or VPN interface for such address.
<code>-/</code>	It means to clear the routing table.

Example

```
> ip6 route -s FE80::250:7FFF:FE12:500 16 FE80::250:7FFF:FE12:100 LAN1
%      Route FE80::250:7FFF:FE12:500/16 successfully added!
> ip6 route -a LAN1

PREFIX/PREFIX-LEN                                I/F METRIC FLAG NEXT-HOP
-----
::0.0.0.1/128                                    LAN1      0 U  ::
FE80::/128                                        LAN1      0 U  ::
FE80::21D:AAFF:FE15:B0C8/128                     LAN1      0 U  ::
FE80::/64                                         LAN1    256 U  ::
FE80::/16                                         LAN1   1024 UGS FE80::250:7FFF:FE12:100
FF00::/8                                          LAN1    256 U  ::
>
```

Telnet Command: ip6 ping

This command allows you to pin an IPv6 address or a host.

Syntax

ip6 ping [*IPv6 address/ Host*] [*LAN1/ LAN2/ .../ LAN4/ WAN1/ WAN2/ USB*][*send count*]
[*data_size*]

Syntax Description

Parameter	Description
<i>IPv6 address/ Host</i>	It means to specify the IPv6 address or host for ping.
<i>LAN1/ LAN2/ .../ LAN4/ WAN1 / WAN2/ USB</i>	It means to specify LAN or WAN interface for such address.

Example

```
> ip6 ping 2001:4860:4860::8888 WAN2

Pinging 2001:4860:4860::8888 with 64 bytes of Data:

Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms

Packets: Sent = 5, Received = 5, Lost = 0 <% loss>
```

```
>
```

Telnet Command: ip6 tracert

This command allows you to trace the routes from the router to the host.

ip6 tracert [*IPv6 address/ Host*] [*LAN1/ LAN2/ .../ LAN4/ WAN1/ WAN2/ USB*]

Syntax Description

Parameter	Description
<i>IPv6 address/ Host</i>	It means to specify the IPv6 address or host for ping.
<i>LAN1/ LAN2/ .../ LAN4/ WAN1 / WAN2/ USB</i>	It means to specify LAN or WAN interface for such address.

Example

```
> ip6 tracert 2001:4860:4860::8888
traceroute to 2001:4860:4860::8888, 30 hops max through protocol ICMP
 1 2001:5C0:1400:B::10B8      340 ms
 2 2001:4DE0:1000:A22::1      330 ms
 3 2001:4DE0:A::1             330 ms
 4 2001:4DE0:1000:34::1       340 ms
 5 2001:7F8:1: :A501:5169:1   330 ms
 6 2001:4860::1:0:4B3         350 ms
 7 2001:4860::8:0:2DAF        330 ms
 8 2001:4860::2:0:66E        340 ms
 9 Request timed out.         *
10 2001:4860:4860::8888      350 ms
Trace complete.
>
```

Telnet Command: ip6 tspc

This command allows you to display TSPC status.

Syntax

ip6 tspc [*ifno*]

Syntax Description

Parameter	Description
<i>ifno</i>	It means the connection interface. Ifno=1 (means WAN1) Info=2 (means WAN2) ... etc.

Example

```
> ip6 tspc 2
Local Endpoint v4 Address : 111.243.177.223
Local Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b9
Router DNS name : 88866666.broker.freenet6.net
Remote Endpoint v4 Address :81.171.72.11
Remote Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b8
Tspc Prefixlen : 56
```

```
Tunnel Broker: Amsterdam.freenet.net

Status: Connected

>
```

Telnet Command: ip6 radvd

This command allows you to enable or disable RADVD server.

Syntax

ip6 radvd [*LAN1*| *LAN2*| ...| *LAN4*] [-<command> <parameter>| ...]

ip6 radvd [*R*| *u*]

Syntax Description

Parameter	Description
<i>LAN1</i> <i>LAN2</i> ... <i>LAN4</i>	It means to specify LAN interface for such address.
<command> <parameter>	
-s	It means to enable or disable the default lifetime of the RADVD server. 1: Enable the RADVD server. 0: Disable the RADVD server.
-D <1/0>	Enable/Disable the RDNSS.
-d <lifetime>	Set the default lifetime for RADVD server.
-i <lifetime>	Set the minimum interval time(sec) for RADVD server.
-I <lifetime>	Set the maximum interval time(sec) for RADVD server.
-h <hoplimit>	Set hop limit for RADVD server.
-m <mtu/ auto>	Set MTU value for RADVD server. Range: 1280-1500. auto - auto select MTU from WAN.
-e <time>	Set reachable time.
-a <time/infinity>	Set retransmit timer /infinity.
-p <0/ 1/ 2>	Set default preference Low/Medium/High for RADVD server.
-v	View the RADVD server configuration.
-V	It means to show the RADVD configuration.
-L <time/infinity>:	Set prefix valid lifetime.
-P <time/infinity>	Set prefix preferred lifetime.
-r [num]	Make RADVD test for item [num]. num - 0-default, 121:logo 121, 124:logo 124.
-R	Reload Config and send RA for subnets.
-u	View MTU on all interfaces.

Example

```
> ip6 radvd LAN1 -s 1
% [LAN1] setting !
% Enable LAN1 radvd OK!
This setting will take effect after rebooting.
```

```

Please use "sys reboot" command to reboot the router.
> ip6 radvd LAN1 -d 1800
% [LAN1] setting !
%   Set default lifetime ok: 1800 !
> ip6 radvd LAN1 -V
% [LAN1] setting !
%   Default Lifetime      : 0 seconds
%   min interval time    : 200 seconds
%   MAX interval time    : 600 seconds
%   Hop limit            : 64
%   MTU                  : 1280
%   Reachable time       : 0
%   Retransmit time      : 0
%   Preference           : Medium

```

Telnet Command: ip6 mngt

This command allows you to manage the settings for access list.

ip6 mngt list

ip6 mngt list [*add* <IP/ Hostname> <NO.> <Index> | *remove* <NO.>] *flush*

ip6 mngt status

ip6 mngt [*internet* | *http* | *telnet* | *ping* | *https* | *ssh* | *enforce_https*] [*on* | *off*]

Syntax Description

Parameter	Description
<i>list</i>	It means to show the setting information of the access list.
<i>add</i> <IP/ Hostname><NO.> <Index> <i>remove</i> <NO.>] <i>flush</i>	It means to add an IPv6 address which can be used to execute management through Internet. <IP/Hostname>: Select the type, IPv6 or Hostname. <NO.>: 1 to 10. Ten profiles can be set for IPv6 access list. <index>: It means the index number of IP object (1 to 64) or keyword object (1 to 200) . <i>remove</i> <Index>: It means to remove (delete) the specified IP/Keyword object.
<i>flush</i>	It means to clear the IPv6 access table.
<i>status</i>	It means to show the status of IPv6 remote management.
<i>internet</i> / <i>http</i> <i>telnet</i> <i>ping</i> <i>https</i> <i>ssh</i> <i>enforce_https</i>	These protocols are used for accessing Internet.
<i>on</i> / <i>off</i>	It means to enable (on) or disable (off) the Internet accessing through http/telnet/ping.

Example

```

> ip6 mngt list add IP 1 1
%% Set OK. Please do "sys re" to reboot the router!
> ip6 mngt list add hostname 2 1
%% Set OK. Please do "sys re" to reboot the router!
> ip6 mngt list
% IPv6 Access List :
[NO.]      [Type]      [Index]      [Description]
=====
===
1          IPv6 Object   1            Please setting index=1 for IPv6 Object
2          hostname     1

```

```
>
```

Telnet Command: ip6 online

This command allows you to check the online status of IPv6 LAN /WAN.

ip6 online [*WAN1*| *WAN2*| *USB1*| *USB2*]

Syntax Description

Parameter	Description
<i>WAN1</i> <i>WAN2</i> <i>USB1</i> <i>USB2</i>	It means the connection interface.

Example

```
> ip6 online WAN1
% WAN1 online status :
% IPv6 WAN1 Disabled
% Default Gateway : ::
% Interface : DOWN
% UpTime : 0:00:00
% IPv6 DNS Server: :: Static
% IPv6 DNS Server: :: Static
% IPv6 DNS Server: :: Static
% Tx packets = 0, Tx bytes = 0, Rx packets = 0, Rx bytes = 0
% MTU Onlink: 1280 , Config MTU : 0
```

Telnet Command: ip6 aiccu

This command allows you to view IPv6 settings for WAN interface with connection type of AICCU.

Syntax

ip6 aiccu -i <*ifno*> **-r**

ip6 aiccu -i <*ifno*> **-s**

Syntax Description

Parameter	Description
-r	Reset the AICCU retry account for the specified interace.
ifno	ifno=1, WAN1 ifno=2, WAN2 ifno=x, WANx
-s	Show the interface status.

Example

```
> ip6 aiccu -i 1 -r
reset AICCU Retry Account OK!

>
```

Telnet Command: ip6 ntp

This command allows you to set IPv6 settings for NTP (Network Time Protocols) server.

```
ip6 ntp -h
ip6 ntp -v
ip6 ntp -p <0/1>
```

Syntax Description

Parameter	Description
-h	It is used to display the usage of such command.
-v	It is used to show the NTP state.
-p <0/1>	It is used to specify NTP server for IPv6. 0 - Auto 1 - First Query IPv6 NTP Server.

Example

```
> ip6 ntp -p 1
% Set NTP Priority: IPv6 First
```

Telnet Command: ip6 lan

This command allows you to configure settings for IPv6 LAN.

Syntax

```
ip6 lan -l n [-<l:w:d:D:m:o:s> <parameter> | ... ]
```

Syntax Description

Parameter	Description
-h	It is used to display the usage of such command.
<l:w:d:D:m:o:s><parameter>	The following lists all of the available commands with parameters.
-l n	Select LAN interface to be set. n = 1: LAN1. Default is LAN1. n = 2: LAN2 n = x: LANx
-w n	Select WAN interface to be primary. n = 0: None n = 1: WAN1 n = 2: WAN2 n = x: WANx.
-d <server>	Set the first DNS Server IP. <server>= IPv6 Address.
-D <server>	Set second DNS Server IP. <server>= IPv6 Address.
-m n	Set IPv6 LAN management. Default is SLAAC. n = 0: OFF n = 1: SLAAC n = 2: DHCPv6.
-o n	Enable Other option(O-bit) flag. (O-bit is redundant when management is DHCPv6) n= 0: Disable n= 1: Enable.
-e n:	Add an extension WAN. n = 1: WAN1

	n = 2: WAN2 n = x: WANx.
-E n	Delete an extension WAN. n = 1: WAN1 n = 2: WAN2 n = x: WANx.
-b map	Set bit map(decimal) for extension WANs. map = bit 0: WAN1 map = bit 1: WAN2 map = bit n: WAN(n+1)
-f n	Disable IPv6. n = 1: Disable IPv6 n = 0: Enable IPv6.
-R <n>	It means to enable /disable RIPng. n=1: Enable RIPng, n=0: Disable RIPng.
-s n	Show IPv6 LAN setting. n = 0: show all. n = 1: LAN1, 2: LAN2, ... x: LANx, 5: DMZ. Default is show all

Example

```
> ip6 lan -l 1 -w 1 -d 2001:4860:4860::8888 -o 1 -f 0 -s 2
% Set LAN1!

% Set primary WAN1!

% Set 1st DNS server 2001:4860:4860::8888

% Set Other Option Enable!

% [LAN1] support ipv6!

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.

% [LAN2] setting:
% Primary WAN : WAN1
% Management : SLAAC
% Other Option : Disable
% WAN Exten : None
% Subnet ID : 2
% Static IP(0) : ::/0
% [ifno: 0, enable: 0]
% Static IP(1) : ::/0
% [ifno: 0, enable: 0]
% Static IP(2) : ::/0
% [ifno: 0, enable: 0]
% Static IP(3) : ::/0
% [ifno: 0, enable: 0]
% DNS1 : 2001:4860:4860::8888
% DNS2 : 2001:4860:4860::8844
% ULA Type : OFF
% RIPng : Enable
```

Telnet Command: ip6 session

This command allows you to set sessions limit for IPv6 address.

Syntax

ip6 session on

ip6 session off

ip6 session default <num>

ip6 session status

ip6 session show

ip6 session add <IP1-IP2> <num>

ip6 session del <IP1>/ <all>

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. <num>: Enter a number.
<i>status</i>	It means to display the current settings.
<i>show</i>	It means to display all IP range session limit settings.
<i>add <IP1-IP2><num></i>	<add/del>: It means to add the session limit for an IPv6 range. <IP1-IP2> : Specify a range for IPv6 addresses. <num>: Enter a number.
<i>del<IP1> / all</i>	<del>: It means to delete the session limit for an IPv6 range. <IP1> : Specify the first IPv6 address within the IPv6 range. all: Delete all the session limits.

Example

```
> ip6 session on
> ip6 session add 2100:ABCD::2-2100:ABCD::10 100
> ip6 session status

IPv6 range:
  2100:ABCD::2 - 2100:ABCD::10 : 100

Current ip6 session limit is turn on

Current default session number is 100
```

Telnet Command: ip6 bandwidth

This command allows you to set IPv6 settings for bandwidth control.

Syntax

ip6 bandwidth on

ip6 bandwidth off

ip6 bandwidth default <tx_rate> <rx_rate>
ip6 bandwidth status
ip6 bandwidth show
ip6 bandwidth add <IP1-IP2> <tx><rx><shared>
ip6 bandwidth del <IP1-IP2> / all

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on bandwidth limit for each IP.
<i>off</i>	It means to turn off bandwidth limit for each IP.
<i>default <tx_rate> <rx_rate></i>	It means to set the default transmission (tx), receiving (rx) rate of bandwidth limit (0-30000 Kbps/Mbps). <tx_rate>: Enter a number. <rx_rate>: Enter a number.
<i>status</i>	It means to display the current settings.
<i>show</i>	It means to display all IP range bandwidth limit settings.
<i>add <IP1-IP2> <tx><rx><shared></i>	<add>: It means to add the bandwidth limit for an IPv6 range. <del>: It means to delete the bandwidth limit for an IPv6 range by first IP (IP1) or 'del all'. <IP1-IP2> - Specify a range for IPv6 addresses. <tx><rx>: It means the bandwidth limit for transmission and receiving rate. <shared>: It means the bandwidth will be shared for the IPv6 range.
<i>del <IP1-IP2> / all</i>	It means to delete the bandwidth limit for an IPv6 range by first IP (IP1) or 'del all'. <IP1-IP2> - Specify a range for IPv6 addresses. all: Delete all the bandwidth limits.

Example

```

> ip6 bandwidth on
> ip6 bandwidth add 2001:ABCD::2-2001:ABCD::10 512 5M shared
> ip6 bandwidth status

IPv6 range:
  2001:ABCD::2 - 2001:ABCD::10 : Tx:512K Rx:5M shared

Current ip6 Bandwidth limit is turn on

Current default ip6 Bandwidth rate is Tx:2000K Rx:8000K bps
> ip6 bandwidth del 2001:ABCD::2
>
  
```

Telnet Command: ipf view

IPF users to view the version of the IP filter, to view/set the log flag, to view the running IP filter rules.

ipf view [-VcdhrtzZ]

Syntax Description

Parameter	Description
<i>-V</i>	It means to show the version of this IP filter.
<i>-c</i>	It means to show the running call filter rules.
<i>-d</i>	It means to show the running data filter rules.
<i>-h</i>	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
ipf: IP Filter: v3.3.1 (1852)
Kernel: IP Filter: v3.3.1
Running: yes
Log Flags: 0x603a29dc = block, nomatch
Default: pass all, Logging: available
```

Telnet Command: ipf set

This command is used to set general rule, filter set and filter rule for firewall.

ipf set [*Options*]

ipf set [*SET_NO*] [*Options*]

ipf set [*SET_NO*] **rule** [*RULE_NO*] [*Options*]

Syntax Description

Parameter	Description
<i>ipf set</i> [<i>options</i>]	It means to set the firewall general setup and default rule.
<i>ipf set</i> < <i>SET_NO</i> >< <i>Options</i> >	It means to set the firewall filter set including comments and next filter set.
<i>ipf set</i> < <i>SET_NO</i> > rule < <i>RULE_NO</i> > < <i>Options</i> >	It means to set the firewall rule in filter set. For detailed information, refer to Telnet Command: ipf rule.
<i>About ipf set</i> [<i>options</i>]	
-v	Type "-v" to view the configuration of general set.
-c < <i>p1</i> >	It means to setup Call Filter. < <i>p1</i> >: Specify the index number (1 to 12) of the set profile. To disable the setting, enter "0".
-d < <i>p1</i> >	It means to setup Data Filter. < <i>p1</i> >: Specify the index number (1 to 12) of the set profile. To disable the setting, enter "0".
-p < <i>p1</i> >< <i>p2</i> >	It means to setup actions for packet not matching any rule and whether record syslog. < <i>p1</i> >: Type "0" to let packets not matching any rule pass; Type "1" to block the packets not matching any rule. < <i>p2</i> >: "0" means the log related to rule matching will not be recorded on Syslog; "1" means the log related to rule matching will be recorded on Syslog. For example, to set pass for packet not matching any rule and enable syslog, -p 0 1 .
-R < <i>v4/v6</i> > < <i>Enable/Disable</i> >	It means to accept routing packet from WAN. < <i>v4/v6</i> >: IPv4 or IPv6. < <i>Enable/Disable</i> >: Enter 0 (enable) or 1 (disable). Set Accept routing packet from WAN by IPv4, please enter -R v4 0 .
-L < <i>p1</i> >	It means to enable or disable the Strict Security Firewall function.

	<p1>: Enter 1(enable) or 0 (disable).
-C <p1>	It means to setup Code Page. <p1>: Enter a code page number (0 to 20). For example, ipf set -C 20. 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
-M <p1><p2>	It means to setup APP Enforcement and Syslog. <p1>: Enter a number (0 to 32). In which, 0 means none; 1 to 32 mens the index number of the profile. <p2>: "0" means the log related to APP Enforcement will not be recorded on Syslog; "1" means the log related to APP Enforcement will be recorded on Syslog.
-U <p1><p2>	It means to setup URL Content Filter for packets not matching any rule. <p1>: Enter a number (0 to 8). In which, 0 means none; 1 to 8 mens the index number of the profile. <p2>: "0" means the log related to URL Content Filter will not be recorded on Syslog; "1" means the log related to URL Content Filter will be recorded on Syslog.
-W <p1><p2>	It means to setup Web Content Filter for packets not matching any rule. <p1>: Enter a number (0 to 8). In which, 0 means none; 1 to 8 mens the index number of the profile. <p2>: "0" means the log related to Web Content Filter will not be recorded on Syslog; "1" means the log related to Web Content Filter will be recorded on Syslog.
-D <p1><p2>	It means to setup DNS Filter for packets not matching any rule. <p1>: Enter a number (0 to 8). In which, 0 means none; 1 to 8 mens the index number of the profile. <p2>: "0" means the log related to DNS Filter will not be recorded on Syslog; "1" means the log related to DNS Filter will be recorded on Syslog.
-a <p1>	It means to configure the advanced settings.
-f <p1>	It means to accept large incoming fragmented UDP or ICMP packets. <p1>: Enter 1(enable) or 0 (disable).

-t <p1>	It means to enable or disable the Transparent Mode. <p1>: Enter 1(enable) or 0 (disable).
-E <p1><p2>	It means to set the maximum count for session limitation. <p1>: Enter a number (0 to 50000) <p2>: "0" means the log related to session control will not be recorded on Syslog; "1" means the log related to session control will be recorded on Syslog.
-Q <p1><p2>	It means to set the QoS Class. <p1>: Enter a number (0 to 4). 0: None 1: Class 1 2: Class 2 3: Class 3 4: Default Class <p2>: "0" means the log related to QoS Class will not be recorded on Syslog; "1" means the log related to QoS Class will be recorded on Syslog.
-Y <p1><p2>	It means to set the User Management. <p1>: Enter a number (-1 to 2). -1: None 0: All 1: user object 2: user group 4: Default Class <p2>: 1 to 200(if p1 is set with 1, user object) or 1 to 32(if p1 is set with 2, user group)
-y <p1>	It means the log related to User Management will be or be not recorded on Syslog. <p1>: Enter 1(enable) or 0 (disable).
-w <p1>	It means to set the window size of TCP protocol. <p1>: Enter a value (0 to 65535).
-A <p1>	It means to enable or disable the function of packet capture. <p1>: Enter 1(enable) or 0 (disable).
<i>About ipf set [SET_NO] [Options]</i>	
-m [Comments]	It means to set comment for a filter set. [Comments]: Enter a description for the filter set.
-v	It means to view the comment and the next filter set.
-n [NEXT_SET_NO]	It means to specify the next filter set of current filter set. [NEXT_SET_NO]: Enter a number (1 to 12). For example, ipf set 1 -n 2.

Example

```
> ipf set -R "v4 1"
Setting saved.
> ipf set -R "v6 1"
Setting saved.
> ipf set -v
Data Filter: Enable (Start Filter Set = 1)
Log Flag    : Disable
```

```

Actions for packet not matching any rule:
  Pass or Block      : Pass
  CodePage           : ANSI(1252)-Latin I
  Max Sessions Limit: 50000
  Current Sessions   : 0
  Mac Bind IP        : Non-Strict
  QOS Class          : None
  APP Enforcement     : None
  URL Content Filter: None
  WEB Content Filter: None
  DNS Filter         : None
  Load-Balance policy : Auto-select
-----
  CodePage           : ANSI(1252)-Latin I
  Window size        : 65535
  Session timeout    : 60
  DrayTek Banner     : Enable
-----
  Accept large incoming fragmented UDP or ICMP packets: Enable
  Transparent Mode   : Disable
-----
  Block routing packet from WAN:
    [v] IPv4
    [v] IPv6
-----
  [v] Enable Strict Security Firewall
>

```

Telnet Command: ipf rule

This command is used to set filter rule for firewall.

ipf rule s r [-<command> <parameter> | ...

ipf rule s r -v

Syntax Description

Parameter	Description
<i>s</i>	Such word means Filter Set, range form 1-12.
<i>r</i>	Such word means Filter Rule, range from 1-7.
<Command><parameter>	The following lists all of the available commands with parameters.
-e <0/ 1>	It means to enable or disable the rule setting. 0- disable 1- enable
-v	It is used to show current filter rule settings.
-D <value>	It means to set the direction of packet flow. It is for Data Filter only. 0: LAN/DMZ/RT/VPN -> WAN 1: WAN -> LAN/DMZ/RT/VPN 2: LAN/DMZ/RT/VPN -> LAN/DMZ/RT/VPN
-I "<e/d><para1, para2,...>"	It means to set incoming interface. e: Enable the function.

	d: Disable the function. Para1, para2,...: Available values include all, LAN1, LAN2,...LAN8, RT, VPN, WAN1, WAN2,...WAN7 Example: > ipf rule 3 1 -e 1 -I "e LAN1"
-O "<e/d><para1, para2,...>"	It means to set outgoing interface. e: Enable the function. d: Disable the function. Para1, para2,...: Available values include all, LAN1, LAN2,...LAN4, RT, VPN, WAN1, WAN2,...WAN6 Exampe: > ipf rule 3 1 -e 1 -O "e LAN2"
-s "o o6 g g6 c <field> <obj>"	It means to specify source IP object, IP group. o: Indicates "IPv4 object". o6: Indicates IPv6 object". g: Indicates "IPv4 group". g6: Indicates "IPv6 group". c: Indicates country object. field: Indicates the quantity of objects/groups that can be set for this rule at one time. -2 object profiles are allowed for IPv4 -2 group profiles are allowed for IPv4 group -3 object profiles are allowed for IPv6 -1 group profiles is allowed for IPv6 group obj : indicates index number of object or index number of group. -Range for IPv4, from 1 to 192, 0 means none. -Range for IPv4 group, from 1 to 32, 0 means none. -Range for IPv6, from 1 to 64, 0 means none. -Range for IPv6 group, from 1 to 32, 0 means none. -Ranges for country object, from 1 to 32. For example, -s "o 1 2" means IPv4 object profile 1 and 2 are set as souce IP. Exampe: > ipf rule 3 1 -e 1 -s "o 1 2"
-d "o o6 g g6 c <field> <obj>"	It means to specify destination IP object, IP group. o: Indicates "IPv4 object". o6: Indicates IPv6 object". g: Indicates "IPv4 group". g6: Indicates "IPv6 group". c: Indicates country object. field: Indicates the quantity of objects/groups can be set for this rule at one time. -2 object profiles are allowed for IPv4 -2 group profiles are allowed for IPv4 group -3 object profiles are allowed for IPv6 -1 group profiles is allowed for IPv6 group obj : indicates index number of object or index number of group. -Range for IPv4, from 1 to 192, 0 means none. -Range for IPv4 group, from 1 to 32, 0 means none. -Range for IPv6, from 1 to 64, 0 means none. -Range for IPv6 group, from 1 to 32, 0 means none. -Ranges for country object, from 1 to 32. For example, -s "o 1 2" means IPv4 object profile 1 and 2 are set as destination IP. Exampe: > ipf rule 3 1 -e 1 -d "o 2 2"
-d "u <Address Type> <Start	It means to configure destination IP address including address type,

<i>IP Address> <End IP Address> <Address Mask>"</i>	start IP address, end IP address and address mask. u : It means "user defined". <i>Address Type</i> : Type the number (representing different address type). 0 : Subnet Address 1 : Single Address 2 : Any Address 3 : Range Address Example: Set Subnet Address => -d "u 0 192.168.1.10 255.255.255.0" Set Single Address => -d "u 1 192.168.1.10 " Set Any Address => -d "u 2 " Set Range Address => -d "u 3 192.168.1.10 192.168.1.15"
<i>-S o:g <obj></i>	It means to specify Service Type object and IP group. o - indicates "object". g - indicates "group" <obj> - indicates index number of object or index number of group. Available settings range from 1-96. For example, "-S 0 1" means the first service type object profile.
<i>-S "u <protocol> <source_port_value> <destination_port_value>"</i>	It means to configure advanced settings for Service Type, such as protocol and port range. u : it means "user defined". <protocol> : It means TCP(6),UDP(17), TCP/UDP(255), Any(0), ICMP(1), ICMPv6(58), Other(other) <source_port_value> : 1 : Port OP, range is 0-3. 0:=, 1:!=, 2:>, 3:< 3 : Port range of the Start Port Number, range is 1-65535. 5 : Port range of the End Port Number, range is 1-65535. <destination_port_value>: 2 : Port OP, range is 0-3, 0:==, 1:!=, 2:>, 3:< 4 : Port range of the Start Port Number, range is 1-65535. 6 : Port range of the End Port Number, range is 1-65535.
<i>-f <value></i>	It means to set fragment type. 0 : Don't care. 1 : Unfragmented. 2 : Fragmented. 3 : Too Short
<i>-F "<Param 0> <Param 1>"</i>	It means the Filter action you can specify. <param 0>: Enter the number to set the filter action. 0 : Pass Immediately. 1 : Block Immediately. 2 : Pass if no further match. 3 : Block if no further match. <Param 1>: Let the log be recorded on Syslog. 0 : Disable Log. 1 : Enable Log.
<i>-m "<Param 0> <Param 1>"</i>	It means to set MAC Bind IP type and the Syslog. <param 0>: Enter the number to choose the type. 0 : Non-Strict. 1 : Strict. <Param 1>: Let the log be recorded on Syslog.

	0 : Disable Log. 1 : Enable Log.
-Y <Param 0> <Param 1>	It means to set the User Management. <param 0>: Enter the number to choose the type. -1 : None. 0 : All. 1 : User Object 2 : User group <Param 1>: Let the log be recorded on Syslog if <param 0> is set with None/ALL. 0 : Disable. 1 : Enable. Enter the the user object number (1 to 200) / group number (1 to 32) if <param 0> is set with User Object.
-y <value>	It means the log related to User Management will be or be not recorded on Syslog. <value>: Enter 1(enable) or 0 (disable)
-L <Param 0> <Param 1>	It means to set the maximum count for the session limitation. <param 0>: Enter the number (0 to 50000) to choose the type. <Param 1>: Let the log be recorded on Syslog. 0 : Disable. 1 : Enable.
-q <Param 0> <Param 1>	It means to set the classification for QoS. <Param 0>: 1- Class 1, 2 - Class 2, 3 - Class 3, 4 - Other <Param 1>: Let the log be recorded on Syslog. 0 : Disable. 1 : Enable.
-l <Param 0> <Param 1>	It means load balance policy. Such function is used for “debug” only. <Param 0>: Enter 0, 1, 2, or 3. 0:Auto-Select, 1:WAN 1. 2:WAN 2. 3:WAN 3. <Param 1>: Enter 0 or 1. 0:Disable Log. 1:Enable Log.
-a "<Param 0> <Param 1>"	It means to specify which APP Enforcement profile will be applied. <Param 0> : Available settings range from 0 - 32. “0” means no profile will be applied. <Param 1> : Let the log be recorded on Syslog. 0 : Disable. 1 : Enable.
-u <Param 0> <Param 1>	It means to specify which URL Content Filter profile will be applied. <Param 0> : Available settings range from 0 - 8. “0” means no profile will be applied. <Param 1> : Let the log be recorded on Syslog. 0 : Disable.

	1 : Enable.
-w "<Param 0> <Param 1>"	It means to specify which Web Content Filter profile will be applied. <Param 0> : Available settings range from 0 ~ 8. "0" means no profile will be applied. <Param 1> : Let the log be recorded on Syslog. 0 : Disable. 1 : Enable.
-n "<Param 0> <Param 1>"	It means to specify which DNS Filter profile will be applied. <Param 0> : Available settings range from 0 ~ 8. "0" means no profile will be applied. <Param 1> : Let the log be recorded on Syslog. 0 : Disable. 1 : Enable.
-N <value>	It means to set the Next Filter Set. <value> : Available settings range from 0 ~ 12. "0" means no profile will be applied. 0 : None 1 : Set#1; 2: Set#2, and so on.
-c <0~20>	It means to set code page. Different number represents different code page. 0. None 1. ANSI(1250)-Central Europe 2. ANSI(1251)-Cyrillic 3. ANSI(1252)-Latin I 4. ANSI(1253)-Greek 5. ANSI(1254)-Turkish 6. ANSI(1255)-Hebrew 7. ANSI(1256)-Arabic 8. ANSI(1257)-Baltic 9. ANSI(1258)-Viet Nam 10. OEM(437)-United States 11. OEM(850)-Multilingual Latin I 12. OEM(860)-Portuguese 13. OEM(861)-Icelandic 14. OEM(863)-Canadian French 15. OEM(865)-Nordic 16. ANSI/OEM(874)-Thai 17. ANSI/OEM(932)-Japanese Shift-JIS 18. ANSI/OEM(936)-Simplified Chinese GBK 19. ANSI/OEM(949)-Korean 20. ANSI/OEM(950)-Traditional Chinese Big5
-C "<Windows Size> <Session_Timeout>"	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.
-b <value>	It means to enable or disable the DrayTek Banner. <value>: 0 : Disable; 1 : Enable.
-t "i <Param 0> <Param 1>"	It means to set schedule profile. Totally, there are four sets of schedule profiles can be specified. <param 0>: Enter the index number (1 to 4) for each set. <param 1>: Enter the index number (0 to 15) of the schedule profile for each set. 0 means none. For example, -t "i 1 3" means schedule profile #3 is configured for

	set #1. Exampe: > ipf rule 3 1 -e 1 -t "i 1 3"
-t "c <value>"	It means to enable or disable the function of clearing sessions when the schedule is ON. <value>: 0 : Disable; 1 : Enable.
-M <Your Comments>	It means to set comments for the fitler rule. <Your Comments>: Enter a brief description.
-U "<up/ down>"	It means to move up or move down the order of a filter rule in the filter set. up: It indicates move the filter rule up. down: It indicates move the filter rule down.

Example

```
> ipf rule 2 1 -e 1 -M "Your Comments" -s "o 1" -d "o 2" -S "o 1" -F "1 1"

Setting saved.
> ipf rule 2 1 -v

Filter Set 2 Rule 1:

Status      : Enable
Comments: Your
Index(1-15) in Schedule Setup: <null>, <null>, <null>, <null>

Direction   : LAN -> WAN
Source IP    : Object1,
Destination IP: Object2,
Service Type : TCP/UDPObject1,
Fragments    : Don't Care

Pass or Block      : Block Immediately
Branch to Other Filter Set: None
Max Sessions Limit : 60000
Current Sessions   : 0
Mac Bind IP        : Non-Strict
Qos Class          : None
APP Enforcement    : None
URL Content Filter : None
WEB Content Filter : None
DNS Filter         : None
Load-Balance policy : Auto-select
Log                : Enable
-----
CodePage          : ANSI(1252)-Latin I
Window size       : 65535
Session timeout   : 1440
DrayTek Banner    : Enable
-----
Strict Security Checking
[ ] APP Enforcement
>
```

Telnet Command: ipf flowtrack

This command is used to set and view flowtrack sessions.

ipf flowtrack set [-re]

ipf flowtrack view [-fb]

Syntax Description

Parameter	Description
-r	It means to refresh the flowtrack.
-e	It means to enable or disable the flowtrack.
-f	It means to show the sessions state of flowtrack. If you do not specify any IP address, then all the session state of flowtrack will be displayed.
-b	It means to show all of IP sessions state.

Example

```
>ipf flowtrack set -r
Refresh the flowstate ok
> ipf flowtrack view -f
Start to show the flowtrack sessions state:

ORIGIN>> 192.168.1.11:59939 -> 8.8.8.8: 53 ,ifno=0
REPLY >> 8.8.8.8: 53 -> 192.168.1.11:59939 ,ifno=3
        proto=17, age=93023180(3920), flag=203
ORIGIN>> 192.168.1.11:15073 -> 8.8.8.8: 53 ,ifno=0
REPLY >> 8.8.8.8: 53 -> 192.168.1.11:15073 ,ifno=3
        proto=17, age=93025100(2000), flag=203
ORIGIN>> 192.168.1.11: 7247 -> 8.8.8.8: 53 ,ifno=0
REPLY >> 8.8.8.8: 53 -> 192.168.1.11: 7247 ,ifno=3
        proto=17, age=93020100(7000), flag=203
End to show the flowtrack sessions state
> ipf flowtrack set -e

Current flow_enable=0
> ipf flowtrack set -e

Curretn flow_enable=1
```

Telnet Command: ipf flowtest, ipf hash_analysis

These commands are used for RD debug in firewall diagnose.

Telnet Command: Log

This command allows users to view log for WAN interface such as call log, IP filter log, flush log buffer, etc.

log [-cfhiptwx?] [-F a| c | f | w]

Syntax Description

Parameter	Description
-c	It means to show the latest call log.
-f	It means to show the IP filter log.

-F	It means to show the flush log buffer. a: flush all logs c: flush the call log f: flush the IP filter log w: flush the WAN log
-h	It means to show this usage help.
-p	It means to show PPP/MP log.
-t	It means to show all logs saved in the log buffer.
-w	It means to show WAN log.
-x	It means to show packet body hex dump.

Example

```
> log -w
25:36:25.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
    Client IP      = 0.0.0.0
    Your IP        = 0.0.0.0
    Next server IP = 0.0.0.0
    Relay agent IP = 0.0.0.0
25:36:33.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
    Client IP      = 0.0.0.0
    Your IP        = 0.0.0.0
    Next server IP = 0.0.0.0
    Relay agent IP = 0.0.0.0
25:36:41.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
    Client IP      = 0.0.0.0
    Your IP        = 0.0.0.0
    Next server IP = 0.0.0.0
    Relay agent IP = 0.0.0.0
25:36:49.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
    Client IP      = 0.0.0.0
    Your IP        = 0.0.0.0
    Next server IP = 0.0.0.0
    Relay agent IP = 0.0.0.0
25:36:57.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
    Client IP      = 0.0.0.0
    Your IP        = 0.0.0.0
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
```

Telnet Command: mngt ftpport

This command allows users to set FTP port for management.

mngt ftpport [*FTP port*]

Syntax Description

Parameter	Description
<i>FTP port</i>	It means to 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.

mngt httpport [*Http port*]

Syntax Description

Parameter	Description
<i>Http port</i>	It means to enter the number for HTTP port. The default setting is 80.

Example

```
> mngt httpport 80
% Set web server port to 80 done.
```

Telnet Command: mngt httpsport

This command allows users to set HTTPS port for management.

mngt httpsport [*Https port*]

Syntax Description

Parameter	Description
<i>Https port</i>	It means to 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 sslvpnport

This command allows users to set SSL VPN port for management.

Syntax

mngt sslvpnport <*SSL VPN port*>

Syntax Description

Parameter	Description
<i>SSL VPN port</i>	It means to type the number for SSL VPN port. The default setting is 443.

Example

```
> mngt sslvpnport 1010
% Set SSL VPN port to 1010 done.
```

Telnet Command: mngt telnetport

This command allows users to set telnet port for management.

mngt telnetport [*Telnet port*]

Syntax Description

Parameter	Description
<i>Telnet port</i>	It means to 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.

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 noping

This command is used to pass or block Ping from LAN PC to the internet.

mngt noping *on*

mngt noping *off*

mngt noping *viewlog*

mngt noping *clearlog*

Syntax Description

Parameter	Description
<i>on</i>	All PING packets will be forwarded from LAN PC to Internet.
<i>off</i>	All PING packets will be blocked from LAN PC to Internet.
<i>viewlog</i>	It means to display a log of ping action, including source MAC and source IP.
<i>clearlog</i>	It means to clear the log of ping action.

Example

```
> mngt noping off
No Ping Packet Out is OFF!!
```


Telnet Command: mngt defenseworm

This command can block specified port for passing through the router.

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.

mngt rmtcfg [*status*]

mngt rmtcfg [*enable*]

mngt rmtcfg [*disable*]

mngt rmtcfg [*http/https/ftp/telnet/ssh/tr069/snmp/enforce_https*] [*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</i>	It means to specify one of the servers/protocols for enabling or

<i>r069/snmp/enforce_https</i>	disabling.
<i>on/off</i>	on - enable the function. off - disable the function.

Example

```
> mngt rmtcfg ftp on
Enable server fail
Remote configure function has been disabled
please enable by enter mngt rmtcfg enable

> mngt rmtcfg enable
%% Remote configure function has been enabled.
> mngt rmtcfg ftp on
%% FTP server has been enabled.
```

Telnet Command: mngt lanaccess

This command allows users to manage accessing into Vigor router through LAN port.

mngt lanaccess *-e [0/ 1] -s [value] -i [value]*

mngt lanaccess *-l <value>*

mngt lanaccess *-E <0/ 1>*

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>-l <value></i>	It means the IP object index allowed to access. Available values include: 1 to 192
<i>-E <0/ 1></i>	It means to enable the function of specific IP allowed to be access. 0-disable the function. 1-enable the function.
<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.

mngt echoicmp *[enable]*

mngt echoicmp *[disable]*

Syntax Description

Parameter	Description
<i>enable</i>	It means to accept the echo ICMP packet.
<i>disable</i>	It means to drop the echo ICMP packet.

Example

```
> mngt echoicmp enable
%% Echo ICMP packet enabled.
```

Telnet Command: mngt accesslist

This command allows you to specify that the system administrator can login from a specific host or network. A maximum of three IPs/subnet masks is allowed.

mngt accesslist *list*

mngt accesslist *add* *[IP/ Host name][NO.][Index]*

mngt accesslist *remove* *[index] [NO.]*

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>IP/ Host name</i>	It means to specify the IP object or the name of the host. Available settings: ● IP ● hostname
<i>No.</i>	A maximum of 10 IP objects are allowed to be assigned.
<i>index</i>	It means the index number (1 to 192) of the IP objects preconfigured.
<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 ip 1 1
%% Set OK. Please do "sys re" to reboot the router!

> mngt accesslist add ip 2 2
%% Set OK. Please do "sys re" to reboot the router!

> mngt accesslist add ip 3 3
%% Set OK. Please do "sys re" to reboot the router!

> mngt accesslist list
%% Access list :
  [NO.]      [Type]      [Index]      [Description]
=====
1           IP Object    1           Please setting index=1 for IP Object
2           IP Object    2           Please setting index=2 for IP Object
3           IP Object    3           Please setting index=3 for IP Object
```

Telnet Command: mngt wanlogin

This command allows you to enable or disable WAN login function.

Syntax

mngt wanlogin *enable*

mngt wanlogin *disable*

Example

```
> mngt wanlogin enable
%% wan login enabled.

>
```

Telnet Command: mngt snmp

This command allows you to configure SNMP for management.

mngt snmp [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
[<command> <parameter> ..]	The available commands with parameters are listed below. [..] means that you can type in several commands in one line.
-e <1/ 2>	1: Enable the SNMP function. 2: Disable the SNMP function.
-a <1/ 2>	1: Enable the SNMPV1 function. 2: Disable the SNMPV1 function.
-b <1/ 2>	1: Enable the SNMPV2C function. 2: Disable the SNMPV2C function.
-c <1/ 2>	1: Enable the SNMPV3 function. 2: Disable the SNMPV3 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. It allows to set 3 IPs, separated by ",".
-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.
-o <username>	It means to set a user account (maximum 23 characters) for user management.
-p <0/ 1/ 2>	It means to set the authentication algorithm. 0: No auth 1: MD5_AUTH 2: SHA_AUTH
-q <password>	It means to set the password (maximum 23 characters) for authentication.
-r <0, 3/ 4/ 6>	It means to set privacy algorithm 0, 3: No_PRIV 4: DES_PRIV 6: AES_PRIV
-u <password>	It means to set the password (maximum 23 characters) for privacy.
-V	It means to list SNMP setting.

Example

```
>mngt snmp -e 1 -g draytek -s DK -m  
192.168.1.20,192.168.5.192/26,10.20.3.40/24 -t trapcom -n  
192.168.1.20,10.20.3.40 -T 88
```

```
SNMP Agent Turn on!!!  
Get Community set to draytek
```

```

Set Community set to DK
Manager Host IP set to 192.168.1.20,192.168.5.192/26,10.20.3.40/24
Trap Community set to trapcom
Notification Host IP set to 192.168.1.20,10.20.3.40
Trap Timeout set to 88 seconds
>

```

Telnet Command: mngt bfp

This command allows you to configure brute force protect (BFP) for system management.

Syntax

mngt bfp [*<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.
-e 0/1	Enable / disable the BFP function. 0 - Disable 1 - Enable
-s <i><service></i>	It means to enable different service. service - Available types are FTP, HTTP, HTTPS, TELNET, TR069, SSH, VPN, None, and All.
-l <i><failure></i>	It means to set login failure retry times. failure - Available number is from 1 to 255.
-p <i><penalty></i>	It means to set penalty time for BFP. The unit is sec.
-v	It means to view current settings.

Example

```

> mngt bfp -e 1
> mngt bfp -s FTP
> mngt bfp -l 10
> mngt bfp -v
Current Brute Force Protection Setting:
* Enable: yes
* Service:
  - FTP:      yes
  - HTTP:     no
  - HTTPS:    no
  - TELNET:   no
  - TR069:    no
  - SSH:      no
  - VPN:      no
* Maximum login failures: 1
* Penalty period: 0

```

Telnet Command: mngt cert_import

This command allows you to import a certificate to Vigor router.

Syntax

mngt cert_import local_cert *<URL><password>*

mngt cert_import trusted_ca <URL>

Syntax Description

Parameter	Description
<i>local_cert url <URL></i> <i><password></i>	URL - Enter a URL(http://....) for downloading the certificate. The file is encrypted with the file format of "xxxx.p12". Password - Enter the password for decrypting the .p12 certificate.
<i>trusted_ca <URL></i>	URL - Enter a URL(http://....) for downloading the certificate. The file is encrypted with the file format of "xxxx.p12".

Telnet Command: mngt telnettimeout

This command allows you to configure the timeout for telnet connection.

Syntax

mngt telnettimeout <value>

Syntax Description

Parameter	Description
<i><value></i>	Range from 60 to 300. The default value is 300 (seconds).

Example

```
> mngt telnettimeout 100
% Telnet timeout : 100s
```

Telnet Command: mngt ssthtimeout

This command allows you to configure the timeout for SSH connection.

Syntax

mngt ssthtimeout <value>

Syntax Description

Parameter	Description
<i><value></i>	Range from 60 to 300. The default value is 180 (seconds).

Example

```
> mngt ssthtimeout 200
% SSH timeout : 200s
>
```

Telnet Command: mngt ip6_IIDs

This command allows you to configure the IPv6 interface ID.

Syntax

mngt ip6-IIDs -e <val>>

mngt ip6_IIDs -r <interface>

mngt ip6_IIDs -s

Syntax Description

Parameter	Description
-e <value>	It is used to determine the way of generating IPv6 interface id. val = 0 : Use EUI-64 IIDs as interface id val = 1 : Use Random IIDs as interface id
-r <interface>	It is used to re-generate the random IIDs of the specified interface. interface = LAN1 LAN2 ... WAN1 WAN2 USB1 USB2...
-s	Displays the random IIDs for each interface.

Example

```
> mngt ip6_IIDs -e 1
% Setting success, the change will take effect after router rebooting.
> mngt ip6_IIDs -r LAN1
% Setting success, the change will take effect after router rebooting.
> mngt ip6_IIDs -s
% LAN IIDs = 9a5d:06c3:c972:f3ad
% WAN1 IIDs = 7651:92cc:6f8b:42c8
% WAN2 IIDs = 79e5:56cd:be43:384a
% WAN3 IIDs = 0193:56a8:5c6e:01e7
% WAN4 IIDs = 47bf:a971:857d:5a07
% LTE IIDs = e4bf:d21d:f59f:888d
% USB IIDs = 4c55:260c:e5f5:57b7
```

Telnet Command: msubnet switch

This command is used to configure multi-subnet.

msubnet switch [2/ 3/ 4][On/ Off]

Syntax Description

Parameter	Description
2/ 3/ 4/ 5/ 6	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
On/ Off	On means turning on the subnet for the specified LAN interface. Off means turning off the subnet.

Example

```
> msubnet switch 2 On
% LAN2 Subnet On!

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```


Telnet Command: msubnet addr

This command is used to configure IP address for the specified LAN interface.

msubnet addr [2/ 3/ 4][IP address]

Syntax Description

Parameter	Description
2/ 3/ 4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
IP address	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.

msubnet nmask [2/ 3/ 4][IP address]

Syntax Description

Parameter	Description
2/ 3/ 4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
IP address	Type the subnet mask address for the specified LAN interface.

Example

```
> msubnet nmask 2 255.255.0.0
% Set LAN2 subnet mask done !!!

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet status

This command is used to display current status of subnet.

msubnet status [2/ 3/ 4]

Syntax Description

Parameter	Description
2/ 3/ 4	It means LAN interface.

	2=LAN2
	3=LAN3
	4=LAN4

Example

```
> msubnet status 2
% LAN2      Off: 0.0.0.0/0.0.0.0, PPP Start IP: 0.0.0.60
% DHCP server: Off
% Dhcp Gateway: 0.0.0.0, Start IP: 0.0.0.10, Pool Count: 50
```

Telnet Command: msubnet dhcps

This command allows you to enable or disable DHCP server for the subnet.

msubnet dhcps [*2/ 3/ 4*][*On/ Off*]

Syntax Description

Parameter	Description
<i>2/ 3/ 4</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<i>On/ Off</i>	On means enabling the DHCP server for the specified LAN interface. Off means disabling the DHCP server.

Example

```
> msubnet dhcps 3 off
% LAN3      Subnet DHCP Server disabled!

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet nat

This command is used to configure the subnet for NAT or Routing usage.

msubnet nat [*2/ 3/ 4*] [*On/ Off*]

Syntax Description

Parameter	Description
<i>2/ 3/ 4</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<i>On/ Off</i>	On - It means the subnet will be configured for NAT usage. Off - It means the subnet will be configured for Routing usage.

Example

```
> > 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.

msubnet gateway [2/ 3/ 4] [Gateway IP]

Syntax Description

Parameter	Description
2/ 3/ 4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
Gateway IP	Specify an IP address as the gateway IP.

Example

```
> msubnet gateway 2 192.168.1.13
% Set LAN2 Dhcp Gateway IP done !!!
```

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.

Telnet Command: msubnet ipcnt

This command is used to defined the total number allowed for each LAN interface.

msubnet ipcnt [2/ 3/ 4] [IP counts]

Syntax Description

Parameter	Description
2/ 3/ 4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
IP counts	Specify a total number of IP address allowed for each LAN interface. The available range is from 0 to 220.

Example

```
> msubnet ipcnt 2 15
This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet talk

This command is used to establish a route between two LAN interfaces.

msubnet talk [1/ 2/ 3/ 4] [1/ 2/ 3/ 4] [On/ Off]

Syntax Description

Parameter	Description
1/2/3/4	It means LAN interface. 1=LAN1 2=LAN2 3=LAN3 4=LAN4
On/Off	On - It means to establish a link for the selected LAN with others. Off - It means to terminate the link.

Example

```
> msubnet talk 1 2 on
% Enable routing between LAN1 and LAN2!

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.

> msubnet talk
% msubnet talk <1/2/3/4> <1/2/3/4> <On/Off>
% where 1:LAN1, 2:LAN2, 3:LAN3, 4:LAN4
% Now:
%           LAN1   LAN2   LAN3   LAN4
% LAN1       V
% LAN2       V     V
% LAN3               V
% LAN4                   V
```

Telnet Command: msubnet startip

This command is used to configure a starting IP address for DHCP.

msubnet startip [2/3/4] [Gateway IP]

Syntax Description

Parameter	Description
2/3/4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
Gateway IP	Type an IP address as the starting IP address for a subnet.

Example

```
> msubnet startip 2 192.168.2.90
%Set LAN2 Dhcp Start IP done !!!

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
> msubnet startip ?
% msubnet startip <2/3/4> <Gateway IP>
% Now: LAN2 192.168.2.90; LAN3 192.168.3.10; LAN4 192.168.4.10;
```

Telnet Command: msubnet pppip

This command is used to configure a starting IP address for PPP connection.

msubnet pppip [*2/3/4*] [*Start IP*]

Syntax Description

Parameter	Description
<i>2/3/4</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<i>Start IP</i>	Type an IP address as the starting IP address for PPP connection.

Example

```
> msubnet pppip 2 192.168.2.250
% Set LAN2 PPP(IPCP) Start IP done !!!

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.

> msubnet pppip ?
% msubnet pppip <2/3/4> <Start IP>
% Now: LAN2 192.168.2.250; LAN3 192.168.3.200; LAN4 192.168.4.200
```

Telnet Command: msubnet nodetype

This command is used to specify the type for node which is required by DHCP option.

msubnet nodetype [*2/3/4*][*count*]

Syntax Description

Parameter	Description
<i>2/3/4</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<i>count</i>	Choose the following number for specifying different node type. 1= B-node 2= P-node 4= M-node 8= H-node 0= Not specify any type for node.

Example

```
> msubnet nodetype ?
% msubnet nodetype <2/3/4> <count>
% Now: LAN2 0; LAN3 0; LAN4 0

% count: 1. B-node 2. P-node 4. M-node 8. H-node

> msubnet nodetype 2 1
% Set LAN2 Dhcp Node Type done !!!
```

```

> msubnet nodetype ?
% msubnet nodetype <2/3/4> <count>
% Now: LAN2 1; LAN3 0; LAN4 0

% count: 1. B-node 2. P-node 4. M-node 8. H-node

```

Telnet Command: msubnet primWINS

This command is used to configure primary WINS server.

msubnet primWINS [2/3/4] [WINS IP]

Syntax Description

Parameter	Description
2/3/4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
WINS IP	Type the IP address as the WINS IP.

Example

```

> msubnet primWINS ?
% msubnet primWINS <2/3/4> <WINS IP>
% Now: LAN2 0.0.0.0; LAN3 0.0.0.0; LAN4 0.0.0.0
> msubnet primWINS 2 192.168.3.5
% Set LAN2 Dhcp Primary WINS IP done !!!

> msubnet primWINS ?
% msubnet primWINS <2/3/4> <WINS IP>
% Now: LAN2 192.168.3.5; LAN3 0.0.0.0; LAN4 0.0.0.0

```

Telnet Command: msubnet secWINS

This command is used to configure secondary WINS server.

msubnet secWINS [2/3/4] [WINS IP]

Syntax Description

Parameter	Description
2/3/4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
WINS IP	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> <WINS IP>
% Now: LAN2 192.168.3.89; LAN3 0.0.0.0; LAN4 0.0.0.0
```

Telnet Command: msubnet tftp

This command is used to set TFTP server for multi-subnet.

msubnet tftp [*2/3/4*] [*TFTP server name*]

Syntax Description

Parameter	Description
<i>2/3/4</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<i>TFTP server name</i>	Type a name to indicate the TFTP server.

Example

```
> msubnet tftp ?
% msubnet tftp <2/3/4> <TFTP server name>
% Now: LAN2
      LAN3
      LAN4

> msubnet tftp 2 publish
% Set LAN2 TFTP Server Name done !!!

> msubnet tftp ?
% msubnet tftp <2/3/4> <TFTP server name>
% Now: LAN2 publish
      LAN3
      LAN4
```

Telnet Command: msubnet mtu

This command allows you to configure MTU value for LAN/IP Routed Subnet.

msubnet mtu [*interface*][*value*]

Syntax Description

Parameter	Description
<i>interface</i>	Available settings include LAN1-LAN4, IP_Routed_Subnet.
<i>value</i>	1000 ~ 1500 (Bytes), default: 1500 (Bytes)

Example

```
> msubnet mtu LAN1 1492%
Set LAN1 subnet mtu as 1492
> msubnet mtu ?
Usage:
```

```

>msubnet mtu <interface> <value>

<interface>: LAN1~LAN4,IP_Routed_Subnet, <value>: 1000 ~ 1500
(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)
IP Routed Subnet MTU: 1500 (Bytes)

```

Telnet Command: ms subnet leasetime

This command is used to set leasetime for multi-subnet.

Syntax

msubnet leasetime <1/ 2/ 3/ 4> <Lease Time sec.>

Syntax Description

Parameter	Description
1/ 2/ 3/ 4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
Lease Time sec.	Enter a value (range: 10 to 259200).

Example

```

> ms subnet leasetime ?
% ms subnet leasetime <1/2/3/4 > <Lease Time (sec.)>
% Now: LAN1 86400; LAN2 259200; LAN3 259200; LAN4 259200
> ms subnet leasetime 2 2300
% Set LAN8 lease time: 300

```

Telnet Command: object ip obj

This command is used to create an IP object profile.

object ip obj **setdefault**

object ip obj *INDEX -v*

object ip obj *INDEX -n NAME*

object ip obj *INDEX -i INTERFACE*

object ip obj *INDEX -s INVERT*

object ip obj INDEX -a TYPE [START_IP] [END/MASK_IP]

Syntax Description

Parameter	Description
<i>set default</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number of the specified object profile.
<i>-v</i>	It means to view the information of the specified object profile. Example: <i>object ip obj 1 -v</i>
<i>-n NAME</i>	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: <i>object ip obj 9 -n bruce</i>
<i>-i INTERFACE</i>	It means to define an interface for the IP object. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=3, means WAN Example: <i>object ip obj 8 -i 0</i>
<i>-s INVERT</i>	It means to set invert selection for the object profile. INVERT=0, means disabling the function. INVERT=1, means enabling the function. Example: <i>object ip obj 3 -s 1</i>
<i>-a TYPE</i>	It means to set the address type and IP for the IP object profile. TYPE=0, means Mask TYPE=1, means Single TYPE=2, means Any TYPE=3, means Rang Example: <i>object ip obj 3 -a 2</i>
<i>[START_IP]</i>	When the TYPE is set with 2, you have to type an IP address as a starting point and another IP address as end point. Type an IP address.
<i>[END/MASK_IP]</i>	Type an IP address (different with START_IP) as the end IP address.

Example

```
> object ip obj 1 -n marketing
> object ip obj 1 -a 1 192.168.1.45
> object ip obj 1 -v
IP Object Profile 1
Name      :[marketing]
Interface:[Any]
Address type:[single]
Start ip address:[192.168.1.45]
End/Mask ip address:[0.0.0.0]
Invert Selection:[0]
```

Telnet Command: object ip grp

This command is used to integrate several IP objects under an IP group profile.

object ip grp setdefault

object ip grp INDEX -v

object ip grp INDEX -n NAME

object ip grp INDEX -i INTERFACE

object ip grp INDEX -a IP_OBJ_INDEX

Syntax Description

Parameter	Description
<i>set default</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]
[8:] [0]
[9:] [0]
[10:] [0]
[11:] [0]

> object ip grp 2 -i 1
> object ip grp 2 -a 1
IP Group Profile 2
Name      :[First]
Interface:[Lan]
Included ip object index:
[0:] [1]
[1:] [0]
[2:] [0]
[3:] [0]
```

```
[4:] [0]
[5:] [0]
[6:] [0]
[7:] [0]
[8:] [0]
[9:] [0]
[10:] [0]
[11:] [0]
```

Telnet Command: object ipv6 obj

This command is used to create an IP object profile.

object ipv6 obj setdefault

object ipv6 obj INDEX -v

object ipv6 obj INDEX -n NAME

object ipv6 obj INDEX -i INTERFACE

object ipv6 obj INDEX -s INVERT

object ipv6 obj INDEX -a TYPE <START_IP><END_IP>/ <Prefix Length>

Syntax Description

Parameter	Description
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number of the specified object profile.
<i>-v</i>	It means to view the information of the specified object profile. Example: <i>object ipv6 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 ipv6 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 ipv6 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 ipv6 obj 3 -s 1</i>
<i>-e [0/ 1]</i>	It means to set the match type of the IPv6 object profile. 0: means 128 Bits 1: means suffix 64 bits interface ID.
<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 TYPE=4, means MAC Example: <i>object ipv6 obj 3 -a 2</i>

<START_IP><END_IP>	When the TYPE is set with 0, 1,3, you have to type an IP address as a starting point and another IP address as end point. Type the IP address(es) based on the selection of TYPE.
<Prefix Length>	When the TYPE is set with 0, 1 or 3, you have to enter a number as prefix length for the IPv6 address.

Example

```
> obj ipv6 obj 3 -a 3 2607:f0d0:1002:51::4 2607:f0d0:1002:51::4
Setting saved.
> obj ipv6 obj 3 -v
IPv6 Object Profile 3
Name      :[]
Address Type:[range]
Start IPv6 Address:[2607:F0D0:1002:51::4]
End IPv6 Address:[2607:F0D0:1002:51::4]
Prefix Length:[0]
MAC Address:[00:00:00:00:00:00]
Invert Selection:[0]
Match Type:[0]
```

Telnet Command: object ipv6 grp

This command is used to integrate several IP objects under an IP group profile.

object ipv6 grp setdefault

object ipv6 grp INDEX -v

object ipv6 grp INDEX -n NAME

object ipv6 grp INDEX -a IP_OBJ_INDEX

Syntax Description

Parameter	Description
<i>set default</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>-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 ipv6 grp 1 -n marketingtest
IP Group Profile 1
Name      :[marketingtest]
Included ip object index:
[0:][0]
[1:][0]
```

```

[2:] [0]
[3:] [0]
[4:] [0]
[5:] [0]
[6:] [0]
[7:] [0]

> object ipv6 grp 1 -a 1 2 3 4 5
> IPv6 Group Profile 1
Name      :[marketingtest]
Included ip object index:
[0:] [1]
[1:] [2]
[2:] [3]
[3:] [4]
[4:] [5]
[5:] [0]
[6:] [0]
[7:] [0]

```

Telnet Command: object country obj

This command is used to create country object profile.

Syntax

```

object country set INDEX -v
object country set INDEX -n NAME
object country set INDEX -a COUNTRY_INDEX
object country activate
object country setdefault
object country list

```

Syntax Description

Parameter	Description
<i>INDEX</i>	It means the index number of the specified country object profile (1 to 32).
<i>COUNTRY_INDEX</i>	It means the code number of a country. To get the detailed information of the code number, use "object country list" to get the one you need.
<i>activate</i>	It means to activate the country object profile.
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>list</i>	Displays a list of country with code number. For example, "222" means "Taiwan"; "241" means "United States".

Example

```

> object country set 1 -n Best
> Object country set 1 -a 222
Country object Profile 1
Name      :[Best]
Included country index:
[0:] [222] Taiwan

Set ok!

```

>

Telnet Command: **object service obj**

This command is used to create service object profile.

object service obj setdefault

object service obj INDEX -v

object service obj INDEX -n NAME

object service obj INDEX -p PROTOCOL

object service obj INDEX -s CHK [START_P] [END_P]

object service obj INDEX -d CHK [START_P] [END_P]

Syntax Description

Parameter	Description
<i>set default</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number of the specified service object profile.
<i>-v</i>	It means to view the information of the specified service object profile. Example: <i>object service obj 1 -v</i>
<i>-n NAME</i>	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: <i>object service obj 9 -n bruce</i>
<i>-i PROTOCOL</i>	It means to define a PROTOCOL for the service object profile. PROTOCOL =0, means any PROTOCOL =1, means ICMP PROTOCOL =2, means IGMP PROTOCOL =6, means TCP PROTOCOL =17, means UDP PROTOCOL =255, means TCP/UDP Other values mean other protocols. Example: <i>object service obj 8 -i 0</i>
<i>CHK</i>	It means the check action for the port setting. 0=equal(=), when the starting port and ending port values are the same, it indicates one port; when the starting port and ending port values are different, it indicates a range for the port and available for this service type. 1=not equal(!=), when the starting port and ending port values are the same, it indicates all the ports except the port defined here; when the starting port and ending port values are different, it indicates that all the ports except the range defined here are available for this service type. 2=larger(>), the port number greater than this value is available.. 3=less(<), the port number less than this value is available for this profile.
<i>-s CHK [START_P] [END_P]</i>	It means to set source port check and configure port range (1-65565) for TCP/UDP. START_P: Enter a port number to indicate the starting source port. END_P: Enter a port number to indicate the ending source port. Example: <i>object service obj 3 -s 0 100 200</i>
<i>-d CHK [START_P] [END_P]</i>	It means to set destination port check and configure port range

	(1-65565) for TCP/UDP. START_P: Enter a port number to indicate the starting destination port. END_P: Enter a port number to indicate the ending destination port. Example: <i>object service obj 3 -d 1 100 200</i>

Example

```

> object service obj 1 -n limit
> object service obj 1 -p 255
> object service obj 1 -s 1 120 240
> object service obj 1 -d 1 200 220
> object service obj 1 -v
Service Object Profile 1
Name      :[limit]
Protocol:[255]
Source port check action:[!=]
Source port range:[120~240]
Destination port check action:[!=]
Destination port range:[200~220]

```

Telnet Command: object service grp

This command is used to integrate several service objects under a service group profile.

object service grp setdefault

object service grp INDEX -v

object service grp INDEX -n NAME

object service grp INDEX -a SER_OBJ_INDEX

Syntax Description

Parameter	Description
<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 service grp 1 -v</i>
<i>-n NAME</i>	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.

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>set default</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.

object fe show

object fe setdefault

object fe obj INDEX -v

object fe obj INDEX -n NAME

object fe obj INDEX -e CATEGORY| FILE_EXTENSION

object fe obj INDEX -d CATEGORY| FILE_EXTENSION

Syntax Description

Parameter	Description
<i>show</i>	It means to show the contents for all of the profiles.
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number (from 1 to 8) of the specified file extension object profile.
<i>-v</i>	It means to view the information of the specified file extension object profile.
<i>-n NAME</i>	It means to define a name for the file extension object profile. NAME: Type a name with less than 15 characters.
<i>-e</i>	It means to enable the specific CATEGORY or FILE_EXTENSION.
<i>-d</i>	It means to disable the specific CATEGORY or FILE_EXTENSION
<i>CATEGORY FILE_EXTENSION</i>	CATEGORY: Image, Video, Audio, Java, ActiveX, Compression, Execution Example: <i>object fe obj 1 -e Image</i> FILE_EXTENSION: ".bmp", ".dib", ".gif", ".jpeg", ".jpg", ".jpg2", ".jp2", ".pct", ".pcx", ".pic", ".pict", ".png", ".tif", ".tiff", ".ico", ".asf", ".avi", ".mov", ".mpe", ".mpeg", ".mpg", ".mp4", ".qt", ".rm", ".wmv", ".3gp", ".3gpp", ".3gpp2", ".3g2", ".flv", ".swf", ".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", ".vrn", ".ace", ".arj", ".bzip2", ".bz2", ".cab", ".gz", ".gzip", ".rar", ".sit", ".zip", ".bas", ".bat", ".com", ".exe", ".inf", ".pif", ".reg", ".scr", ".torrent", ".doc", ".docx", ".odp", ".ods", ".odt", ".pdf", ".ppt", ".pptx", ".xls", ".xlsx" Example: <i>object fe obj 1 -e .bmp</i>

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
[ ].vrn
-----
Compression category:
[ ].ace [ ].arj [ ].bzip2 [ ].bz2 [ ].cab [ ].gz [ ].gzip [ ].rar
[ ].sit [ ].zip
-----
Execution category:
[ ].bas [ ].bat [ ].com [ ].exe [ ].inf [ ].pif [ ].reg [ ].scr
...
```

Telnet Command: object sms

This command is used to create short message object profile.

Syntax

```
object sms show
object sms setdefault
object sms obj INDEX -v
object sms obj INDEX -n NAME
object sms obj INDEX -s Service Provider
object sms obj INDEX -u Username
object sms obj INDEX -p Password
object sms obj INDEX -q Quota
object sms obj INDEX -i Interval
object sms obj INDEX -l URL
```

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 10) of the specified SMS

	object profile.
-v	It means to view the information of the specified SMS object profile.
-n [NAME]	It means to define a name for the SMS object profile. NAME: Type a name with less than 15 characters.
-s [Service Provider]	It means to specify the number of the service provider which offers the service of SMS. Different numbers represent different service provider. 0 : kotsms.com.tw (TW) 2 : textmarketer.co.uk (UK) 4 : messagemedia.co.uk (UK) 5 : bulksms.com (INT) 6 : bulksms.co.uk (UK) 7 : bulksms.2way.co.za (ZA) 8 : bulksms.com.es (ES) 9 : usa.bulksms.com (US) 10 : bulksms.de (DE) 11 : www.pswin.com (EU) 12 : www.messagebird.com (EU) 13 : www.lusosms.com (EU) 14 : www.vibeactivemedia.com (UK)
-u [Username]	It means to define a user name for the SMS object profile. Type a user name that the sender can use to register to selected SMS provider.
-p [Password]	It means to define a password for the SMS object profile. Type a password that the sender can use to register to selected SMS provider.
-q [Quota]	Enter the number of the credit that you purchase from the service provider. Note that one credit equals to one SMS text message on the standard route.
-I [Interval]	It means to set the sending interval for the SMS to be delivered. Enter the shortest time interval for the system to send SMS.
-l [URL]	It means to set the URL for Custom 1 and Custom 2 profiles. The profile name for Custom 1 and Custom 2 are defined in default and can not be changed.

Example

```

> object sms obj 1 -n CTC
> object sms obj 1 -s 0
> object sms obj 1 -u carrie
> object sms obj 1 -p 19971125cm
> object sms obj 1 -q 2
> object sms obj 1 -i 50
> object sms obj 1 -v
Profile Index: 1
Profile Name:[CTC]
SMS Provider:[kotsms.com.tw (TW)]
Username:[carrie]
Password:[*****]
Quota:[2]
Sending Interval:[50(seconds)]

```

Telnet Command: object mail

This command is used to create mail object profile.

Syntax

object mail show

object mail setdefault

object mail obj INDEX -v

object mail obj INDEX -n Profile Name

object mail obj INDEX -I Connection security

object mail obj INDEX -s SMTP Server

object mail obj INDEX -l Use SSL

object mail obj INDEX -m SMTP Port

object mail obj INDEX -a Sender Address
object mail obj INDEX -t Authentication
object mail obj INDEX -u Username
object mail obj INDEX -p Password
object mail obj INDEX -i Sending Interval

Syntax Description

Parameter	Description
<i>show</i>	It means to show the contents for all of the profiles.
<i>set default</i>	It means to return to default settings for all profiles.
[INDEX]	It means the index number (from 1 to 10) of the specified mail object profile.
-v	It means to view the information of the specified mail object profile.
-n [Profile Name]	It means to define a name for the mail object profile. <i>Profile Name:</i> Type a name with less than 15 characters.
-l Connection security	It means to set the connection security (0 to 3). 0: Plaintext 1: SSL 2: StartTLS ,nice to have 3: StartTLS ,MUST
-s [SMTP Server]	It means to set the IP address of the mail server.
-l [Use SSL]	It means to use port 465 for SMTP server for some e-mail server uses https as the transmission method. 0 - disable 1 - enable to use the port number.
-m [SMTP Port]	It means to set the port number for SMTP server.
-a [Sender Address]	It means to set the e-mail address (e.g., johnwash@abc.com.tw) of the sender.
-t Authentication	The mail server must be authenticated with the correct username and password to have the right of sending message out. 0 - disable 1 - enable to use the port number.
-u Username	Type a name for authentication. The maximum length of the name you can set is 31 characters.
-p Password	Type a password for authentication. The maximum length of the password you can set is 31 characters.
-i Sending Interval	Define the interval for the system to send the SMS out. The unit is second.

Example

```

> object mail obj 1 -n buyer
> object mail obj 1 -s 192.168.1.98
> object mail obj 1 -m 25
> object mail obj 1 -t 1
> object mail obj 1 -u john
> object mail obj 1 -p happy123456
> object mail obj 1 -i 25
  
```

```

> object mail obj 1 -v
Profile Index: 1
Profile Name:[buyer]
SMTP Server:[192.168.1.98]
SMTP Port:[25]
Sender Address:[]
Use SSL:[disable]
Authentication:[enable]
Username:[john]
Password:[*****]
Sending Interval:[25(seconds)]

```

Telnet Command: object noti

This command is used to create notification object profile.

Syntax

object noti show

object noti setdefault

object noti obj INDEX -v

object noti obj INDEX -n Profile Name

object noti obj INDEX -e Category Status

object noti obj INDEX -d Category Status

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 notification object profile.
<i>-v</i>	It means to view the information of the specified notification object profile.
<i>-n [Profile Name]</i>	It means to define a name for the notification object profile. <i>Profile Name:</i> Type a name with less than 15 characters.
<i>-e</i>	It means to enable the status of specified category.
<i>-d</i>	It means to disable the status of specified category.
<i>[Category]</i>	Available categories are: 1: WAN; 2: VPN Tunnel; 3: Temperature Alert; 4: WAN Budget; 5: CVM; 9: Security
<i>[status]</i>	For WAN - 1: Disconnected; 2: Reconnected. For VPN Tunnel - 1: Disconnected; 2: Reconnected. For Temperature Alert - 1: Out of Range. For WAN Budget - 1: Limit Reached. For Security - 1 : Web Log-in event occurs. 2 : Telnet Log-in event occurs. 3 : SSH Log-in event occurs. 4 : TR069 Log-in event occurs. 5 : FTP User Log-in event occurs. 6 : Config-Changed event occurs.

Example

```

> object noti obj 1 -n market
> object noti obj 1 -e 1 1
> object noti obj 1 -e 2 1
> object noti obj 1 -e 9 1
> object noti obj 1 -v

```

```

Profile Index: 1
Profile Name:[]
    Category                               Status
WAN [v]Disconnected [ ]Reconnected
VPN Tunnel [v]Disconnected [ ]Reconnected
Temperature Alert [ ]Out of Range
WAN Budget Alert [ ]Limit Reached
Security [v]Web Log-in event occurs
[ ]Telnet Log-in event occurs
[ ]SSH Log-in event occurs
[ ]TR069 Log-in event occurs
[ ]FTP User Log-in event occurs
[ ]Config-Changed event occurs
>

```

Telnet Command: object schedule

This command is used to create schedule object profile.

Syntax

object schedule set *INDEX option*

object schedule view

object schedule setdefault

Syntax Description

Parameter	Description
<i>set</i>	It means to set the schedule profile.
<i>[INDEX]</i>	It means the index number (from 1 to 15) of the specified object profile.
<i>option</i>	Available options for schedule.
<i>-e [value]</i>	It means to enable the schedule setup. 0 - disable 1 - enable
<i>-c [comment]</i>	It means to set brief description for the specified profile. The length range of the comment: 0 ~ 32 characters.
<i>-D [year][month][day]</i>	It means to set the starting date of the profile. [year] - Must be between 2000-2049. [month] - Must be between 1-12. [day] - Must be between 1-31. For example: To set Start Date 2015/10/6, type > <i>object schedule set 1 -D "2015 10 6"</i>
<i>-T [hour][minute]</i>	It means to set the starting time of the profile. [hour] - Must be between 0-23. [minute] - Must be between 0-59. For example: To set Start Time 10:20, type > <i>object schedule set 1 -T "10 20"</i>
<i>-d [hour][minute]</i>	It means to set the duration time of the profile. [hour] - Must be between 0-23. [minute] - Must be between 0-59. For example: To set Duration Time 3:30, type > <i>object schedule set 1 -d "3 30"</i>
<i>-a [value]</i>	It means to set the action used for the profile. [value] - 0:Force On, 1:Force Down, 2:Enable Dial-On-Demand, 3:Disable Dial-On-Demand
<i>-l [value]</i>	It means to set idle time. [value] - Must be between 0-255(minute). The default is 0.
<i>-h [option] [day]</i>	Set how often the schedule will be applied. [option] - 0: Once, 1: Weekdays [day] - Sun, Mon, Tue, Wed, Thu, Fri, Sat If the [option] set Weekdays, then must select which days of Week. example: To select Sunday, Monday, Thursday, type > <i>object schedule set 1 -h "1 Sun Mon Thu"</i>

<code>view [INDEX]</code>	It means to show the content of the profile.
<code>setdefault</code>	It means to return to default settings for all profiles.

Example

```
> object schedule set 1 -e 1
> object schedule set 1 -c Working
> object schedule set 1 -D "2016 11 8"
> object schedule set 1 -T "8 1"
> object schedule set 1 -d "2 30"
> object schedule set 1 -a 0
> object schedule set 1 -h "1 Mon Wed"
> object schedule view 1
Index No.1

-----

[v] Enable Schedule Setup
    Comment [ Working ]
    Start Date (yyyy-mm-dd) [ 2016 ]-[ 11 ]-[ 8 ]
    Start Time (hh:mm)      [ 8 ]:[ 1 ]
    Duration Time (hh:mm)   [ 2 ]:[ 30 ]
    Action                  [ Force On ]
    Idle Timeout            [ 0 ] minute(s).(max. 255, 0 for
                                default)

-----

How Often
[ ] Once
[v] Weekdays
    [ ]Sun [v]Mon [ ]Tue [v]Wed [ ]Thu [ ]Fri [ ]Sat

>
```

Telnet Command: port

This command allows users to set the speed for specific port of the router.

Syntax

port <1, 2, 3, 4, all> <AN, 1G, 100F, 100H, 10F, 10H, status>

port <wan2> <AN, 1000F, 100F, 100H, 10F, 10H, status>

port <enable, disable><1, 2, 3, 4, all>

port status

port sniff <on, off, port, txrx, restart, status>

port 802.1x <enable, disable, status, addport, delport>

port jumbo

port wanfc

Syntax Description

Parameter	Description
1, 2, 3, 4, 5, 6, wan2, all	It means the number of LAN port and WAN port.
AN... 10H	It means the physical type for the specific port. AN: auto-negotiate. 1G: 1G 1000F: 1000M Full Duplex. 100F: 100M Full Duplex. 100H: 100M Half Duplex. 10F: 10M Full Duplex. 10H: 10M Half Duplex.
status	It means to view the Ethernet port status.
sniff <on, off, port, txrx, restart, status>	Set the LAN Port Mirror function. On: Enable the function. Off: Disable the function. Port: Set the mirror port. E.g., port sniff p1 TXRX: Set the port number to be mirrored for transmitting/receiving the packets. E.g., port sniff txrx p2 p3 Restart: After finished the setting, use such command to activate port mirror function. Status: Display the status of LAN port mirror.
802.1x <enable, disable, status, addport, delport>	Each LAN port with Wired 802.1x configured will only forward 802.1x packets and block all other packets until the authentication has successfully completed. enable: Enable the function. disable: Disable the function. Status: Display the status of 802.1x configuration. Addport: Set the interface (LAN port 1 ~ 4) for applying 802.1x. E.g., 802.1x addport 1 Delport: Delete the interface (LAN port 1-4) with 802.1x applied. E.g., 802.1x delport 1
wanfc	It means to set WAN flow control.

Example

```
> port 1 100F
%Set Port 1 Force speed 100 Full duplex OK !!!
```

Telnet Command: portmaptime

This command allows you to set a time of keeping the session connection for specified protocol.

portmaptime [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-t <sec>	It means "TCP" protocol. <sec>: Type a number to set the TCP session timeout.
-u <sec>	It means "UDP" protocol. <sec>: Type a number to set the UDP session timeout.
-i <sec>	It means "IGMP" protocol. <sec>: Type a number to set the IGMP session timeout.
-w <sec>	It means "TCP WWW" protocol. <sec>: Type a number to set the TCP WWW session timeout.
-s <sec>	It means "TCP SYN" protocol. <sec>: Type a number to set the TCP SYN session timeout.
-f	It means to flush all portmaps (useful for diagnostics).
-l <List>	List all settings.

Example

```
> portmaptime -t 86400 -u 300 -i 10
> portmaptime -l
----- Current setting -----
TCP Timeout      : 86400 sec.
UDP Timeout      : 300 sec.
IGMP Timeout     : 10 sec.
TCP WWW Timeout  : 60 sec.
TCP SYN Timeout  : 60 sec.
```

Telnet Command: ppa

This command allows you to configure PPA mode.

ppa [-<command> <parameter> | ...]

ppa n [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can Enter several commands in one

	line.
-z <1/0>	Enable (1) or disable (0) the PPPA hardware acceleration function.
-m <mode>	Specify a mode. 1=auto 2=manual(traffic) 3=manual(qos) 4=manual(specific hosts) 0=disable
-p <proto>	Specify a protocol. proto - 1-TCP; 2-UDP; 3-Both.
-b 1/0	Enable/disable TWO-way hardware acceleration function.
-M enable/disable	Enable/disable the multicast hardware acceleration.
-S	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>	Enter 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 acceleration is disable

> ppa -v
%PPA is disabled
%PPA NAT is disabled
%PPA Protocol TCP 0, UDP 0
%PPA Multicast is enabled
%PPA two way enable
%PPA time is 10
%PPA range is 8000
%PAE range is 2048
%MPE range is 5952
%PPA LAN entries 0, working 0
%PPA WAN entries 0, working 0
%PPA statistics interval: 5 sec
> ppa -x
WAN1 status : Enable
WAN1 phy_type : VDSL
WAN1 session check = hw_acc_general
WAN2 status : Disable
WAN2 phy_type : ETHERNET
WAN2 session check = NULL

```

Telnet Command: prn

This command allows you to view current status (interface and driver) of USB printer.

prn status

prn debug

Example

```
> prn status
Interface: USB bus 2.0
Printer: NotReady

> prn debug
conn[0] :
none
conn[1] :
none
conn[2] :
none
conn[3] :
none
LPD_data_total=0

usbip_ptr=0
UsbPrintReady=0, UsbIsPrinting=0
```

Telnet Command: qos setup

This command allows user to set general settings for QoS.

Syntax

qos setup [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-h	Type it to display the usage of this command.
-W <1~3>	It means to select an interface. <1~3>: 1 is WAN1; 2 is WAN2; 3 is WAN3. The default is WAN1.
-m <mode>	It means to define which traffic the QoS control settings will apply to and enable QoS control. 0: disable. 1: in, apply to incoming traffic only. 2: out, apply to outgoing traffic only. 3: both, apply to both incoming and outgoing traffic. Default is enable (for outgoing traffic).
-i <bandwidth>	It means to set inbound bandwidth in kbps (Ethernet WAN only). The available setting is from 1 to 100000.
-o <bandwidth>	It means to set outbound bandwidth in kbps (Ethernet WAN only). The available setting is from 1 to 100000.

<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>-I <bandwidth></code>	It means the minimum available non-VoIP Inbound Bandwidth when VoIP is detected (Kbps). <bandwidth>: Enter a value. Default value: half of WAN inbound bandwidth.
<code>-O <bandwidth></code>	It means the minimum available non-VoIP Outbound Bandwidth when VoIP is detected (Kbps). <bandwidth>: Enter a value. Default value: half of WAN outbound bandwidth.
<code>-v <0/ 1></code>	It means to adjust to minimum In/Out bandwidth setting (or half QoS bandwidth). 0: Auto bandwidth adjustment. 1: When VoIP detected, QoS In/Out bandwidth will be adjusted to minimum values.
<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 -W 2 -m 3 -i 9500 -o 8500 -r 3:20 -u 1 -p 50 -t 1
Setup WAN2 !!!!
WAN2 QoS mode is both
inbound bandwidth set to 9500
outbound bandwidth set to 8500
WAN2 class 3 ratio set to 20
WAN2 udp bandwidth control set to enable
WAN2 udp bandwidth limit ratio set to 50
WAN2 Outbound TCP ACK Prioritizel set to enable
QoS WAN2 set complete; restart QoS
>
```

Telnet Command: qos class

This command allows user to set QoS class.

Syntax

qos class -c [*no*] [-*a*/*e*/*d*] [*no*][-<command> <parameter> | ...]

Syntax Description

Parameter	Description
[<command> <parameter> ..]	The available commands with parameters are listed below. [..] means that you can type in several commands in one line.
-h	Type it to display the usage of this command.
-c <no>	Specify the inde number for the class. Available value for <no> contains 1, 2 and 3. The default setting is class 1.
-n <name>	It means to type a name for the class.
-a	It means to add rule for specified class.
-e <no>	It means to edit specified rule. <no>: 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".0 <i>any</i> -It means Any address. Simple type "-l" to specify any address for this command.
-r <addr>	Set the remote address. <i>addr1</i> - It means Single address. Please specify the IP address directly, for example, "-r 172.16.3.9". <i>addr1:addr2</i> - It means Range address. Please specify the IP addresses, for example, "-r 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, "-r 172.16.3.9:255.255.0.0".0 <i>any</i> -It means Any address. Simple type "-r" to specify any address for this command.
-p <DSCP id>	Specify the ID.
-s <Service type>	Specify the predefined service type by typing the number. The available types are listed as below: 1:ANY 2:DNS 3:FTP 4:GRE 5:H.323 6:HTTP 7:HTTPS 8:IKE 9:IPSEC-AH 10:IPSEC-ESP 11:IRC 12:L2TP 13:NEWS 14:NFS 15:NNTP 16:PING 17:POP3 18:PPTP 19:REAL-AUDIO 20:RTSP 21:SFTP 22:SIP 23:SMTP 24:SNMP 25:SNMP-TRAPS 26:SQL-NET 27:SSH 28:SYSLOG 29:TELNET 30:TFTP

-u <Service type>	Specify the user defined service type by typing the number (1 to 40).
-S <d/ s>	Show the content for specified DSCP ID/Service type.
-V <1/ 2/ 3>	Show the rule in the specified class.

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
-a <name>	It means to add rule.
-e <no>	It means to edit user defined service type. "no" means the index number. Available numbers are 1-40.
-d <no>	It means to delete user defined service type. "no" means the index number. Available numbers are 1-40.
-n <name>	It means the name of the service.
-t <type>	It means protocol type. 6: tcp(default) 17: udp 0: tcp/udp <1-254>: other
-p <port>	It means service port. The typing format must be [start:end] (ex., 510:330).
-l	List user defined types. "no" means the index number. Available numbers are 1-40.

Example

```
> qos type -a draytek -t 6 -p 510:1330

service name set to draytek
service type set to 6:TCP
Port type set to Range
Service Port set to 510 ~ 1330
>
```

Telnet Command: qos voip

This command allows user to enable or disable the QoS for VoIP and RTP.

Syntax

qos voip [*on/off*]

Syntax Description

Parameter	Description
<i>on/off</i>	On - Enable the QoS for VoIP. Off - Disable th QoS for VoIP.

Example

```
> qos voip off
QoS for VoIP: Disable; SIP Port: 5060
```

Telnet Command: quit

This command can exit the telnet command screen.

Telnet Command: show lan

This command displays current status of LAN IP address settings.

Example

```
> show lan
The LAN settings:
Status   IP                Mask                DHCP Start IP      Pool Gateway
-----
[V]LAN1  192.168.1.1       255.255.255.0      V   192.168.1.10      200
192.168.1.1

[X]LAN2  192.168.2.1       255.255.255.0      V   192.168.2.90     100
192.168.2.1

[X]LAN3  192.168.3.1       255.255.255.0      V   192.168.3.10     100
192.168.3.1

[X]LAN4  192.168.4.1       255.255.255.0      V   192.168.4.10     100
192.168.4.1

[X]Route 192.168.0.1       255.255.255.0      V   0.0.0.0          0   192.168.0.1
```

Telnet Command: show dmz

This command displays current status of DMZ host.

Example

```
> show dmz
%      WAN1 DMZ mapping status:
Index  Status  WAN1 aux IP    Private IP
-----
1      Disable 0.0.0.0

%      WAN2 DMZ mapping status:
Index  Status  WAN2 aux IP    Private IP
-----
1      Disable 0.0.0.0

%      WAN3 DMZ mapping status:
Index  Status  WAN3 aux IP    Private IP
-----
1      Disable 0.0.0.0

%      WAN4 DMZ mapping status:
Index  Status  WAN4 aux IP    Private IP
-----
1      Disable 0.0.0.0
```

Telnet Command: show dns

This command displays current status of DNS setting

Example

```
> show dns
%%      Domain name server settings:
% LAN1  Primary DNS: [Not set]
% LAN1  Secondary DNS: [Not set]

% LAN2  Primary DNS: [Not set]
% LAN2  Secondary DNS: [Not set]

% LAN3  Primary DNS: [Not set]
% LAN3  Secondary DNS: [Not set]

% LAN4  Primary DNS: [Not set]
% LAN4  Secondary DNS: [Not set]
```

Telnet Command: show openport

This command displays current status of open port setting.

Example

```
> show openport
```



```

%%      Openport settings:
Index   Status  Comment           Local IP Address
*****
                        No data entry.

```

Telnet Command: show nat

This command displays current status of NAT.

Example

```

> show nat
Port Redirection Running Table:

Index  Protocol  Public Port  Private IP      Private Port
-----
1      0           0           0.0.0.0         0
2      0           0           0.0.0.0         0
3      0           0           0.0.0.0         0
4      0           0           0.0.0.0         0
5      0           0           0.0.0.0         0
6      0           0           0.0.0.0         0
7      0           0           0.0.0.0         0
8      0           0           0.0.0.0         0
9      0           0           0.0.0.0         0
10     0           0           0.0.0.0         0
11     0           0           0.0.0.0         0
12     0           0           0.0.0.0         0
13     0           0           0.0.0.0         0
14     0           0           0.0.0.0         0
15     0           0           0.0.0.0         0
16     0           0           0.0.0.0         0
17     0           0           0.0.0.0         0
18     0           0           0.0.0.0         0
19     0           0           0.0.0.0         0
20     0           0           0.0.0.0         0
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]

```

Telnet Command: show portmap

This command displays the table of NAT Active Sessions.

Example

```

> show portmap
-----
Private_IP:Port Pseudo_IP:Port Peer_IP:Port [Timeout/Protocol/Flag]
-----

```

Telnet Command: show pmtime

This command displays the reuse time of NAT session.

Level0: It is the default setting.

Level1: It will be applied when the NAT sessions are smaller than 25% of the default setting.

Level2: It will be applied when the NAT sessions are smaller than the eighth of the default setting.

Example

```
> show pmtime
Level0 TCP=86400001 UDP=300001 ICMP=10001
Level1 TCP=600000 UDP=90000 ICMP=7000
Level2 TCP=60000 UDP=30000 ICMP=5000
```

Telnet Command: show session

This command displays current status of current session.

Example

```
> show session
% Maximum Session Number: 50000
% Maximum Session Usage: 0
% Current Session Usage: 0
% Current Session Used(include waiting for free): 0
% WAN1 Current Session Usage: 0
% WAN2 Current Session Usage: 0
% WAN3 Current Session Usage: 0
% WAN4 Current Session Usage: 0
>
```

Telnet Command: show status

This command displays current status of LAN and WAN connections.

Example

```
> show status
System Uptime:1:4:49
LAN Status
Primary DNS:8.8.8.8      Secondary DNS:8.8.4.4
IP Address:192.168.1.1   Tx Rate:3266   Rx Rate:2245

WAN 1 Status: Disconnected
Enable:Yes      Line:xDSL      Name:
Mode:PPPoE      Up Time:0:00:00   IP:---      GW IP:---
TX Packets:0      TX Rate:0   RX Packets:0      RX Rate:0

WAN 2 Status: Disconnected
Enable:Yes      Line:Ethernet   Name:
Mode:---      Up Time:0:00:00   IP:---      GW IP:---
TX Packets:0      TX Rate:0   RX Packets:0      RX Rate:0

WAN 3 Status: Disconnected
Enable:Yes      Line:USB      Name:
Mode:---      Up Time:0:00:00   IP:---      GW IP:---
TX Packets:0      TX Rate:0   RX Packets:0      RX Rate:0

WAN 4 Status: Disconnected
Enable:Yes      Line:USB      Name:
```

Telnet Command: show adsl

This command displays current status of ADSL.

Example

```
> show adsl
----- ATU-R Info (hw: annex A, f/w: annex A) -----
Running Mode      :                      State      : TRAINING
DS Actual Rate    :          0 bps   US Actual Rate    :          0 bps
DS Attainable Rate :          0 bps   US Attainable Rate :          0 bps
DS Path Mode      :          Fast    US Path Mode      :          Fast
DS Interleave Depth :          0     US Interleave Depth :          0
NE Current Attenuation :          0 dB   Cur SNR Margin    :          0 dB
DS actual PSD     :          0.0 dB   US actual PSD     :          0.0 dB
NE Rcvd Cells     :          0       NE Xmitted Cells    :          0
NE CRC Count      :          0       FE CRC Count      :          0
NE ES Count       :          0       FE ES Count      :          0
Xdsl Reset Times  :          0       Xdsl Link Times   :          0
ITU Version[0]    : b5004946        ITU Version[1]      : 544e0000
ADSL Firmware Version : 06-06-01-07-00-01
Power Management Mode : DSL_G997_PMS_NA
Test Mode         : DISABLE
----- ATU-C Info -----
Far Current Attenuation :          0 dB   Far SNR Margin    :          0 dB
CO ITU Version[0]      : 00000000        CO ITU Version[1] : 00000000
DSLAM CHIPSET VENDOR   : < ----- >

>
```

Telnet Command: show traffic

This command can display traffic graph for WAN1 to WAN4, transmitted bytes, received bytes and sessions.

Syntax

```
show traffic [wan1/ wan2/ wan3] [tx/ rx] [weekly]
```

show traffic *[ipaddr] [tx/rx]*

show traffic session *[weekly]*

```
show traffic ip [0/ 1]
```

Example

[illegible]


```
WAN1 total TX: 0 Bytes ,RX: 0 Bytes
WAN2 total TX: 0 Bytes ,RX: 0 Bytes
WAN3 total TX: 0 Bytes ,RX: 0 Bytes
WAN4 total TX: 0 Bytes ,RX: 0 Bytes
WAN5 total TX: 0 Bytes ,RX: 0 Bytes
WAN6 total TX: 0 Bytes ,RX: 0 Bytes
WAN7 total TX: 0 Bytes ,RX: 0 Bytes
> show statistic reset wan1
Reset WAN1 tx/rx Bytes to zero
>
```

Telnet Command: smb setting

This command is used to configure file sharing settings for SMB server.

Syntax

smb setting [*enable/ disable*]

smb setting *show status*

smb setting *set workgroup* [*Workgroup name*]

smb setting *set host* [*host name*]

smb setting *set access* [*LAN or LANWAN*]

smb setting *set version* [*v1v2/ v2*]

Syntax Description

Parameter	Description
<i>enable/ disable</i>	Enable or disable the SMB service.
<i>show status</i>	Display current status of SMB service.
<i>Set workgroup</i> [<i>Workgroup name</i>]	Set a name of workgroup for SMB service.
<i>set host</i> [<i>host name</i>]	Set a name of the host for SMB service.
<i>set access</i> [<i>LAN or LANWAN</i>]	Allow to access into SMB server by LAN or borth LA N and WAN.
<i>set version</i> [<i>v1v2/ vs</i>]	It means to set SMB server version.

Example

```
> smb setting enable
SMB service is enabled.

> smb setting set access LAN
Allow SMB access from LAN only.
>smb setting set version v1v2
SMB version: v1 and v2.
```

Telnet Command: srv dhcp dhcp2

This command is used to enable DCHP2 server.

Syntax

srv dhcp dhcp2 [*-<command> <parameter> | ...*]

Syntax Description

Parameter	Description
[<i><command></i> <i><parameter> ...</i>]	The available commands with parameters are listed below. [<i>...</i>] means that you can type in several commands in one line.
<i>-l<enable></i>	It menas to enable the LAN port to public DHCP. 0: Disenable 1: Enable
<i>-m<enable></i>	It menas to enable MAC address to public DHCP. 0: Disenable 1: Enable

-e<id>	It means to turn on the flag of LAN port 1/2.
-d<id>	It means to turn off the flag of LAN port 1/2.
-v	It means to view current status.

Example

```
> srv dhcp dhcp2 -l 1 -e 1
> srv dhcp dhcp2 -v
2nd DHCP server flag status --
  Server works on specified MAC address: ON
  Server works on specified LAN port: ON
  Port 1 flag: ON
  Port 2 flag: ON
```

Telnet Command: **srv dhcp public**

This command allows users to configure DHCP server for second subnet.

srv dhcp public start [*IP address*]

srv dhcp public cnt [*IP counts*]

srv dhcp public status

srv dhcp public add [*MAC Addr XX-XX-XX-XX-XX-XX*]

srv dhcp public del [*MAC Addr XX-XX-XX-XX-XX-XX all/ ALL*]

Syntax Description

Parameter	Description
<i>start</i> <IP address>	It means the starting point of the IP address pool for the DHCP server. <IP address>: Specify an IP address as the starting point in the IP address pool.
<i>cnt</i> <IP counts>	It means the IP count number. <IP counts>: 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> <MAC Addr XX-XX-XX-XX-XX-XX>	It means creating a list of hosts to be assigned. <MAC Addr XX-XX-XX-XX-XX-XX>: Specify MAC Address of the host.
<i>del</i> <MAC Addr XX-XX-XX-XX-XX-XX all/ ALL>	It means removing the selected MAC address. <MAC Addr XX-XX-XX-XX-XX-XX>: Specify MAC Address of the host. all/ALL: It means all of the MAC addresses.

Example

```
> ip route add 192.168.1.56 255.255.255.0 192.168.1.12 3 default
> 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 <lan1/ lan2/ lan3/ lan4> <DNS IP address>

Syntax Description

Parameter	Description
<i>lan1/lan2/lan3/lan4</i>	It means to sepcify the LAN interface for setting the DNS server.
<i>DNS IP address</i>	It means the IP address that you want to use as DNS1. Note: The IP Routed Subnet DNS must be the same as NAT Subnet DNS).

Example

```
> srv dhcp dns1 lan1 192.168.1.100
% srv dhcp dns1 lan1 <DNS IP address>
% Now: 192.168.1.100
>
```

Telnet Command: **srv dhcp dns2**

This command allows users to set Secondary IP Address for DNS Server in LAN.

Syntax

srv dhcp dns2 <*lan1/lan2/lan3/lan4*> <*DNS IP address*>

Syntax Description

Parameter	Description
<i><lan1/lan2/lan3/lan4</i>	It means to sepcify the LAN interface for setting the DNS server.
<i>DNS IP address</i>	It means the IP address that you want to use as DNS2. Note: The IP Routed Subnet DNS must be the same as NAT Subnet DNS).

Example

```
> srv dhcp dns2 10.1.1.1
% srv dhcp dns2 <DNS IP address>
% Now: 10.1.1.1
(IP Routed Subnet dns same as NAT Subnet dns)
```


Telnet Command: `srv dhcp frcdnsmanl`

This command can force the router to invoke DNS Server IP address.

`srv dhcp frcdnsmanl [on]`

`srv dhcp frcdnsmanl [off]`

Syntax Description

Parameter	Description
<i>on</i>	It means to use manual setting for DNS setting.
<i>Off</i>	It means to use auto settings acquired from ISP.

Example

```
> srv dhcp frcdnsmanl on
% Domain name server now is using manual settings!
> srv dhcp frcdnsmanl off
% Domain name server now is using auto settings!
```

Telnet Command: `srv dhcp gateway`

This command allows users to specify gateway address for DHCP server.

`srv dhcp gateway [Gateway IP]`

Syntax Description

Parameter	Description
<i>Gateway IP</i>	It means to specify a gateway address used for DHCP server.

Example

```
> srv dhcp gateway 192.168.2.1
This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

Telnet Command: **srv dhcp ipcnt**

This command allows users to specify IP counts for DHCP server.

srv dhcp ipcnt [*IP counts*]

Syntax Description

Parameter	Description
<i>IP counts</i>	It means the number that you have to specify for the DHCP server.

Example

```
> srv dhcp ipcnt ?  
% srv dhcp ipcnt <IP counts>  
% Now: 150
```

Telnet Command: **srv dhcp off**

This function allows users to turn off DHCP server. It needs rebooting router, please type "sys reboot" command to reboot router.

Telnet Command: **srv dhcp on**

This function allows users to turn on DHCP server. It needs rebooting router, please type "sys reboot" command to reboot router.

Telnet Command: **srv dhcp relay**

This command allows users to set DHCP relay setting.

srv dhcp relay servip [*server ip*]

srv dhcp relay 2nd_servip [*server ip*]

srv dhcp relay subnet [*index*]

Syntax Description

Parameter	Description
<i>server ip</i>	It means the IP address that you want to used as DHCP server.
<i>Index</i>	It means subnet 1 or 2. Please type 1 or 2. The router will invoke this function according to the subnet 1 or 2 specified here.

Example

```
> srv dhcp relay servip 192.168.1.46  
> srv dhcp relay subnet 2  
> srv dhcp relay servip ?  
% srv dhcp relay servip <server ip>  
% Now: 192.168.1.46
```

Telnet Command: **srv dhcp startip**

srv dhcp startip [*IP address*]

Syntax Description

Parameter	Description

<i>IP address</i>	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.

Syntax

srv dhcp status <LAN1/ 2/ 3/ 4/ ip_routed_subnet>

Example

```
> srv dhcp status
DHCP server: Relay Agent
Default gateway: 192.168.1.1
Index   IP Address      MAC Address      Leased Time      HOST ID
1       192.168.1.113   00-05-5D-E4-D8-EE  17:20:08         A1000351
```

Telnet Command: `srv dhcp leasetime`

This command can set the lease time for the DHCP server.

`srv dhcp leasetime` [*Lease Time (sec)*]

Syntax Description

Parameter	Description
<i>Lease Time (sec)</i>	It means the lease time that DHCP server can use. The unit is second.

Example

```
> srv dhcp leasetime ?
% srv dhcp leasetime <Lease Time (sec.)>
% Now: 86400
>
```

Telnet Command: `srv dhcp nodetype`

This command can set the node type for the DHCP server.

`srv dhcp nodetype` *<count>*

Syntax Description

Parameter	Description
<i>count</i>	It means to specify a type for node. 1. B-node 2. P-node 4. M-node 8. H-node

Example

```
> srv dhcp nodetype 1
> srv dhcp nodetype ?
%% srv dhcp nodetype <count>
%% 1. B-node 2. P-node 4. M-node 8. H-node
% Now: 1
```

Telnet Command: **srv dhcp primWINS**

This command can set the primary IP address for the DHCP server.

srv dhcp primWINS [*WINS IP address*]

srv dhcp primWINS clear

Syntax Description

Parameter	Description
<i>WINS IP address</i>	It means the IP address of primary WINS server.
<i>clear</i>	It means to remove the IP address settings of primary WINS server.

Example

```
> srv dhcp primWINS 192.168.1.88
> srv dhcp primWINS ?
%% srv dhcp primWINS <WINS IP address>
%% srv dhcp primWINS clear
% Now: 192.168.1.88
```

Telnet Command: **srv dhcp secWINS**

This command can set the secondary IP address for the DHCP server.

srv dhcp secWINS [*WINS IP address*]

srv dhcp secWINS clear

Syntax Description

Parameter	Description
<i>WINS IP address</i>	It means the IP address of secondary WINS server.
<i>clear</i>	It means to remove the IP address settings of second WINS server.

Example

```
> srv dhcp secWINS 192.168.1.180
> srv dhcp secWINS ?
%% srv dhcp secWINS <WINS IP address>
%% srv dhcp secWINS clear
% Now: 192.168.1.180
```

Telnet Command: **srv dhcp expRecycleIP**

This command can set the time to check if the IP address can be assigned again by DHCP server or not.

srv dhcp expRecycleIP <sec time>

Syntax Description

Parameter	Description
<i>sec time</i>	It means to set the time (5-300 seconds) for checking if the IP can be assigned again or not.

Example

```
> srv dhcp expRecycleIP 250
% DHCP expired_RecycleIP = 250
```

Telnet Command: **srv dhcp tftp**

This command can set the TFTP server as the DHCP server.

srv dhcp tftp <TFTP server name>

Syntax Description

Parameter	Description
<i>TFTP server name</i>	It means to 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 tftpdcl**

This command can remove the name defined for the TFTP server.

Syntax

srv dhcp tftpdcl

Example

```
> srv dhcp tftp TF123
> srv dhcp tftp ?
%% srv dhcp tftp <TFTP server name>
% Now: TF123
> srv dhcp tftpdcl
% The TFTP Server Name had been deleted !!!
```

Telnet Command: **srv dhcp option**

This command can set the custom option for the DHCP server.

srv dhcp option -h

srv dhcp option -/

srv dhcp option -d <idx>

srv dhcp option -e <1 or 0> -i <lan number> -s <Next Server IP Address>

srv dhcp option -e <1 or 0> -i <lan number> -c <option number> -v <option value>

srv dhcp option -e <1 or 0> -i <lan number> -c <option number> -x <option value>

srv dhcp option -e <1 or 0> -i <lan number> -c <option number> -a <option value>

srv dhcp option -u <idx number>

Syntax Description

Parameter	Description
-h	It means to display usage of this command.
-l	It means to display all the user defined DHCP options.
-d [idx]	It means to delete the option number by specifying its index number.
-e [1 or 0]	It means to enable/disable custom option feature. 1:enable 0:disable
-i <lan number>	<lan number> : It means to specify the LAN interface. 1: lan1 a: all LAN r: routed subnet d: DMZ
-s <Next Server IP Address>	It means to set the next server IP address. Next Server IP Address: Enter an IP address.
-c <option number>	It means to set option number. Available number ranges from 0 to 255. Option number: Enter a number.
-v <option value>	It means to set option number by typing string. option value: Enter a string.
-x <option value>	It means to set option number with the format of Hexadecimal characters. option value: Enter a number (hex).
-a <option value>	It means to set the option value by specifying the IP address. option value: Enter an IP address.
-u <idx number>	It means to update the option value of the sepecified index. idx number: Enter the index number of the option value.
-r	Remove all the custom DHCP server options.

Example

```
>srv dhcp option -e 1 -i 2/r -c 44 -a 192.168.1.10,192.168.1.20
```

Telnet Command: **srv nat dmz**

This command allows users to set DMZ host. Before using this command, please set WAN IP Alias first.

Srv nat dmz n m [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
<i>n</i>	It means to map selected WAN IP to certain host. 1: wan1 2: wan2
<i>m</i>	It means the index number (1 to 32) 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 ~ 32 in this field. If WAN IP alias has been configured, then the number of DMZ host can be added more.
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-e	It means to enable/disable such feature. 1:enable 0:disable
-i	It means to specify the private IP address of the DMZ host.
-r	It means to remove DMZ host setting.
-v	It means to display current status.

Example

```
> 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
[options]	The available commands with parameters are listed below.
<i>on</i>	It means to enable IPSec ESP tunnel passthrough and IKE source port (500) preservation.
<i>off</i>	It means to disable IPSec ESP tunnel passthrough and IKE source port (500) preservation.
<i>status</i>	It means to display current status for checking.

Example

```
> srv nat ipsecpass status
%% Status: IPsec ESP pass-thru and IKE src_port:500 preservation is
OFF.
```

Telnet Command: **srv nat openport**

This command allows users to set open port settings for NAT server.

srv nat openport n m [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
n	It means the index number for the profiles. The range is from 1 to 40.
m	It means to specify the sub-item number for this profile. The range is from 1 to 10.
-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.
-l <source ip idx>	It means to set source IP object. 1 to 192: for IP object 1 to 32: for IP group 0: Any For example: srv nat openport 1 1 -l 1 -g 0
-g <source ip type>	It means to set IP type. 0: IP object 1: IP group For example: srv nat openport 1 1 -l 1 -g 0
-i <local ip>	It means to set the IP address for local computer. Local ip: Type an IP address in this field.
-w <widx><ipidx>	widx: Specify the public IP. 1: WAN1 Default, 2: WAN1 Alias 1, ...and so on. ipidx: Specify the index number of an alias IP (1 to 32).
-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 192.168.1.55 -w 1 1 -p TCP -s
56
-e 83
Set WAN Port ok!!

DrayTek> srv nat openport 1 1 -v
%% Status: Enable
%% Comment: games
%% WAN Interface: WAN1
%% Private IP address: 192.168.1.55
Index   Protocol      Start Port    End Port
*****
  1.     TCP        56           83
>
```

Telnet Command: **srv nat portmap**

This command allows users to set port redirection table for NAT server.

srv nat portmap add *<idx>* *<serv name>* *<proto>* *<pub port>* *<src ip type>* *<src ip idx>* *<pri ip>*
<pri port> *<wan idx>* *<alias IP>*

srv nat portmap del *[idx]*

srv nat portmap disable *[idx]*

srv nat portmap enable *[idx]* *[proto]*

srv nat portmap flush

srv nat portmap table

srv nat portmap view

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 40.
<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><src ip type></i>	It means to specify the IP type (object or group). ip type: 0 means IP object; 1 means IP group.
<i><src ip idx></i>	It means to specify the index number of the object profile. ip idx: 1 to 192 for IP object profile; 1 to 32 for IP group profile. 0 means any object or group.
<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 (1 to 65535) of the service offered by the internal host.

<i><wan idx></i>	It means to specify WAN interface for the port redirection. Idx: wan1 to wan4, all
<i><alias IP></i>	It means to specify an alias IP by entering the index number (1 to 32). ip: 1 to 32.
<i>del <idx></i>	It means to remove the selected port redirection setting.
<i>disable <idx></i>	It means to inactivate the selected port redirection setting.
<i>enable <idx></i>	It means to activate the selected port redirection setting.
<i>flush</i>	It means to clear all the port mapping settings.
<i>table</i>	It means to display Port Redirection Configuration Table.

Example

```
> srv nat portmap add 1 game tcp 100 0 0 192.168.1.11 100 wan1 1
> srv nat portmap table
```

NAT Port Redirection Configuration Table:

Index	Service Name	Protocol	Public Port	Private IP	Private
Port ifno					
1	game	6	80	192.168.1.11	100
-1					
2		0	0		-2
3		0	0		-2
4		0	0		-2
5		0	0		-2
6		0	0		-2
7		0	0		-2
8		0	0		-2
9		0	0		-2
10		0	0		-2
11		0	0		-2
12		0	0		-2
13		0	0		-2
14		0	0		-2
15		0	0		-2
16		0	0		-2
17		0	0		-2
18		0	0		-2
19		0	0		-2
20		0	0		-2

Protocol: 0 = Disable, 6 = TCP, 17 = UDP

Telnet Command: **srv nat trigger**

This command allows users to configure port triggering settings for NAT.

Syntax

srv nat trigger setdefault

srv nat trigger view

srv nat trigger *n* [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
<i>setdefault</i>	Set to factory default settings.
<i>view</i>	Display all of the port triggering settings.
<i>n</i> <command><parameter> ...]	"n" means the rule number. The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-c [XXX]	Type a comment for such rule if required.
-e [0/ 1]	Enable (1) or disable (0) a rule (specified with rule number).
-s	Specify the index number of the IP object/group. Any: 255 IP object: 0-191 IP group: 0-31
-g [0/ 1]	Set the source IP type. 0: IP object; 1: IP group.
-p [1/ 2/ 3]	Specify the protocol for such trigger rule. 1 - TCP 2 - UDP 3 - All
-t	Specify the port number (0-65535) for trigger.
-P	Specify the incoming protocol for such trigger rule. 1 - TCP 2 - UDP 3 - All
-i	Specify the port number (0-65535) for incoming protocol.
-d	Delete the selected trigger rule.
-v	Display the port trigger settings for specified rule.

Example

```
> srv nat trigger 1 -c after_dinner
> srv nat trigger 1 -e 1
> srv nat trigger 1 -p 1
> srv nat trigger 1 -t 2000
> srv nat trigger 1 -P 2
> srv nat trigger 1 -i 3000
> srv nat trigger 1 -v
```

Port Trigger Rule Index:1

Status:Enable

Comment:after_dinner2000

Triggering Protocol:TCP

Triggering Port:2000

```
Incoming Protocol:UDP
Incoming Port:3000
```

Telnet Command: **srv nat status**

This command allows users to view NAT Port Redirection Running Table.

Example

```
> srv nat status
NAT Port Redirection Running Table:

Index  Protocol  Public Port  Private IP      Private Port
-----
1       6          80          192.168.1.11    100
2       0          0           0.0.0.0         0
3       0          0           0.0.0.0         0
4       0          0           0.0.0.0         0
5       0          0           0.0.0.0         0
6       0          0           0.0.0.0         0
7       0          0           0.0.0.0         0
8       0          0           0.0.0.0         0
9       0          0           0.0.0.0         0
10      0          0           0.0.0.0         0
11      0          0           0.0.0.0         0
12      0          0           0.0.0.0         0
13      0          0           0.0.0.0         0
14      0          0           0.0.0.0         0
15      0          0           0.0.0.0         0
16      0          0           0.0.0.0         0
17      0          0           0.0.0.0         0
18      0          0           0.0.0.0         0
19      0          0           0.0.0.0         0
20      0          0           0.0.0.0         0

--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
```

Telnet Command: **srv nat showall**

This command allows users to view a summary of NAT port redirection setting, open port and DMZ settings.

Example

```
> srv nat showall ?
Index  Proto  WAN IP:Port      Private IP:Port  Act
*****
R01    TCP    0.0.0.0:80       192.168.1.11:100  Y
O01    TCP    0.0.0.0:23~83    192.168.1.100:23~83  Y
D01    All    0.0.0.0          192.168.1.96     Y
```

Telnet Command: **srv nat pseudoctl**

This command allows users to check the pseudo port number to prevent from port conflict.

Syntax

srv nat pseudoctl *session* <value>

srv nat pseudoctl *function* <0-3>

Syntax Description

Parameter	Description
<i>session</i> <value>	Set the threshold of the session. <value>: 0 to 2147483647.
<i>function</i> <0-3>	0: It means "Auto". Check the created pseudo port number automatically when the session number is over the threshold. 1: It means "Not". Create a pseudo port number based on subnet setting. No verification. 2: It means "Must". Check the created pseudo port number if it is used by other client. 3: Create a pseudo port number. No verification.

Example

```
> srv nat pseudoctl function 2
pseudo port: get hash pseudo port + subnet.
pseudo port search: check pseudo port (Must).

> srv nat pseudoctl function 3
pseudo port: get hash pseudo port.

> srv nat pseudoctl function 0
pseudo port: get hash pseudo port + subnet.
pseudo port search: check pseudo port (Auto).
```

Telnet Command: **srv nat RSTTimeout**

This command is used for forwarding RST out via TCP after a period of time.

Syntax

srv nat RSTTimeout <value>

Syntax Description

Parameter	Description
<value>	Set the timeout value. <value>: 0 to 10 (one unit is 10msec).

Example

```
> srv nat RSTTimeout 2
Set timeout 2 unit
```

```

> srv nat RSTTimeout ?
%% srv RSTTimeout <value> (unit is 10msec). (0<=value<=10)
-----
now timeout set 2 unit
>

```

Telnet Command: switch -i

This command is used to obtain the TX (transmitted) or RX (received) data for each connected switch.

Syntax

switch -i [*switch idx_no*] [*option*]

Syntax Description

Parameter	Description
<i>switch idx_no</i>	It means the index number of the switch profile.
<i>option</i>	The available commands with parameters are listed below. <i>cmd</i> <i>acc</i> <i>traffic [on/ off/ status/ tx/ rx]</i>
<i>cmd</i>	It means to send command to the client.
<i>acc</i>	It means to set the client authentication account and password.
<i>traffic [on/ off/ status/ tx/ rx]</i>	It means to turn on/off or display the data transmission from the client.

Example

```

> switch -i 1 traffic on
External Device NO. 1 traffic statistic function is enable

```

Telnet Command: switch status

This command is used to check the status for the auto discovery of external devices.

Example

```

> switch status
External Device auto discovery status : Disable

No Respond to External Device : Enable

```

Telnet Command: switch not_respond

This command is used to detect the external device automatically and display on this page.

Syntax

switch not_respond 0

switch not_respond 1

Syntax Description

Parameter	Description
0	Disable the option of "No Respond to External Device packets".
1	Enable the option of "No Respond to External Device packets".

Example

```
> switch not_respond 1
slave not respond!
>
```

Telnet Command: switch on

This command is used to turn on the auto discovery for external devices.

Example

```
> switch on
Enable Extrnal Device auto discovery!
```

Telnet Command: switch off

This command is used to turn off the auto discovery for external devices.

Example

```
> switch off
Disable External Device auto discovery!
```

Telnet Command: switch list

This command is used to display the connection status of the switch.

Example

```
> switch list?
No.      Mac      IP      status  Dur Time  Model_Name
-----
[1]  00-50-7f-cd-07-48  192.168.1.3    On-Line  00:01:01
Vigor2920 Series
```

Telnet Command: switch clear

This command is used to reset the switch table and reboot the router.

switch clear [*idx*]

Syntax Description

Parameter	Description
<i>idx</i>	It means the index number of each item shown on the table. The range is from 1 to 8.
-f	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: switch syslog

This command is used to enable or disable the external device syslog.

Example

```
> switch syslog on
Extern Device status is Enable
> switch syslog off
Extern Device status is Disable
```

Telnet Command: sys admin

This command is used for RD engineer to access into test mode of Vigor router.

Telnet Command: sys adminuser

This command is used to create user account. The server will authenticate the local user who wants to access into the web user interface of Vigor router.

sys adminuser *[option]*

sys adminuser edit *[index] username password*

Syntax Description

Parameter	Description
<i>option</i>	Available options includes: Local [0-1] edit [INDEX] delete [INDEX] view [INDEX]
<i>Local [0-1]</i>	0 - Disable the local user. 1 - Enable the local user.
<i>edit [INDEX] username password</i>	Edit an existed user account or create a new local user account. [INDEX] - 1 -8. There are eight profiles to be added / edited. Username - Type a new name for local user. Password - Type a password for local user.
<i>delete [INDEX]</i>	Delete a local user account.
<i>view [INDEX]</i>	Show the user account/password detail information.

Example

```
> sys adminuser Local 1
Local User has enabled!
> sys adminuser edit 1 carrie test123
Updated!
> sys adminuser view 1

Index:1
User Name:carrie
User Password:test123
```

Telnet Command: sys board

This command is used to disable/enable and configure the panel control.

Syntax

sys board button def *<on/ off>*

sys board button wlan *<on/ off>*

sys board led control *<on/ off>*

sys board led sleepMode *<on/ off>*

sys board led sleepMode time *<minute>*

sys board usb *<p1~p2> <on/ off>*

Syntax Description

Parameter	Description
<i>button def <on/ off></i>	The default reset button will be invalid if turn it off. On - The button is valid. Off - The button is invalid.
<i>Button wlan <on/ off></i>	The wireless button will be invalid if turn it off. On - The button is valid. Off - The button is invalid.
<i>led control <on/ off></i>	All LEDs on the front panel will be invalid if turn it off. On - The LEDs are valid. Off - The LEDs are invalid.
<i>led sleepMode <on/ off></i>	All LEDs on the front panel will be set in sleep mode. On - The sleep mode is on. Off - The sleep mode is off. If the sleep mode is on, push the "wireless button" and the "factory reset button" to turn the LED on (even the buttons are disabled).
<i>led sleepMode time [minutes]</i>	After enableing the sleep mode for all LEDs, they will sleep after the minutes configured here. Minutes: Enter the number of the time.
<i>usb <on/ off></i>	The USB port (p1~p2) will be invalid if turn it off. On - The port is valid. Off - The port is invalid.

Example

```
> sys board led sleepMode on
```

```
LEDs Sleep Mode is on now.
```

```
> sys board led sleepMode time 10  
Sleep Countdown Time set as 10 minute(s).  
Reset the led sleep timer success..
```

Telnet Command: **sys bonjour**

This command is used to disable/enable and configure the Bonjour service.

sys bonjour [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
-e <enable>	It is used to disable/enable bonjour service (0: disable, 1: enable).
-h <enable>	It is used to disable/enable http (web) service (0: disable, 1: enable).
-t <enable>	It is used to disable/enable telnet service (0: disable, 1: enable).
-f <enable>	It is used to disable/enable FTP service (0: disable, 1: enable).
-s <enable>	It is used to disable/enable SSH service (0: disable, 1: enable).
-p <enable>	It is used to disable/enable printer service (0: disable, 1: enable).
-6 <enable>	It is used to disable/enable IPv6 (0: disable, 1: enable).

Example

```
> sys bonjour -s 1  
>
```

Telnet Command: **sys cfg**

This command reset the router with factory default settings. When a user types this command, all the configuration will be reset to default setting.

sys cfg default

sys cfg status

Syntax Description

Parameter	Description
<i>default</i>	It means to reset current settings with default values.
<i>status</i>	It means to display current profile version and status.

Example

```
> sys cfg status
Profile version: 3.0.0      Status: 1 (0x491e5e6c)
> sys cfg default
>
```

Telnet Command: **sys cmdlog**

This command displays the history of the commands that you have typed.

Example

```
> sys cmdlog
% Commands Log: (The lowest index is the newest !!!)
[1] sys cmdlog
[2] sys cmdlog ?
[3] sys ?
[4] sys cfg status
[5] sys cfg ?
```

Telnet Command: **sys ftpd**

This command displays current status of FTP server.

sys ftpd on

sys ftpd off

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on the FTP server of the system.
<i>off</i>	It means to turn off the FTP server of the system.

Example

```
> sys ftpd on
% sys ftpd turn on !!!
```

Telnet Command: **sys domainname**

This command can set and remove the domain name of the system when DHCP mode is selected for WAN.

sys domainname [wan1/ wan2] [Domain Name Suffix]

sys domainname [wan1/ wan2] clear

Syntax Description

Parameter	Description
wan1/ wan2	It means to specify WAN interface for assigning a name for it.
Domain Name Suffix	It means the name for the domain of the system. The maximum number of characters that you can set is 39.
clear	It means to remove the domain name of the system.

Example

```
> sys domainname wan1 clever
> sys domainname wan2 intellegent
> sys domainname ?
% sys domainname <wan1/wan2> <Domain Name Suffix (max. 40 characters)>
% sys domainname <wan1/wan2> clear
% Now: wan1 == clever, wan2 ==intelligent
>
```

Telnet Command: sys iface

This command displays the current interface connection status (UP or Down) with IP address, MAC address and Netmask for the router.

Example

```
> sys iface
Interface 0 Ethernet:
Status: UP
IP Address: 192.168.1.1      Netmask: 0xFFFFFF00 (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.

Syntax

sys passwd *<old password>* *<new password>*

Syntax Description

Parameter	Description
<i>old password</i>	Enter the old password.
<i>new password</i>	Enter a string as the new password for administrator. The maximum character that you can set is 83.

Example

```

> sys passwd admin123
Password change successful !!!

```

```
>
```

Telnet Command: **sys reboot**

This command allows users to restart the router immediately.

Example

```
> sys reboot
>
```

Telnet Command: **sys autoreboot**

This command allows users to restart the router automatically within a certain time.

sys autoreboot [*on/off/hour(s)*]

Syntax Description

Parameter	Description
<i>on/off</i>	On - It means to enable the function of auto-reboot. Off - It means to disable the function of auto-reboot.
<i>hours</i>	It means to set the time schedule for router reboot. For example, if you type "2" in this field, the router will reboot with an interval of two hours.

Example

```
> sys autoreboot on
autoreboot is ON
> sys autoreboot 2
autoreboot is ON
autoreboot time is 2 hour(s)
```

Telnet Command: **sys commit**

This command allows users to save current settings to FLASH. Usually, current settings will be saved in SRAM. Yet, this command will save the file to FLASH.

Example

```
> sys commit
>
```

Telnet Command: **sys tftpd**

This command can turn on TFTP server for upgrading the firmware.

Example

```
> sys tftpd
% TFTP server enabled !!!
```

Telnet Command: **sys cc**

This command can display current country code and wireless region of this device.

Example

```
> sys cc
Country Code      : 0x 0 [International]
Wireless Region Code: 0x30
>
```

Telnet Command: sys version

This command can display current version for the system.

Example

```
> sys version
Router Model: Vigor2765Vac   Version: 4.3.1_STD English
Profile version: 4.0.0      Status: 1 (0x9df515cf)
Router IP: 192.168.1.1      Netmask: 255.255.255.0
Firmware Build Date/Time: Apr 26 2021 10:19:42
Router Name: DrayTek
Revision: 6988_1790_7d830fb99 master
Current VDSL2 Firmware Version: 08-0B-00-0F-00-07
ADSL Firmware Version: 08-0B-00-07-00-01 Annex A
VDSL2 Firmware Version: 08-0B-00-0F-00-07
Router serial no: None
```

Telnet Command: sys qrybuf

This command can display the system memory status and leakage list.

Example

```
> sys qrybuf
System Memory Status and Leakage List

Buf sk_buff ( 200B), used#: 1647, cached#: 30
Buf KMC4088 (4088B), used#: 0, cached#: 8
Buf KMC2552 (2552B), used#: 1641, cached#: 42
Buf KMC1016 (1016B), used#: 7, cached#: 1
Buf KMC504 ( 504B), used#: 8, cached#: 8
Buf KMC248 ( 248B), used#: 26, cached#: 22
Buf KMC120 ( 120B), used#: 67, cached#: 61
Buf KMC56 ( 56B), used#: 20, cached#: 44
Buf KMC24 ( 24B), used#: 58, cached#: 70
Dynamic memory: 13107200B; 4573168B used; 190480B/0B in level 1/2
cache.

FLOWTRACK Memory Status
# of free = 12000
# of maximum = 0
# of flowstate = 12000
# of lost by siganture = 0
# of lost by list = 0
```


Telnet Command: **sys pollbuf**

This command can turn on or turn off polling buffer for the router.

sys pollbuf *[on]*

sys pollbuf *[off]*

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on pulling buffer.
<i>off</i>	It means to turn off pulling buffer.

Example

```
> sys pollbuf on
% Buffer polling is on!

> sys pollbuf off
% Buffer polling is off!
```

Telnet Command: **sys britask**

This command can improve triple play quality.

sys britask *[on]*

sys britask *[off]*

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on the bridge task for improving the triple play quality.
<i>off</i>	It means to turn off the bridge task.

Example

```
> sys britask on
% bridge task is ON, now
```

Telnet Command: **sys tr069**

This command can set CPE settings for applying in VigorACS.

sys tr069 get *<parm>* *<option>*

sys tr069 set *<parm>* *<value>*

sys tr069 getnoti *<parm>*

sys tr069 setnoti *<parm>* *<value>*

sys tr069 log

sys tr069 debug *<on/ off>*

sys tr069 save

sys tr069 inform *<event code>*

sys tr069 port *<port num>*

sys tr069 cert_auth*<on/ off>*

sys tr069 only_standard_parm <on/ off>

sys tr069 notify -S

sys tr069 notify -n <on/ off>

sys tr069 notify -l <on/ off>

sys tr069 notify -c <on/ off>

sys tr069 notify -b <on/ off>

sys tr069 notify -B "<WAN number> <Medium threthold> <High threthold> <TX Speed>Mb <RX Speed>Mb"

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.
<i>only_standard_parm</i> <on/ off>	It means to turn on or off to exclude all the Vendor-Specific ("X_") parameters, and only send out standard parameters.
<i>notify -n</i> <on/ off>	It means to set CPE notification settings. It means to / not to record the CPE notify log on the Syslog. on: Record on the Syslog. off: Not record on the Syslog.
<i>notify -l</i> <on/ off>	It means to / not to record the web login log on the Syslog. on: Record on the Syslog. off: Not record on the Syslog.
<i>notify -c</i> <on/ off>	It means to / not to record the web changed log on the Syslog. on: Record on the Syslog. off: Not record on the Syslog.

<i>notify -h <on/off></i>	It means to / not to record the high availability log on the Syslog. on: Record on the Syslog. off: Not record on the Syslog.
<i>notify -b [on/off]</i>	It means to / not to record the bandwidth utilization log on the Syslog. on: Record on the Syslog. off: Not record on the Syslog.
<i>notify -B "<WAN number> <Medium threthold> <High threthold> <TX Speed>Mb <RX Speed>Mb"</i>	It means to set bandwidth utilization setting. <WAN number>: Enter the index number of WAN interface(s). <Medium threthold>: Enter a value. <High threthold>: Enter a value. <TX Speed>Mb: Enter a value. <RX Speed>Mb: Enter a value.
<i>-S</i>	Show the CPE notification settings.

Example

```
> sys tr069 get InternetGatewayDevice.ManagementServer.
Total number of parameter is 54
Total content length of parameter is 3517

InternetGatewayDevice.ManagementServer.URL=
InternetGatewayDevice.ManagementServer.Username=
InternetGatewayDevice.ManagementServer.Password=
InternetGatewayDevice.ManagementServer.PeriodicInformEnable= 0
InternetGatewayDevice.ManagementServer.PeriodicInformInterval=
900
InternetGatewayDevice.ManagementServer.PeriodicInformTime=
1970-01-01T00:00:00
InternetGatewayDevice.ManagementServer.ParameterKey=
InternetGatewayDevice.ManagementServer.ConnectionRequestURL=
InternetGatewayDevice.ManagementServer.ConnectionRequestUsername=
vigor
InternetGatewayDevice.ManagementServer.ConnectionRequestPassword=
InternetGatewayDevice.ManagementServer.UpdatesManaged= 0
InternetGatewayDevice.ManagementServer.UDPConnectionRequestAddres
s=
InternetGatewayDevice.ManagementServer.UDPConnectionRequestAddres
sNotification-L
imit= 0
InternetGatewayDevice.ManagementServer.STUNEnable= 0
InternetGatewayDevice.ManagementServer.STUNServerAddress=
InternetGatewayDevice.ManagementServer.STUNServerPort= 3478
InternetGatewayDevice.ManagementServer.STUNUsername=
InternetGatewayDevice.ManagementServer.STUNPassword=
InternetGatewayDevice.ManagementServer.STUNMaximumKeepAlivePeriod
= -1
InternetGatewayDevice.ManagementServer.STUNMinimumKeepAlivePeriod
= 60
InternetGatewayDevice.ManagementServer.NATDetected= 0
InternetGatewayDevice.ManagementServer.ManageableDeviceNumberOfEn
tries= 0--- 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 <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 <0/ 1>	0: Disable the function of SIP ALG. 1: Enable the function of SIP ALG.
-p <parameter>	It means to set the listening port for SIP ALG. <parameter> : Ranges from 1 to 65535.
-u	It means to enable or disable the listen along UDP path setting. 0: Disable 1: Enable
-t	It means to enable or disable the listen along TCP path setting. 0: Disable 1: Enable

Example

```
> sys sip_alg -e 1
Enable SIP ALG
> sys sip_alg -p 65535
Current listening port: 65535
> sys sip_alg ?
Usage: sys sip_alg <command> <parameter>
-e: enable SIP ALG (0:disable, 1:enable)
-p: set your listening port for SIP ALG
-u: enable listen along UDP path (0:disable, 1:enable)
-t: enable listen along TCP path (0:disable, 1:enable)

Current SIP ALG status
-ALG Master Switch: Enabled
-SIP ALG: Enabled
-Listen along UDP path: Yes
-Listen along TCP path: Yes
-Listening Port: 65535
-Max sipalg session num: 256
-Remain sipalg session num: 256
```

Telnet Command: **sys rtsp_alg**

This command can turn on/off RTSP ALG (Application Layer Gateway) for traversal.

Syntax

sys rtsp_alg [<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 <0/ 1>	0: Disable the function of RTSP ALG. 1: Enable the function of RTSP ALG.
-p <parameter>	It means to set the listening port for RTSP ALG. <parameter> : Ranges from 1 to 65535.
-u	It means to enable or disable the listen along UDP path setting. 0: Disable 1: Enable
-t	It means to enable or disable the listen along TCP path setting. 0: Disable 1: Enable
-v	It displays RTP and RTCP portmap information of RTSP ALG.

Example

```
> sys rtsp_alg -e 1
Enable RTSP ALG

> sys rtsp_alg -p 60000
Current listening RTSP Port: 60000

> sys rtsp_alg -v
Current Open PortMap Number of RTSP ALG: 0

> sys rtsp_alg ?
Usage: sys rtsp_alg <command> <parameter>
-e: enable RTSP ALG (0:disable, 1:enable)
-p: set your listening port for RTSP ALG
-u: enable listen along UDP path (0:disable, 1:enable)
-t: enable listen along TCP path (0:disable, 1:enable)
-v: show rtp and rtcp portmap information of RTSP ALG

Current RTSP ALG status
-ALG Master Switch: Enabled
-RTSP ALG: Enabled
-Listen along UDP path: Yes
-Listen along TCP path: Yes
-Listening Port: 60000
-Max RTSP session num: 256
-Remain RTSP session num: 256
>
```

Telnet Command: sys license

This command can process the system license.

Syntax

sys license *reset_regser*

sys license *licera*

sys license *licifno* <AUTO/ WAN#>
sys license *licalias* <index>
sys license *lic_trigger*
sys license *licelog*

Syntax Description

Parameter	Description
<i>reset_regser</i>	It means the license register server setting or register service in portal.
<i>licera</i>	It means to erase license setting.
<i>licifno</i> <AUTO/ WAN#>	It means license and signature download interface setting.
<i>licalias</i> <index>	It means to specify an IP alias by entering the index number of the IP alias profile.
<i>lic_trigger</i>	It means to trigger the license.
<i>licelog</i>	It means to show the authentication log.
<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 wan3
Download interface is set as "WAN3" now.

```

Telnet Command: sys diag_log

This command is used for RD debug.

sys diag_log [*status*| *enable*| *disable*| *flush*| *lineno* [*w*] | *level* [*x*] | *feature* [*on*|*off*][*y*]| *log*]

Syntax Description

Parameter	Description
<i>status</i>	It means to show the status of diagnostic log.
<i>enable</i>	It means to enable the function of diag_log.
<i>disable</i>	It means to disable the function of diag_log.
<i>flush</i>	It means the flush log buffer.
<i>lineno</i> [<i>w</i>]	It means the total lines for displaying message. w - Available value ranges from 100 to 50000.
<i>level</i> [<i>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</i> [<i>on</i> / <i>off</i>][<i>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</i> [<i>on</i> / <i>off</i>][<i>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 DRVAPI, DRVMMC, DRVMP, 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: sys arp_AutoReq

This command is used to enable / disable the function that Vigor router sends ARP request to the connected device(s) periodically.

Syntax

sys arp_AutoReq -d <value>

Syntax Description

Parameter	Description
-d [value]	Disable the function of ARP auto request. 0 - Enable 1 - Disable

Example

```
> sys arp_AutoReq -d 1
Arp auto-request disable.
>
```

Telnet Command: sys daylightsave

This command is used to configure daylight save setting.

Syntax

sys daylightsave [*-<command> <parameter> | ...*]

Syntax Description

Parameter	Description
[<command><parameter> ...]	The available commands with parameters are listed below. [..] means that you can type in several commands in one line.
-v	Display the daylight saving settings.
-r	Set to factory default setting.
-e [1/0]	Enable (1) / disable (0) daylight saving.
-t [0/1/2]	Specify the saving type for daylight setting. 0 - Default 1 - Time range 2 - Yearly
-s <year> <month> <day> <hour>	Set the detailed settings of the starting day for time range type. year - must be the year after 2013. month - 1 ~ 12 day - 1 ~ 31 hour - 0 ~ 23 e.g., sys daylightsave -s 2014 3 10 12
-d <year> <month> <day> <hour>	Set the detailed settings of the ending day for time range type. year - After 2013. month - 1 ~ 12 day - 1 ~ 31 hour - 0 ~ 23 e.g., sys daylightsave -d 2014 9 10 12
-y <month> <th weekday> <day in week> <hour>	Set the detailed settings of the starting day for yearly type. month - 1 ~ 12 th weekday - 1 ~ 5, 9: last week day in week - 0:Sun, 1:Mon, 2:Tue, 3:Wed, 4:Thu, 5: Fri, 6:Sat hour - 0 ~ 23 e.g., sys daylightsave -y 9 1 0 14
-z <month> <th weekday> <day in week> <hour>	Set the detailed settings of the ending day for yearly type. month - 1 ~ 12 th weekday - 1 ~ 5, 9: last week day in week - 0:Sun, 1:Mon, 2:Tue, 3:Wed, 4:Thu, 5: Fri, 6:Sat hour - 0 ~ 23 e.g., sys daylightsave -z 3 1 6 14

Example

```
> sys daylightsave -y 9 1 0 14
% Start: Yearly on Sep 1th Sun 14:00
```

Telnet Command: sys dnsCacheTbl

This command is used to configure TTL settings which will be displayed in DNS Cache table.

Syntax

sys dnsCacheTbl [*<command><parameter>| ...*]

Syntax Description

Parameter	Description
[<i><command><parameter> ...</i>]]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-l	Display DNS IPv4 entry in the DNS cache table.
-s	Display DNS IPv6 entry in the DNS cache table.
-v	Display the TTL limit value in the DNS cache table.
-t <0/n >	Set the TTL limit value in the DNS cache table. 0- No limit N - Greater than or equal to 5.
-c	Clear the DNS cache table.

Example

```
> sys dnsCacheTbl -l
%DNS Cache Table List
> sys dnsCacheTbl -t 65
% Set TTL limit: 65 seconds.
% When TTL larger than 65s , delete the DNS entry in the router's DNS cache
table.
>
```

Telnet Command: sys syslog

This command is used to configure

Syntax

sys syslog -a *<enable>* [*<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.
-a <1/0>	Enable (1) or disable (0) Syslog Access Setup.
-s <1/0>	Enable (1) or disable (0) Syslog Save to Syslog Server.
-i <IP address>	Define the IP address of the Syslog server.
-d <port number>	Define the port number (1 ~ 65535) as the destination port.
-u <1/0>	Enable (1) or disable (0) Syslog Save to USB Disk.
-m <1/0>	Enable (1) or disable (0) Mail Syslog.
-f <1/0>	Enable (1) or disable (0) Firewall Log.
-v <1/0>	Enable (1) or disable (0) VPN Log.
-e <1/0>	Enable (1) or disable (0) User Access Log.
-c <1/0>	Enable (1) or disable (0) Call Log.
-w <1/0>	Enable (1) or disable (0) WAN Log.

-r <1/ 0>	Enable (1) or disable (0) Router/DSL Information.
-t <1/ 0>	Enable (1) or disable (0) AlertLog Setup.
-o <port number>	Define the port number (1 ~ 65535) for AlertLog.
-p	Update the server IP address.
-W <1/ 0>	Set the mode for writing Syslog. 0: overwrite oldest logs; 1: stop logging.
-U <1/ 0>	Set the unit for the Syslog saved to a USB disk. 0:GB; 1:MB
-S <capacity>	Set the folder capacity for the syslog saved in the USB disk. 1 ~16(GB); 1 ~1024(MB)

Example

```
> sys syslog -a 1 -s 1 -i 192.168.1.25 -d 514
>
```

Telnet Command: sys mailalert

This command is used to configure settings for syslog mail alert.

Syntax

sys mailalert [-<command> <parameter>]

Syntax Description

Parameter	Description
[<command><parameter>]	The available commands with parameters are listed below.
-e <0/ 1>	Enable/disable Mail Alert. 0 - Disable. 1 - Enable.
-w <0/ 1/ 2/ ...>	Set Interface (Physical) Any/WAN1/WAN2/WAN... and etc.
-x <WAN IP Alias index>	Set WAN IP Alias. Index 1 is reserved and must set an interface first.
-i <SMTP Server IP>	Set IP Address for SMTP server.
-o <SMTP Server Port>	Set port number for SMTP server..
-a <Mail Address>	Set E-mail address for alert mail reciver.
-r <Mail Address>	Set E-mail Address for mail return.
-s <0/ 1>	Enable/disable the function of Use SSL. 0 - Disable. 1 - Enable.
-h <0/ 1>	Enable/disable SMTP Authentication. 0 - Disable. 1 - Enable.
-u <Username>	Set username for SMTP Authentication.
-p <Password>	Set password for SMTP Authentication.
-l <type><0/ 1>	Enable / disable mail alert for different types. Number 0 ~ 6 represent different types. "0 <0/1>" : Enable/Disable Mail Alert of the DoS Attack. "1 <0/1>" : Enable/Disable Mail Alert of the APPE. "2 <0/1>" : nable/Disable Mail Alert of the VPN Log. "3 <0/1>" : Enable/Disable Mail Alert of the APPE Signature. "6 <0/1>" : Enable/Disable Mail Alert of the Reboot Debug Log. In which, 0 - Disable. 1 - Enable.

-f	Reset Mail Alert setting to factory default.
-v	Show current Mail Alert setting.
-R <0/ 1>	Set Mail Alert Reboot debug log mode. 0: Limited Mode 1: Unlimited Mode.

Example

```
> sys mailalert -e 1
Set Enable Mail Alert.
> sys mailalert -v
----- Current setting for Mail Alert -----
Mail Alert: Enable
SMTP Server IP Address: 0.0.0.0
SMTP Server Port: 25
Alert Mail Reciver E-maill Address:
Mail Return E-mail Address:
Use SSL: Disable
SMTP Authentication: Disable
Username for SMTP Authentication:
Password for SMTP Authentication:
Mail Alert for DoS Attack: Enable.
Mail Alert for APPE: Enable.
Mail Alert for VPN Log: Enable.
Mail Alert for APPE Signature: Disable.
Mail Alert for Reboot Debug Log: Disable, Mode: Limited.
-----
```

Telnet Command: sys time

This command is used to configure system time and date.

Syntax

sys time server [*domain*]

sys time inquire

sys time show

sys time zone [*index*]

Syntax Description

Parameter	Description
<i>domain</i>	Type the domain name of the time server. The maximum length is 39 characters.
<i>index</i>	Different number means different time zone. 1 - GMT-12:00 Eniwetok, Kwajalein 2 - GMT-11:00 Midway Island, Samoa 3 - GMT-10:00 Hawaii 4 - GMT-09:00 Alaska 5 - GMT-08:00 Pacific Time (US & Canada) 6 - GMT-08:00 Tijuana 7 - GMT-07:00 Mountain Time (US & Canada) 8 - GMT-07:00 Arizona 9 - GMT-06:00 Central Time (US & Canada) 10 - GMT-06:00 Saskatchewan 11 - GMT-06:00 Mexico City, Tegucigalpa 12 - GMT-05:00 Eastern Time (US & Canada) 13 - GMT-05:00 Indiana (East)

14 - GMT-05:00	Bogota, Lima, Quito
15 - GMT-04:00	Atlantic Time (Canada)
16 - GMT-04:00	Caracas, La Paz
17 - GMT-04:00	Santiago
18 - GMT-03:30	Newfoundland
19 - GMT-03:00	Brasilia
20 - GMT-03:00	Buenos Aires, Georgetown
21 - GMT-02:00	Mid-Atlantic
22 - GMT-01:00	Azores, Cape Verde Is.
23 - GMT	Greenwich Mean Time : Dublin
24 - GMT	Edinburgh, Lisbon, London
25 - GMT	Casablanca, Monrovia
26 - GMT+01:00	Belgrade, Bratislava
27 - GMT+01:00	Budapest, Ljubljana, Prague
28 - GMT+01:00	Sarajevo, Skopje, Sofija
29 - GMT+01:00	Warsaw, Zagreb
30 - GMT+01:00	Brussels, Copenhagen
31 - GMT+01:00	Madrid, Paris, Vilnius
32 - GMT+01:00	Amsterdam, Berlin, Bern
33 - GMT+01:00	Rome, Stockholm, Vienna
34 - GMT+02:00	Bucharest
35 - GMT+02:00	Cairo
36 - GMT+02:00	Helsinki, Riga, Tallinn
37 - GMT+02:00	Athens, Istanbul, Minsk
38 - GMT+02:00	Jerusalem
39 - GMT+02:00	Harare, Pretoria
40 - GMT+03:00	Volgograd
41 - GMT+03:00	Baghdad, Kuwait, Riyadh
42 - GMT+03:00	Nairobi
43 - GMT+03:00	Moscow, St. Petersburg
44 - GMT+03:30	Tehran
45 - GMT+04:00	Abu Dhabi, Muscat
46 - GMT+04:00	Baku, Tbilisi
47 - GMT+04:30	Kabul
48 - GMT+05:00	Ekaterinburg
49 - GMT+05:00	Islamabad, Karachi, Tashkent
50 - GMT+05:30	Bombay, Calcutta
51 - GMT+05:30	Madras, New Delhi
52 - GMT+06:00	Astana, Almaty, Dhaka
53 - GMT+06:00	Colombo
54 - GMT+07:00	Bangkok, Hanoi, Jakarta
55 - GMT+08:00	Beijing, Chongqing
56 - GMT+08:00	Hong Kong, Urumqi
57 - GMT+08:00	Singapore
58 - GMT+08:00	Taipei
59 - GMT+08:00	Perth
60 - GMT+09:00	Seoul
61 - GMT+09:00	Osaka, Sapporo, Tokyo
62 - GMT+09:00	Yakutsk
63 - GMT+09:30	Darwin
64 - GMT+09:30	Adelaide
65 - GMT+10:00	Canberra, Melbourne, Sydney
66 - GMT+10:00	Brisbane
67 - GMT+10:00	Hobart
68 - GMT+10:00	Vladivostok
69 - GMT+10:00	Guam, Port Moresby
70 - GMT+11:00	Magadan, Solomon Is.
71 - GMT+11:00	New Caledonia
72 - GMT+12:00	Fiji, Kamchatka, Marshall Is.
73 - GMT+12:00	Auckland, Wellington

Example

```
> sys time zone 8
Set Time Zone OK
```

```

> sys time show
***** System Time *****
Current System Time: [2000 Jan 01 Sat 02:09:29]
Time Server: [pool.ntp.org]
Time Zone Index: [8]. GMT-07:00
*****

```

Telnet Command: sys dashboard

This command is used to display / hide items (such as System Information, Interface...) on dashboard.

Syntax

sys dashboard [-<command> <value> | ...]

sys dashboard show

Syntax Description

Parameter	Description
[<command> <value> ...]	The available commands with parameters are listed below. [...] means that you can type in several parameters in one line. <command> “0 ~ 9” and “a” represent different sections to be displayed on the dashboard. 0 : Front Panel 1 : System Information 2 : IPv4 LAN Information 3 : IPv4 Internet Access 4 : IPv6 Internet Access 5 : Interface 6 : Security 7 : System Resource 8 : LTE Status 9 : Quick Access - a : VoIP <value> 1 : Enable 0 : Disable
show	Display current status (enabled /disabled) for each item.

Example

```

> sys dashboard -0 1
Front Panel enabled
> sys dashboard show
Front Panel enabled
System Information enabled
IPv4 LAN Information enabled
IPv4 Internet Access enabled
IPv6 Internet Access enabled
Interface enabled
Security enabled
System Resource enabled
LTE Status enabled
Quick Access enabled
VoIP enabled

```

Telnet Command: testmail

This command is used to display current settings for sending test mail.

Example

```
> testmail
Send out test mail
Mail Alert:[Disable]
Interface :Any
WAN_Alias index:[0]
SMTP_Server:[0.0.0.0]
SMTP_Port:[25]
Mail to:[]
Return-Path:[]
Connection Security:[Plaintext]
```

Telnet Command: upnp off

This command can close UPnP function.

Example

```
>upnp off
UPNP say bye-bye
```

Telnet Command: upnp on

This command can enable UPnP function.

Example

```
>upnp on
UPNP start.
```

Telnet Command: upnp nat

This command can display IGD NAT status.

Example

```
> upnp nat ?
***** IGD NAT Status *****

((0))
InternalClient >>192.168.1.10<<, RemoteHost >>0.0.0.0<<
InternalPort >>21<<, ExternalPort >>21<<
PortMapProtocol >>TCP<<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
Ftp Example [MICROSOFT]
((1))
InternalClient >>0.0.0.0<<, RemoteHost >>0.0.0.0<<
InternalPort >>0<<, ExternalPort >>0<<
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
```

```

PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
0<<

--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---

```

Telnet Command: upnp service

This command can display the information of the UPnP service. UPnP service must be enabled first.

Example

```

> upnp on
UPNP start.

> upnp service
>>>>> SERVICE TABLE1 <<<<<
    serviceType urn:schemas-microsoft-com:service:OSInfo:1
    serviceId   urn:microsoft-com:serviceId:OSInfo1
    SCPDURL     /upnp/OSInfo.xml
    controlURL  /OSInfo1
    eventURL    /OSInfoEvent1
    UDN         uuid:774e9bbe-7386-4128-b627-001daa843464

>>>>> SERVICE TABLE2 <<<<<
    serviceType
urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1
    serviceId   urn:upnp-org:serviceId:WANCommonIFC1
    SCPDURL     /upnp/WComIFCX.xml
    controlURL  /upnp?control=WANCommonIFC1
    eventURL    /upnp?event=WANCommonIFC1
    UDN         uuid:2608d902-03e2-46a5-9968-4a54ca499148
.
.
.

```

Telnet Command: upnp subscribe

This command can show all UPnP services subscribed.

Example

```

> upnp on
UPNP start.
> upnp subscribe
Vigor> upnp subscribe
>>>> (1) serviceType urn:schemas-microsoft-com:service:OSInfo:1

----- Subscribtion1 -----

    sid = 7a2bbdd0-0047-4fc8-b870-4597b34da7fb

    eventKey =1, ToSendEventKey = 1

```

```

        expireTime =6926

        active =1

        DeliveryURLs
=<http://192.168.1.113:2869/upnp/eventing/twtnpnsiun>

>>>> (2) serviceType
urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1

----- Subscribtion1 -----

        sid = d9cd47a5-d9c9-4d3d-8043-d03a82f27983

        eventKey =1, ToSendEventKey = 1
.
.
.

```

Telnet Command: upnp tmpvs

This command can display current status of temp Virtual Server of your router.

Example

```

Vigor> upnp tmpvs
***** Temp virtual server status *****

((0))
real_addr >>192.168.1.10<<, pseudo_addr >>172.16.3.229<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>TCP<<
time >>0<<

((1))
real_addr >>0.0.0.0<<, pseudo_addr >>0.0.0.0<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>0<<
time >>0<<
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---

```

Telnet Command: upnp wan

This command is used to specify WAN interface to apply UPnP.

upnp wan [*n*]

Syntax Description

Parameter	Description
<i>n</i>	It means to specify WAN interface to apply UPnP.

	n=0, it means to auto-select WAN interface. n=1, WAN1 n=2, WAN2

Example

```
> upnp wan 1
use wan1 now.
```

Telnet Command: usb list

This command is use to display the information about the brand name and model name of the USB modems which are supported by Vigor router.

Example

```
> usb list ?
Brand      Module      Standard
-----
Aiko       Aiko 83D      3.5G      Y
BandRich   Bandlux C170  3.5G      Y
BandRich   Bandlux C270  3.5G      Y
BandRich   Bandlux C321  3.5G      Y
BandRich   Bandlux C330  3.5G      Y
BandRich   Bandlux C331  3.5G      Y
BandRich   Bandlux C502  3.5G      Y
Huawei      Huawei E169u  3.5G      Y
Huawei      Huawei E220   3.5G      Y
Huawei      Huawei E303D  3.5G      Y
Huawei      Huawei E392   3.5G      Y
Huawei      Huawei E398   3.5G      Y
Sony 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: usb user

This command is used to set profiles for FTP/SMB users.

Syntax Description

usb user add [Index] [Username] [Password] [Permission] [Home path]

usb user rm [Index]

usb user enable [Index]

usb user disable [Index]

usb user list

Syntax Description

Parameter	Description
<i>add</i> <Index> <Username> <Password> <Permission> <Home path>	Add a new user profile. <Index>: It means the index number of the user profile. There are 16 profiles allowed to be configured. So the range of such option is 1 ~ 16. <Username>: Enter a text (maximum 131 characters) as the username for the user profile. <Password>: Enter a text (maximum 131 characters) as the password for the user profile. <Permission>: Specify the action (RWDLCR) permitted. If one of the actions is not allowed, simple type “-” instead. R - Read File. W - Write File. D - Delete File. L - List directory. C - Create directory. R - Remove selected directory. <Home path>: Set the path (maximum 159 characters) for the USB user profile.
<i>rm</i> <Index>	Delete an existed user profile. <Index>: It means the index number of the user profile.
<i>enable</i> <Index>	Enable a user profile. <Index>: It means the index number of the user profile.
<i>disable</i> <Index>	Disable a user profile. <Index>: It means the index number of the user profile.
<i>list</i>	Display all of the user profile.

Example

```
> usb user add 1 root 1234 R-DLCR /usr  
> No usb storage is available!!
```

Telnet Command: usb temp

This command is to configure USB temperature.

Syntax Description

usb temp set <-c| -f| -a| -b| -m| -u| -l| -r>

usb temp show

usb temp all_data

Syntax Description

Parameter	Description
<i>set -c</i>	Set the temperature unit (Celsius).
<i>set -f</i>	Set the temperature unit (Fahrenheit).
<i>set -a</i>	Set the temperature sensor by using a probe or the built-in sensor automatically. The probe will be detected and used first, and fall back to the built-in sensor if the probe is not detected.
<i>set -b</i>	Set to use the built-in sensor.

<i>set -m</i>	Enable or disable the Alarm Setting. 1: Enable 0: Disable
<i>set -u <value></i>	Set the upper temperature limit. <value>: Enter a value, e.g., 30.35.
<i>set -l <value></i>	Set the lower temperature limit. <value>: Enter a value, e.g., 10.35.
<i>set -r</i>	Shows the setting of temperature unit and sensor type.
<i>show</i>	Displays current temperature.
<i>all_data</i>	Displays all temperature data.

Example

```
> usb temp set -r
Show setting:temp set -r

Alarm Settings: 1 (0:Disable, 1: Enable.)
upper temperature limit: 30.0 C
lower temperature limit: 18.0 C
unit: 0 (0:Celsius, 1: Fahrenheit.)
sensor: 1 (0:Auto select, 1: built-in.)
```

Telnet Command: **vigbrg set**

This command is to configure specified WAN as bridge mode.

Syntax Description

vigbrg set -v [*IP version*] -w [*WAN_idx*] -l [*LAN_idx*] -e [0/ 1] -f [0/ 1]

Syntax Description

Parameter	Description
-v [<i>IP version</i>]	Indicate the IP version for the IP address. 4 - IPv4. 6 - IPv6.
-w [<i>WAN_idx</i>]	WAN_idx - Indicate the WAN interface. 1 - WAN1 2 - WAN2 3 - WAN3 4 - WAN4
-l [<i>LAN_idx</i>]	LAN_idx - Indicate the LAN interface. 1 - LAN1 2 - LAN2 3 - LAN3 4 - LAN4
e [0/ 1]	Enable (1) or disable (0) the Vigor Bridge for WAN or/and LAN.
f [0/ 1]	Enable (1) or disable (0) the firewall functions.

Example

```
> vigbrg set -v 4 -w 1 -l 1 -e 1
```

```
[WAN1] IPv4 bridge is enable. Set subnet[LAN1]
```

Telnet Command: vigbrg closeall

This command can disable vigor bridge function.

Example

```
> vigbrg closeall  
Close all bridge and bridge firewall
```

Telnet Command: vigbrg status

This command can show whether the Vigor Bridge Function is enabled or disabled.

Example

```
> vigbrg status  
%Vigor Bridge Function is enable!  
  
%Wan1 management is disable!
```

Telnet Command: **vigbrg cfgip**

This command allows users to transfer a bridge modem into ADSL router by accessing into and adjusting specified IP address. Users can access into Web UI of the router to manage the router through the IP address configured here.

vigbrg cfgip [*IP Address*]

Syntax Description

Parameter	Description
<i>IP Address</i>	It means to type an IP address for users to manage the router.

Example

```
> vigbrg cfgip 192.168.1.15
> vigbrg cfgip ?
% Vigor Bridge Config IP,
% Now: 192.168.1.15
```

Telnet Command: **vigbrg wanstatus**

This command can display the existed WAN connection status for the modem (change from ADSL router into bridge modem), including index number, MAC address, Stamp Time, PVC, VLAN port for Vigor Bridge Function.

Example

```
> vigbrg wanstatus
Vigor Bridge: Running
WAN mac table:
Index  MAC Address          Stamp Time      PVC      VLan
      Port
```

Telnet Command: **vigbrg wlanstatus**

This command can display the existed WLAN connection status for the modem (change from router into bridge modem), including index number, MAC address, Stamp Time, PVC, VLAN port for Vigor Bridge Function.

Example

```
> vigbrg wlanstatus
Vigor Bridge: Running
WAN mac table:
Index  MAC Address          Stamp Time      PVC      VLan      Port
```

Telnet Command: **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

<code>-l [WAN index]</code>	WAN index: Ranges from 1 to 10. 1: WAN1, 2: WAN2, ...etc., In which, WAN3 and WAN 4 are USB WAN.
<code>-n [Subnet index]</code>	Subnet index: Ranges from 1 to 8. 1: Subnet 1, 2: Subnet 2, ...etc.
<code>-b [Bridge mode]</code>	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: vlan group

This command allows you to set VLAN group. You can set four VLAN groups. Please run `vlan restart` command after you change any settings.

Syntax

vlan group *id* [*set/ set_ex*] [*p1/ p2/ p3/ p4/ s1/ s2/ s3/ s4*]

Syntax Description

Parameter	Description
<i>id</i>	It means the group 0 to 7 for VLAN.
<i>set</i>	It indicates each port can join more than one VLAN group.
<i>set_ex</i>	It indicates each port can join one VLAN group at one time.
<i>p1/ p2/ p3/ p4</i>	It indicates LAN port 1 to LAN port 4. To group LAN1, LAN2, LAN3 and/or LAN4 under one VLAN group, please type the port number(s) you want.
<i>s1/ s2/ s3/ s4</i>	It is only available for WALN models.

Example

```
> vlan group 3 set p1 s3 s4
VLAN   p1   p2   p3   p4   s1   s2   s3   s4
-----
   3    V                               V    V
>
```

Telnet Command: vlan off

This command allows you to disable VLAN function.

Syntax

vlan off

Example

```
> vlan off

VLAN is Disable!

Force subnet LAN2/3/4 to be disabled!!
```

Telnet Command: vlan on

This command allows you to enable VLAN function.

Syntax

vlan on

Example

```
> vlan on

VLAN is Enable!
```

Telnet Command: vlan pri

This command is used to define the priority for each VLAN profile setting.

Syntax

vlan pri *n pri_no*

Syntax Description

Parameter	Description
<i>n</i>	It means VLAN ID number. n=VLAN ID number (from 0 to 7).
<i>pri_no</i>	It means the priority of VLAN profile. pri_no=0 ~7 (from none to highest priority).

Example

```
> vlan pri 1 2

VLAN1: Priority=2
```

Telnet Command: vlan restart

This command can make VLAN settings restarted with newest configuration.

Syntax

vlan restart

Example

```
> vlan restart ?
VLAN restarts!!!
```

Telnet Command: vlan status

This command display current status for VLAN.

Syntax

vlan status

Example

```
> vlan status
VLAN is Enable :
-----
VLAN Enable VID Pri p1 p2 p3 p4 s1 s2 s3 s4 subnet
-----
0 OFF 0 0 1:LAN1
1 OFF 0 2 1:LAN1
2 OFF 0 0 1:LAN1
3 OFF 0 0 V V 1:LAN1
4 OFF 0 0 1:LAN1
5 OFF 0 0 1:LAN1
6 OFF 0 0 1:LAN1
7 OFF 0 0 1:LAN1
-----
Note: they are only untag for s1/s2/s3/s4, but they can join tag vlan
with lan ports.
Permit untagged device in P1 to access router: ON.
```

Telnet Command: vlan subnet

This command is used to configure the LAN interface used by the VLAN group.

Syntax

vlan subnet group_id [1/2/3/4]

Syntax Description

Parameter	Description
[1/2/3/4]	It means interfaces, LAN1 ~ LAN4.

Example

```
> vlan subnet group_id 2
% Vlan Group-0 using LAN2      !
```


This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.

Telnet Command: vlan submode

This command changes the VLAN encapsulation mechanisms in the LAN driver.

Syntax

vlan submode [*on*/*off*] *status*

Syntax Description

Parameter	Description
<i>on</i>	It means to enable the promiscuous mode.
<i>off</i>	It means to enable the normal mode.
<i>status</i>	It means to display if submode is normal mode or promiscuous mode.

Example

```
> vlan submode status
% vlan subnet mode : normal mode
> vlan submode on
% vlan subnet mode modified to promiscuous mode.
> vlan submode status
% vlan subnet mode : promiscuous mode
```

Telnet Command: vlan tagged

This command is used to enable or disable the incoming of untagged packets.

Syntax

vlan tagged [*n*] [*on*/*off*]

vlan tagged [*unlimited*] [*on*/*off*]

vlan tagged [*p1_untag*] [*on*/*off*]

Syntax Description

Parameter	Description
<i>n</i>	It means VLAN channel. The range is from 0 to 7.
<i>on/off</i>	It means to enable/disable the tagged VLAN.
[<i>unlimited</i>] [<i>on/off</i>]	unlimited on: It allows the incoming of untagged packets even all VLAN are tagged. unlimited off: It does not allow the incoming of untagged packets.
[<i>p1_untag</i>] [<i>on/off</i>]	P1_untag on: It allows the incoming of untagged packets from LAN port 1. P1_untag off: It does not allow the incoming of untagged packets from LAN port 1.

Example

```
> vlan tagged unlimited on
unlimited mode is ON
```

Telnet Command: vlan vid

This command is used to configure VID number for each VLAN channel.

Syntax

vlan vid *n vid_no*

Syntax Description

Parameter	Description
<i>n</i>	It means VLAN channel. The range is from 0 to 7.
<i>vid_no</i>	It means the value of VLAN ID. Type the value as the VLAN ID number. The range is from 0 to 4095.

Example

```
> vlan vid 1 4095
VLAN1, vid=4095
```

Telnet Command: vlan sysvid

This command is used to modify and show the scope (reserved 78) of the VLAN IDs used internally by the system.

Syntax

vlan sysvid [*show* | *n*]

Syntax Description

Parameter	Description
<i>show</i>	It means to show the scope of VLAN ID used internally.
<i>n</i>	It means the value to be set as VLAN ID. The range is from 0 to 4018.

Example

```
> vlan sysvid 100
You have set system VLAN ID to range: 100 ~ 177,
We recommend that you reboot the system now.

> vlan sysvid 200
You have set system VLAN ID to range: 200 ~ 263,
We recommend that you reboot the system now.

> vlan sysvid show
The system VLAN ID is in range: 200 ~ 263
```

Telnet Command: 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 <i>0/1</i>	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	
n	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 l(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 disable 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	
enable/disable	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 pstnringfixs [1| 2] [on| off]
voip dsp relaydbounce [on| off]
voip dsp setRingPat [ring_pattern_index] [patten_num]
voip dsp setDtmfCidlevel -l [value]
voip dsp setDtmfCidlevel -h [value]
voip dsp setDtmfCidlevel -r 0
voip dsp cidplusdigit [1/ 0] [channel] [value]

Syntax Description

Parameter	Description
voip dsp countrytone	
[channel] [value]	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
voip dsp dialtonepwr	
channel	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
AbsoluteValue	AbsoluteValue - In -1 dB increments, with 1 corresponding to 6 dBm. Range - 1 to 30
voip dsp EchoCanceler	
type	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.
w_size	The Line Echo Canceller (LEC) window size is 4, 6, 8 or 16 (ms).
nlp	Nlp - Non-linear processing (NLP) for more smooth transitions. 1 - disable 0 - enable
voip dsp cidtype	
channel	Set the caller ID type for FXS 1 (Channel 1) or FXS 2 (Channel 2). 1 - FXS 1 2 - FXS 2
value	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).
voip dsp micgain	
<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.
voip dsp spkgain	
<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.
voip dsp jb	
<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
voip dsp timer	
<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
Voip dsp debugMsg	
<i>?</i>	Available 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
voip dsp dtmfDetset	
<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)
voip dsp dtmfTonepwr	

<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
voip dsp cwtonepwr	
<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.
voip dsp pstnringfxs	
<i>1/ 2</i>	Enable or disable PSTN ring on FXS 1/FXS 2. 1 meansFXS1; 2 means FXS2.
<i>on/ off</i>	On means enable; off means disable.
voip dsp relaydbounce	
<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!!!
voip dsp setRingPat	
<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>
voip dsp setFaxECmode -s	
<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
voip dsp setDtmfCidlevel -l / voip dsp setDtmfCidlevel -h [value] voip dsp setDtmfCidlevel -r 0	
<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.
voip dsp setfxoCY	
<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"
voip dsp setfxoringl	
<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.
voip dsp setfxoCid	
<i>value</i>	Set FXO detect caller ID type. It is available only for the model with FXO port.
voip dsp cidplusdigit	
<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
voip dsp setRingThres	
<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.
voip dsp setCidDetGain	
<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 ?

```

```

> 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
voip rtp codec	
[<i>sip acc index</i>][<i>type size vad one</i>][<i>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
voip sip acc - 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 8 - wan1 first 9 - wan2 first 10 - wan3 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 255 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. 256 characters.
<i>-a [id]</i>	Set SIP authentication ID. Id - max. 256 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. 256 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

-u [url]	Set SIP URL for call forwarding (max. 255 characters).
-t [sec]	Set call forwarding timer. For example, voip sip acc 1 -t 30
-g [port]	Set the ring port for incoming call. For example, Port - r1 means FXS1; r2 means FXS2.
-z [pattern]	Set account ring pattern (1 ~ 6).
-i [enable]	Remove all bindings while they are un-registered. 0 means Disable; and 1 means Enable.
-l [option]	Enable to fix from header for Italian ITSP.
-B <enable>	Enable / disable the function of Broadsoft Call Control. 0 - disable 1 - enable
-C [number]	Set the alias index number (1 to 30).
-S [idx]	Enable and use alias IP to register. idx - 1 to 31. If 0 is used, such function will be disabled.
-k [num1 num2...]	Set backup wan list (first wan, second wan...). range: 1 to 4.
-v	View current status for account settings.
Voip sip calllog	Display current status for SIP call log.
voip sip ep	
n	The index number of the VoIP settings. n - 1, 2.
-o [acc]	Available dial out account (1 ~ 12).
-L [url]	Set SIP URL (max. 63 characters) for hot line.
-l [enable]	Enable / disable the function of hot line. 0 - disable 1 - enable
-W [enable]	Enable / disable the function of warm line. 0 - disable 1 - enable
-w [enable]	Enable / disable the function of call waiting enable. 0 - disable 1 - enable
-E [enable]	Enable / disable the function of call waiting enable but only remind one time. 0 - disable 1 - enable
-x <enable>	Enable / disable the function of call transfer. 0 - disable 1 - enable
-d [enable]	Enable / disable the function of DND (Do Not Disturb) 0 - disable 1 - enable
-s [id]	Indicate DND schedule. Id - s1, s2, s3, s4 (max. 4 schedule)
-h [enable]	Enable / disable the function of calling line identification restriction (CLIR). 0 - disable 1 - enable

<i>-u [mode]</i>	Set CLIR mode. 0 - means "draft-ietf-sip-privacy" 1 - means "rfc 3323/3325"
<i>-C [mode]</i>	Set the CLIR mode. 0 - not trusted. 1 - used among trusted SIP entities.
<i>-z [enable]</i>	Enable / disable playing dial tone when registered on sip server. 0 - disable 1 - enable
<i>-n [enable]</i>	Enable / disable session timer. 0 - disable 1 - enable
<i>-m [sec]</i>	Set the value for session timer (unit: sec).
<i>-R [min,max]</i>	Set the flash hook time range 100-2000 (unit: ms).
<i>-8 [enable]</i>	Enable or disable T.38 fax relay feature. 0 - disable 1 - enable
<i>-v</i>	View current settings.
voip sip misc - Allows users to set miscellaneous settings for the device.	
<i>-c [enable]</i>	Enable compact header to shorten the packet (0: disable, 1: enable).
<i>-s [enable]</i>	Change "#" into digit number. 0 - disable 1 - enable
<i>-e [enable]</i>	Enable Europe style flash hook operation mode. 0 - disable 1 - enable
<i>-h [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
<i>-p [enable]</i>	Enable PRACK message. 0 - Not support PRACK. 1 - Support PRACK.
<i>-P [enable]</i>	Enable IP Call. 0 - Disable IP call. 1 - Enable IP call.
<i>-H [enable]</i>	SIP INFO packet will be sent out when encountering hook flash event. 0 - disable 1 - enable
<i>-t [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 UAValue</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.

-D [disable]	Disable VoIP Service. 1 - disable VoIP service. 0 - enable VoIP service. System will automatic reboot to activate voip service
-v	View current status for miscellaneous settings.
voip sip nat - Allows users to set NAT Traversal Setting.	
-s [server]	Set the IP address for STUN server.
-t [sec]	Set ping interval for SIP account. Sec - 6 ~ 600
-i [ip]	Indicate external IP address.
-v	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
alias list idx : 0
>
```

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
<i>voip secure general -e</i>	Enable / disable secure phone feature. 0 - disable 1 - enable
<i>voip secure general -p</i>	Enable /disable SAS voice prompt. 0 - disable 1 - enable
<i>voip secure general -v</i>	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.

```
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]
vpn l2lset list index] x509localid [0/ 1]
```

Syntax Description

Parameter	Description
<i><list index></i>	It means the index number of L2L (LAN to LAN) profile.
<i>peerid <peerid></i>	It means the peer identity for aggressive mode.
<i>localid <localid></i>	It means the local identity for aggressive mode.
<i>main <auto/proposal index></i>	It means to choose proposal for main mode. <auto>: Choose default proposals. <proposal index>: choose specified proposal.
<i>aggressive <g1/ g2></i>	It means the chosen DH group for aggressive mode.
<i>pfs <on/ off></i>	It means “perfect forward secrete”. <on/off>: Turn on or off the PFS function.
<i>phase1 <lifetime> / phase2 <lifetime></i>	It means phase 1 or 2 of IKE. <lifetime>: Set the lifetime value (in second) for phase 1 and phase 2.
<i>x509localid <0/ 1></i>	It means to enable (1) or disable (0) the X509 local ID.

Example

```
> VPN l2lset 1 peerid 10226
```


Telnet Command: vpn l2lDrop

This command allows users to terminate current LAN to LAN VPN connection.

Syntax

vpn l2lDrop l2lname <name>

vpn l2lDrop l2lidx <idx>

vpn l2lDrop h2lname <name>

vpn l2lDrop h2lidx <idx>

vpn l2lDrop <ifno>

vpn l2lDrop

Syntax Description

Parameter	Description
<i>l2lname</i> <name>	It means to drop VPN connection by specifying the name of the LAN to LAN profile.
<i>l2lidx</i> <idx>	It means to drop VPN connection by specifying the index number of LAN to LAN profile.
<i>h2lname</i> <name>	It means to drop VPN connection by specifying the name of the remote dial-in user profile.
<i>h2lidx</i> <idx>	It means to drop VPN connection by specifying the index number of the remote dial-in user profile.
<ifno>	It means to drop VPN connection by using VPN ifno.
<i>l2lDrop</i>	It means to drop all VPN connections.

Example

```
> vpn l2lDrop
Drop all VPN
```

Telnet Command: vpn l2lDialout

This command allows users to terminate current LAN to LAN VPN connection (dial-out).

Syntax

vpn l2lDialout <idx>

vpn l2lDialout list

Syntax Description

Parameter	Description
<i>l2lDialout</i> <idx>	It means to build VPN connection by specifying the index number of dial-out LAN to LAN profile. <idx>: Enter an index number (1 to 32).
<i>list</i>	It means to display LAN to LAN profiles (enabled).

Example

```
> vpn l2lDialout list
List LAN to LAN profiles of the status as Enable
Index Profile Status
```

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> username <USERNAME>
vpn dinset <list index> password <PASSWORD>
vpn dinset <list index> motp <on/off>
vpn dinset <list index> pin_secret <pin> <secret>
vpn dinset <list index> timeout <0~9999>
vpn dinset <list index> dintype <Type> <on/off>
vpn dinset <list index> subnet <0~8>
vpn dinset <list index> assignip <on/off>
vpn dinset <list index> srnode <on/off>
vpn dinset <list index> remoteip <Remote_Client_IP_Address>
vpn dinset <list index> peer <Peer_ID>
vpn dinset <list index> naming <pass/block>
vpn dinset <list index> multicastvpn <pass/block>
vpn dinset <list index> prekey <on/off>
vpn dinset <list index> assignkey <Pre_Shared_Key>
vpn dinset <list index> digsig <on/off>
vpn dinset <list index> ipsec <Method> <on/off>
vpn dinset <list index> localid <Local_ID>

```

Syntax Description

Parameter	Description
<list index>	It means the index number of the profile.
<list index> <on/off>	It means to enable or disable the profile. <list index> - Enter the index number of the VPN profile. <on/off> - on: Enable; off: Disable.
<list index> motp <on/off>	It means to enable or disable the authentication with mOTP function. <list index> - Enter the index number of the VPN profile. <on/off> - on: Enable; off: Disable.
<list index> pin_secret <pin> <secret>	It means to set PIN code with secret. <list index> - Enter the index number of the VPN profile. <pin> - Type the code for authentication (e.g, 1234). <secret> - Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6)
<list index> timeout <0~9999>	It means to set idle timeout. The default is 300 (seconds). <list index> - Enter the index number of the VPN profile. <0~9999> - Enter a value.
<list index> dintype <Type> <on/off>	It means to enable/disable the allowed dial-in type. <list index> - Enter the index number of the VPN profile. <Type> - 0 to 3. In which, 0 means PPTP; 1 means IPsec Tunnel; 2 means L2TP with IPsec Policy; 3 means SSL Tunnel. <on/off> - on: Enable; off: Disable.
vpn dinset <list index> subnet <0~4>	It means to set the LAN subnet for the selected VPN profile. <list index> - Enter the index number of the VPN profile.

	<0-4> - Enter a number to specify the LAN subnet. In which, 0 means LAN1 1 means LAN2 2 means LAN3 3 means LAN4 4 means DMZ
<i>vpn dinset <list index> assignip <on/ off></i>	It means to enable or disable the function of assigning the static IP address. <list index> - Enter the index number of the VPN profile. <on/off> - on: Enable; off: Disable.
<i>vpn dinset <list index> srnode <on/ off></i>	It means to enable or disable the function of specifying the remote node. <list index> - Enter the index number of the VPN profile. <on/off> - on: Enable; off: Disable.
<i>vpn dinset <list index> remoteip <Remote_Client_IP_Address ></i>	It means to enable or disable the function of assigning remote client IP. <list index> - Enter the index number of the VPN profile. <Remote_Client_IP_Address> - Set the IP address of the remote client.
<i>vpn dinset <list index> peer <Peer_ID></i>	It means to assign the peer ID. <list index> - Enter the index number of the VPN profile. <Peer_ID> - Enter the string of the peer ID.
<i>vpn dinset <list index> naming <pass/ block></i>	It means to set the Netbiid Naming Packet for the VPN profile. <list index> - Enter the index number of the VPN profile. <pass/block> - Let the packet pass or block the packet.
<i>vpn dinset <list index> multicastvpn <pass/ block></i>	It means to set the multicast via VPN for IGMP, IP-CAM, DHCP relay, and etc. <list index> - Enter the index number of the VPN profile. <pass/block> - Let the packet pass or block the packet.
<i>vpn dinset <list index> prekey <on/ off></i>	It means to enable/disable the Pre-Shared Key setting for IKE Authentication Method. <list index> - Enter the index number of the VPN profile. <on/off> - on: Enable; off: Disable.
<i>vpn dinset <list index> assignkey <Pre_Shared_Key></i>	It means to set the Pre-Shared Key for IKE Authentication Method. <list index> - Enter the index number of the VPN profile. <Pre_Shared_Key> - Enter a string as PSK.
<i>vpn dinset <list index> digsig <on/ off></i>	It means to enable/disable the digital signature (X.509) for IKE Authentication Method. <list index> - Enter the index number of the VPN profile. <on/off> - on: Enable; off: Disable.
<i>vpn dinset <list index> ipsec <Method> <on/ off></i>	It means to enable / disable and set the protocol for IPsec security method. <list index> - Enter the index number of the VPN profile. <Method> - Enter a number (0 to 3) to specify the protocol. 0 means Medium(AH) High(ESP), 1 means DES 2 means 3DES 3 means AES <on/off> - on: Enable; off: Disable.
<i>vpn dinset <list index> localid <Local_ID></i>	It means to set local ID (optional) for IPsec Security Method. <list index> - Enter the index number of the VPN profile. <local_ID> - Enter the string of local ID.

Example

```
> vpn dinset 1

Dial-in profile index 1

Profile Name: ???
Status: Deactive
Mobile OTP: Disabled
Password:
Idle Timeout: 300 sec

> vpn dinset 1 on
% set profile active

> vpn dinset 1 motp on
% Enable Mobile OTP mode!>
> vpn dinset 1 pin_secret 1234 e759bb6f0e94c7ab4fe6
> vpn dinset 1

Dial-in profile index 1

Profile Name: ???
Status: Active

Mobile OTP: Enabled

PIN: 1234

Secret: e759bb6f0e94c7ab4fe6

Idle Timeout: 300 sec
```

Telnet Command: vpn subnet

This command allows users to specify a subnet selection for the specified remote dial-in VPN profile.

vpn subnet [*index*] [1/ 2/ 3/ 4]

Syntax Description

Parameter	Description
< <i>index</i> >	It means the index number of the VPN profile.
<1/ 2/ 3/ 4>	1 - it means LAN1 2 - it means LAN2. 3 - it means LAN3 4 - it means LAN4.

Example

```
> vpn subnet 1 2
>
```

Telnet Command: vpn setup

This command allows users to setup VPN for different types.

Command of PPTP Dial-Out

vpn setup <index> <name> **pptp_out** <ip> <usr> <pwd> <nip> <nmask>

Command of IPsec Dial-Out

vpn setup <index> <name> **ipsec_out** <ip> <key> <nip> <nmask>

Command of L2Tp Dial-Out

vpn setup <index> <name> **l2tp_out** <ip> <usr> <pwd> <nip> <nmask>

Command of Dial-In

vpn setup <index> <name> **dialin** <ip> <usr> <pwd> <key> <nip> <nmask>

Syntax Description

Parameter	Description
For PPTP Dial-Out	
<index>	It means the index number of the profile.
<name>	It means the name of the profile.
<ip>	It means the IP address to dial to.
<usr> <pwd>	It means the user and the password required for the PPTP connection.
<nip> <nmask>	It means the remote network IP and the mask. e.g., vpn setup 1 name1 pptp_out 1.2.3.4 vigor 1234 192.168.1.0 255.255.255.0
For IPsec Dial-Out	
<index>	It means the index number of the profile.
<name>	It means the name of the profile.
<ip>	It means the IP address to dial to.
<key>	It means the value of IPsec Pre-Shared Key.
<nip> <nmask>	It means the remote network IP and the mask. e.g., vpn setup 1 name1 ipsec_out 1.2.3.4 1234 192.168.1.0 255.255.255.0
For L2TP Dial-Out	
<index>	It means the index number of the profile.
<name>	It means the name of the profile.
<ip>	It means the IP address to dial to.
<usr> <pwd>	It means the user and the password required for the L2TP connection.
<nip> <nmask>	It means the remote network IP and the mask. e.g., vpn setup 1 name1 l2tp_out 1.2.3.4 vigor 1234 192.168.1.0 255.255.255.0
For Dial-In	
<index>	It means the index number of the profile.

<i><name></i>	It means the name of the profile.
<i><ip></i>	It means the IP address allowed to dial in.
<i><usr> <pwd></i>	It means the user and the password required for the PPTP/L2TP connection.
<i><key></i>	It means the value of IPsec Pre-Shared Key.
<i><nip> <nmask></i>	It means the remote network IP and the mask. e.g., vpn setup 1 name1 dialin 1.2.3.4 vigor 1234 abc 192.168.1.0 255.255.255.0

Example

```
> vpn setup 1 name1 dialin 1.2.3.4 vigor 1234 abc 192.168.1.0
255.255.255.0
% Profile Change Log ...

% Profile Index : 1
% Profile Name : name1
% Username : vigor
% Password : 1234
% Pre-share Key : abc
% Call Direction : Dial-In
% Type of Server : ISDN PPTP IPSec L2TP
% Dial from : 1.2.3.4
% Remote NEtwork IP : 192.168.1.0
% Remote NEtwork Mask : 255.255.255.0
>
```

Telnet Command: vpn option

This command allows users to configure settings for LAN to LAN profile.

vpn option *<index>* *<cmd1>=<param1> [<cmd2>=<para2> | ...]*

Syntax Description

Parameter	Description
<i><index></i>	It means the index number of the profile. Available index numbers: 1 ~ 32
For Common Settings	
<i><index></i>	It means the index number of the profile.
<i>pname</i>	It means the name of the profile.
<i>ena</i>	It means to enable or disable the profile. on - Enable off - Disable
<i>thr</i>	It means the way that VPN connection passes through. Available settings are w1f, w1o, w2f, and w2o. w1f - WAN1 First. w1o - WAN1 Only. w2f - WAN2 First.

	w2o - WAN2 Only.
<i>nnpkt</i>	It means the NetBios Naming Packet. on - Enable the function to pass the packet. off - Disable the function to block the packet.
<i>dir</i>	It means the call direction. Available settings are b, o and i. b - Both o - Dial-Out i - Dial-In.
<i>idle=[value]</i>	It means Always on and Idle Time out. Available values include: -1 - it means always on for dial-out. 0 - it means always on for dial-in. Other numbers (e.g., idle=200, idle=300, idle=500) mean the router will be idle after the interval (seconds) configured here.
<i>palive</i>	It means to enable PING to keep alive. -1 - disable the function. 1,2,3,4 - Enable the function and PING IP 1.2.3.4 to keep alive.
For Dial-Out Settings	
<i>ctype</i>	It means "Type of Server I am calling". "ctype=t" means PPTP. "ctype=s" means IPsec. "ctype= l" means L2TP(IPsec Policy None). "ctype= l1" means L2TP(IPsec Policy Nice to Have). "ctype= l2" means L2TP(IPsec Policy Must).
<i>dialto</i>	It means Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89).
<i>ltype</i>	It means Link Type. "ltype=0" means "Disable". "ltype=1" means "64kbps". "ltype=2" means "128kbps". "ltype=3" means "BOD".
<i>oname</i>	It means Dial-Out Username. "oname=admin" means to set Username = admin.
<i>opwd</i>	It means Dial-Out Password "opwd=1234" means to set Password = 1234.
<i>pauth</i>	It means PPP Authentication. "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. "ometh=espd/espda/" means ESP DES without/with Authentication. "ometh=esp3/esp3a/" means ESP 3DES without/with Authentication. "ometh=espa/espaa" means ESP AES without/with Authentication.

<i>sch</i>	It means Index(1-15) in Schedule Setup. sch=1,3,5,7 Set schedule 1->3->5->7
<i>rcallb</i>	It means Require Remote to Callback. “rcallb=on/off” means to enable/disable Set Require Remote to Callback.
<i>ikeid</i>	It means IKE Local ID. “ikeid=vigor” means Set Local ID = vigor.
For Dial-In Settings	
<i>itype</i>	It means Allowed Dial-In Type. Available settings include: “itype=t” means PPTP. “itype=s” means IPsec. “itype=L1” means L2TP (None). “itype=L1” means L2TP(Nice to Have). “itype=L2” means L2TP(Must).
<i>peer</i>	It means specify Peer VPN Server IP for Remote VPN Gateway. Type “203.12.23.48” means to allow VPN dial-in with IP address of 203.12.23.48. Type “off” means any remote IP is allowed to dial in.
<i>peerid</i>	It means the peer ID for Remote VPN Gateway. Type “draytek” means the word is used as local ID.
<i>iname</i>	It means Dial-in Username. “iname=admin” means to set username as “admin”.
<i>ipwd</i>	It means Dial-in Password. “ipwd=1234” means to set password as “1234”.
<i>ivj</i>	It means VJ Compression. “ivj=on/off” means to enable /disable VJ Compression.
<i>ikey</i>	It means IKE Pre-Shared Key. “ikey=abcd” means to set IKE Pre-Shared Key = abcd.
<i>imeth</i>	It means IPsec Security Method “imeth=h” means “Allow AH”. “imeth=d” means “Allow DES”. “imeth=3” means “Allow 3DES”. “imeth=a” means “Allow AES”.
For TCP/IP Settings	
<i>mywip</i>	It means My WAN IP. “mywip=1.2.3.4” means to set My WAN IP as “1.2.3.4”.
<i>rgip</i>	It means Remote Gateway IP. “rgip=1.2.3.4” means to set Remote Gateway IP as “1.2.3.4”.
<i>rnip</i>	It means Remote Network IP. “rnip=1.2.3.0” means to set Remote Network IP as “1.2.3.0”.
<i>rnmask</i>	It means Remote Network Mask. “rnmask=255.255.255.0” means to set Remote Network Mask as “255.255.255.0”.
<i>rip</i>	It means RIP Direction. “rip=d” means to set RIP Direction as “Disable”. “rip=t” means to set RIP Direction as “TX”. “rip=r” means to set RIP Direction as “RX”. “rip=b” means to set RIP Direction as “Both”.

<i>mode</i>	It means the option of “From first subnet to remote network, you have to do”. “mode=r” means to set Route mode. “mode=n” means to set NAT mode.
<i>droute</i>	It means to Change default route to this VPN tunnel (Only single WAN supports this). droute=on/off means to enable/disable the function.

Example

```
> vpn option 1 idle=250
% Change Log..

% Idle Timeout = 250
```

Telnet Command: **vpn mroute**

This command allows users to list, add or delete static routes for a certain LAN to LAN VPN profile.

vpn mroute *<index>* **list**

vpn mroute *<index>* **add** *<network ip>/<mask>*

vpn mroute *<index>* **del** *<network ip>/<mask>*

Syntax Description

Parameter	Description
<i>list</i>	It means to display all of the route settings.
<i>add</i>	It means to add a new route.
<i>del</i>	It means to delete specified route.
<i><index></i>	It means the index number of the profile. Available index numbers: 1 ~ 32
<i><network ip>/<mask></i>	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.

vpn list *<index>* **all**

vpn list *<index>* **com**

vpn list *<index>* **out**

vpn list *<index>* **in**

vpn list *<index>* **net**

Syntax Description

Parameter	Description
<i>all</i>	It means to list configuration of the specified profile.
<i>com</i>	It means to list common settings of the specified profile.
<i>out</i>	It means to list dial-out settings of the specified profile.
<i>in</i>	It means to list dial-in settings of the specified profile.
<i>net</i>	It means to list Network Settings of the specified profile.
<i><index></i>	It means the index number of the profile. Available index numbers: 1 ~ 32

Example

```
> vpn list 32 all
% Common Settings

% Profile Name           : ???
% Profile Status         : Disable
% Netbios Naming Packet  : Pass
% Call Direction         : Both
% Idle Timeout           : 300
% PING to keep alive     : off

% Dial-out Settings

% Type of Server         : PPTP
% Link Type:             : 64k bps
% Username               : ???
% Password               :
% PPP Authentication     : PAP/CHAP
% VJ Compression         : on
% Pre-Shared Key         :
% IPSec Security Method  : AH
% Schedule               : 0,0,0,0
% Remote Callback        : off
% Provide ISDN Number    : off
% IKE phase 1 mode       : Main mode
% IKE Local ID           :

% Dial-In Settings

--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
> vpn list 1 com
% Common Settings

% Profile Name           : ???
% Profile Status         : Disable
% Netbios Naming Packet  : Pass
% Call Direction         : Both
% Idle Timeout           : 300
% PING to keep alive     : off
>
```

Telnet Command: vpn remote

This command allows users to enable or disable *PPTP/ IPSec/ L2TP* VPN service.

vpn remote [*PPTP/ IPSec/ L2TP/ SSLVPN*] [*on/ off*]

Syntax Description

Parameter	Description
<i>PPTP/ IPSec/ L2TP/ SSLVPN</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 NetBios

This command allows users to enable or disable NetBios for Remote Access User Accounts or LAN-to-LAN Profile.

Syntax

vpn NetBios set <*H2l/ L2l*> <*index*> <*Block/ Pass*>

Syntax Description

Parameter	Description
< <i>H2l/ L2l</i> >	H2l means Remote Access User Accounts. L2l means LAN-to-LAN Profile. Specify which one will be applied by NetBios.
< <i>index</i> >	The index number of the profile.
< <i>Block/ Pass</i> >	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.
<i><connection type></i>	1-4 represent various type. 1 - PPTP 2 - L2TP 3 - IPSec 4 - L2TP over IPSec 5 - SSL Tunnel
<i><TCP maximum segment size range></i>	Each type has different segment size range. PPTP - 1 ~ 1412 L2TP - 1 ~ 1408 IPSec - 1 ~ 1381 L2TP over IPSec - 1 ~ 1361 SSL Tunnel - 1 ~ 1360

Example

```
>vpn mss set 1 1400
% VPN TCP maximum segment size (MSS) :
  PPTP   = 1400
  L2TP   = 1360
  IPSec  = 1360
  L2TP over IPSec = 1360
  SSL Tunnel = 1260
>vpn mss show
VPN TCP maximum segment size (MSS) :
  PPTP   = 1400
  L2TP   = 1360
  IPSec  = 1360
  L2TP over IPSec = 1360
  SSL Tunnel = 1260
```

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 L2I 1 Pass
% Lan to Lan Profile Index [1] :
% Status Block/Pass: [PASS]
```

Telnet Command: vpn pass2nd

This command allows users to determine if the packets coming from the second subnet passing through current used VPN tunnel.

Syntax

vpn pass2nd [on]

vpn pass2nd [off]

Syntax Description

Parameter	Description
on/ off	on - the packets can pass through NAT. off - the packets cannot pass through NAT.

Example

```
> vpn pass2nd on
% 2nd subnet is allowed to pass VPN tunnel!
```

Telnet Command: vpn pass2nat

This command allows users to determine if the packets passing through by NAT or not when the VPN tunnel disconnects.

Syntax

vpn pass2nat [on]

vpn pass2nat [off]

Syntax Description

Parameter	Description
on/ off	on - the packets can pass through NAT.

	off - the packets cannot pass through NAT.

Example

```
> vpn pass2nat on
% Packets would go through by NAT when VPN disconnect!!
```

Telnet Command: vpn passAPM

This command allows packets from APM to pass the VPN tunnel or not.

Syntax

vpn passAPM on

vpn passAPM off

Example

```
> vpn passAPM on
% APM broadcast is allowed to pass VPN tunnel!
```

Telnet Command: vpn sameSubnet

This command allows users to build VPN between clients via virtual subnet.

Syntax

vpn sameSubnet -i <value>

vpn sameSubnet -E <0/ 1>

vpn sameSubnet -e <value>

vpn sameSubnet -l <Virtual Subnet>

vpn sameSubnet -o <add/ del>

vpn sameSubnet -v

vpn sameSubnet -m

Syntax Description

Parameter	Description
-i <value>	Specify the index number of VPN profile.
-E <0/ 1>	Enable or disable the IPsec with the same subnet. 1 - enable. 0 - disable.
-e <value>	Translate specified LAN to virtual subnet. 1 - LAN1 2 - LAN2 3 - LAN3 ...
-l <Virtual Subnet>	Set the virtual subnet (e.g., 172.16.3.250).
-v	Display current status of virtual subnet.
-m <1/ 2>	Set the Translated Type. <1/ 2> - 1 for Whole Subnet, 2 for Specific IP.

Example

```

> vpn sameS -i 1 -e 1 -E 1 -e 1 -I 10.10.10.0 -o add
> vpn sameS -v
IPsec with the same subnet:
VPN profile 1 enable,
% translated LAN1 to Virtual subnet: 10.10.10.0

```

Telnet Command: vpn ovpn

This command allows users to build VPN between clients via OpenVPN.

Syntax

```

vpn ovpn mode <0/1>
vpn ovpn show
vpn ovpn udp_mode <0/1>
vpn ovpn tcp_mode <0/1>
vpn ovpn udp_port <1-65535>
vpn ovpn tcp_port <1-65535>
vpn ovpn cert <0/1>
vpn ovpn replay <0/1>
vpn ovpn certmode <0/1/2>
vpn ovpn hmacmode <0/1/2>

```

Syntax Description

Parameter	Description
<i>mode</i> <0/ 1>	Enable or disable the OpenVPN function. 1 - enable. 0 - disable.
<i>show</i>	Displays current OpenVPN settings.
<i>udp_mode</i> <0/ 1>	Enable or disable the UDP mode. 1 - enable. 0 - disable.
<i>tcp_mode</i> <0/ 1>	Enable or disable the TCP mode. 1 - enable. 0 - disable.
<i>udp_port</i> <1-65535>	Enter a port number (1-65535) for UDP mode.
<i>tcp_port</i> <1-65535>	Enter a port number (1-65535) for TCP mode.
<i>replay</i> <0/ 1>	Enable or disable the replay option. 1 - enable. 0 - disable.
<i>certmode</i> <0/ 1/ 2>	Set the Cipher Algorithm Mode. 0: AES128, 1: AES256, 2: None
<i>hmacmode</i> <0/ 1/ 2>	Set the Cipher HMAC Mode. 0: SHA1, 1: SHA256, 2: None

Example

```

> vpn ovpn mode 1

```

```

Enable openvpn
> vpn ovpn show

Openvpn: Enable
support UDP: Enable
UDP port: 1194
support TCP: Enable
TCP port: 1194
Use certificate authentication: Enable
replay option: Enable
Cipher Algorithm: AES256
HMAC Algorithm: SHA256
Certificate uid: 65535
Trust CA uid: 0

```

Telnet Command: wan ppp_mru

This command allows users to adjust the size of PPP LCP MRU. It is used for specific network.

wan ppp_mru <WAN interface number> <MRU size >

Syntax Description

Parameter	Description
<WAN interface number>	Type a number to represent the physical interface. For Vigor130, the number is 1 (which means WAN1).
<MRU size >	It means the number of PPP LCP MRU. The available range is from 1400 to 1600.

Example

```

>wan ppp_mru 1 ?
% Now: 1492

> wan ppp_mru 1 1490
>
> wan ppp_mru 1 ?
% Now: 1490

> wan ppp_mru 1 1492
> wan ppp_mru 1 ?
% Now: 1492

```

Telnet Command: wan mtu/wan mtu2

This command allows users to adjust the size of MTU/MTU2 for WAN.

wan mtu [value]

wan mtu2 [value]

Syntax Description

Parameter	Description
value	It means the number of MTU for PPP. The available range is from 1000 to 1500. For Static IP/DHCP, the maximum number will be 1500.

	For PPPoE, the maximum number will be 1492. For PPTP/L2TP, the maximum number will be 1460.

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 dns

This command allows users to configure primary and / or secondary DNS server.

Syntax

wan dns <wan_no> <dns_select> <ipv4_addr>

Syntax Description

Parameter	Description
<wan_no>	Select WAN interface. 1 ~4 - WAN1 ~ WAN4.
<dns_select>	Specify primary and / or secondary DNS server. pri - It means primary DNS server. sec - It means secondary DNS server.
<ipv4_addr>	Enter the IP address of DNS server.

Example

```
> wan dns 1 pri 168.95.1.1
% Set WAN1 primary DNS done.
% Now: 168.95.1.1
```

Telnet Command: wan DF_check

This command allows you to enable or disable the function of DF (Don't fragment)

wan DF_check [on]

wan DF_check [off]

Syntax Description

Parameter	Description
on/off	It means to enable or disable DF.

Example

```
> wan DF_check on
%DF bit check enable!
```

Telnet Command: wan disable

This command allows you to disable WAN connection.

Example

```
> wan disable WAN
%WAN disabled.
```

Telnet Command: wan enable

This command allows you to disable wan connection.

Example

```
> wan enable WAN
%WAN1 enabled.
```

Telnet Command: wan forward

This command allows you to enable or disable the function of WAN forwarding. The packets are allowed to be transmitted between different WANs.

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
PVC_WAN6: 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

This command, wan modem, allows you to configure 3G/4G USB Modem (PPP mode) of WAN3.

Syntax

wan modem [*init/dial/pin*][*string*]

wan modem wakeup [*on/off/value*]

Syntax Description

Parameter	Description
<i>init</i>	Set initial modem AT command (default value is "AT&FE0V1X1&D2&C1S0=0").
<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>wakeup [on/off]</i>	It is for RD debug only. Please don't use it without our advice.

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 wimax

This command allows you to enable or disable WAN 3G/4G DHCP mode for Vigor router.

Syntax

wan wimax <*on/off*>

Syntax Description

Parameter	Description
<i>On</i>	It means to enable WAN 3G/4G DHCP mode.
<i>off</i>	It means to disable WAN 3G/4G DHCP mode.

Example

```
> wan wimax ?
Current status is wimax OFF
DHCP client Disabled
Current wimax zone=0
Current wimax username=
Current wimax password=
Current wimax identity=
> wan wimax on
>
```

Telnet Command: wan detect

This command allows you to Ping a specified IP to detect the WAN connection (static IP or PPPoE mode).

wan detect [*wan1*][*on/ off/ always_on*]

wan detect [*wan1*]**target** [*ip addr*]

wan detect [*wan1*]**tll** [*1-255*]

wan detect status

Syntax Description

Parameter	Description
<i>on</i>	It means to enable ping detection. The IP address of the target shall be set.
<i>off</i>	It means to enable ARP detection (default).
<i>always_on</i>	disable link detect, always connected(only support static IP)
<i>target</i>	It means to set the ping target.
<i>ip addr</i>	It means the IP address used for detection. Type an IP address in this field.
<i>tll</i>	It means to set the ping TTL value (work as trace route) If you do not set any value for ttl here or just type 0 here, the system will use default setting (255) as the ttl value.
<i>status</i>	It means to show the current status.

Example

```
> wan detect status
WAN1: arp detect, send time=30, Interval = 5
WAN2: arp detect, send time=30, Interval = 5
WAN3: arp detect, send time=30, Interval = 5
WAN4: arp detect, send time=30, Interval = 5
WAN5: arp detect, send time=30, Interval = 5
WAN6: arp detect, send time=30, Interval = 5
> wan detect wan1 target 192.168.1.78
Set OK

> wan detect wan1 on
Set OK

> wan detect status
```

```

WAN1: ping detect, Target=192.168.1.78, TTL=255, Target2=0.0.0.0,
TargetGW=off,
Interval=1, Retry=10
WAN2: arp detect, send time=30, Interval = 5
WAN3: arp detect, send time=30, Interval = 5
WAN4: arp detect, send time=30, Interval = 5
WAN5: arp detect, send time=30, Interval = 5
WAN6: arp detect, send time=30, Interval = 5
>

```

Telnet Command: wan lb

This command allows you to Enable/Disable for each WAN to join auto load balance member.

wan lb [*wan1/wan2/..*] *on*

wan lb [*wan1/wan2/..*] *off*

Syntax Description

Parameter	Description
<i>wan1/wan2</i>	It means to specify which WAN will be applied with load balance.
<i>on</i>	It means to make WAN interface as the member of load balance.
<i>off</i>	It means to cancel WAN interface as the member of load balance.

Example

```

> wan lb status
WAN1: on
WAN2: on
WAN3: on
WAN4: on
WAN5: on
WAN6: on
Load balance mode is IP based
>

```

Telnet Command: wan lbel

This command allows you to set load balance exception list.

Syntax

wan lbel <*idx*> <*enable*> <*protocol*> <*ip type*> <*obj_grp idx*> <*port*> <*port_end*> <*comment*>

wan lbel status <*idx*>

Syntax Description

Parameter	Description
<i>idx</i>	Enter the index number (1 to 32) for the exception list.
<i>enable</i>	Enter 1 (enable) or 0 (disable) the selected profile.
<i>protocol</i>	<protocol>: Enter TCP, UDP, ALL (TCP+UDP).
<i>ip type</i>	Set the IP type (0, 1 or 2) for the selected profile. 0: Any 1: IP object

	2: IP group
<i>obj_grp idx</i>	Enter the index number (1 to 32 for IP group; 1 to 192 for IP object). If it is set with "0", then the IP type will be set as "Any".
<i>port</i>	Enter a number (0 to 65535) as starting port. If it is set with "0", then the port range (1 to 65535) will not be applied with load balance.
<i>port_end</i>	Enter a number (0 to 65535) as ending port (must be greater than starting port).
<i>comment</i>	Enter a string (less than 11 characters) as a comment.
<i>status</i>	Show the current status.

Example

```
> wan lbel 1 1 tcp 0 1 0 300 testforload
> wan lbel status 1
list[1] status:enable, protocol:tcp, IP type:any, IP idx:0, port:0~300, comment:testforload
list[2] status:enable, protocol:udp, IP type:any, IP idx:0, port:19302~19302, comment:Google STUN
list[3] status:enable, protocol:tcp+udp, IP type:any, IP idx:0, port:5060~5060, comment:SIP
list[4] status:disable, protocol:tcp, IP type:any, IP idx:0, port:80~80, comment:HTTP
list[5] status:disable, protocol:tcp, IP type:any, IP idx:0, port:443~443, comment:SSL
...
```

Telnet Command: wan mvlan

This command allows you to configure multi-VLAN for WAN and LAN. It supports pure bridge mode (modem mode) between Ethernet WAN and LAN port 2~4.

wan mvlan [*pvc_no/ status/ save/ enable/ disable*] [*on/ off/ clear/ tag tag_no*] [*service type/ vlan priority*] [*px ...*] [*Keep Tag*]

Syntax Description

Parameter	Description
<i>pvc_no</i>	It means index number of PVC. There are 10 PVC, 0(Channel-1) to 9(Channel-9) allowed to be configured. However, only 2 to 9 are available for configuration.
<i>status</i>	It means to display the whole Bridge status.
<i>save</i>	It means to save the configuration into flash of Vigor router.
<i>enable/ disable</i>	It means to enable/disable the Multi-VLAN function.
<i>on/ off</i>	It means to turn on/off bridge mode for the specific channel.
<i>clear</i>	It means to turn off/clear the port.
<i>tag tag_no</i>	It means to tag a number for the VLAN. -1: No need to add tag number. 1-4095: Available setting numbers used as tagged number.
<i>service type</i>	It means to specify the service type for VLAN. 0: Normal. 1: IGMP.
<i>vlan priority</i>	It means to specify the priority for the VALN setting.

	Range is from 0 to 7.
<i>px</i>	It means LAN port. Available setting number is from 2 to 4. Port number 1 is locked for NAT usage.
<i>Keep Tag</i>	It means Multi-VLAN packets will keep their VLAN headers to LAN.

Example

PVC 7 will map to LAN port 2/3/4 in bridge mode; service type is Normal. No tag added.

```
> wan mvlan 7 on p2 p3 p4
PVC Bridge p1 p2 p3 p4 p5 p6 Service Type Tag Priority Keep Tag
-----
7 ON 0 0 1 1 0 0 Normal 0 (OFF) 0 OFF
>
```

Telnet Command: wan multifno

This command allows you to specify a channel (in Multi-PVC/VLAN) to make bridge connection to a specified WAN interface.

wan multifno [*channel #*] [*WAN interface #*]

wan multifno *status*

Syntax Description

Parameter	Description
<i>channel #</i>	There are several channels including VLAN and PVC.
<i>WAN interface #</i>	Type a number to indicate the WAN interface. 1=WAN1, 2=WAN2, 3=WAN3
<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 4 uplink ifno: 3
% Channel 5 uplink ifno: 3
% Channel 6 uplink ifno: 3
% Channel 7 uplink ifno: 3
% Channel 8 uplink ifno: 3
% Channel 9 uplink ifno: 3
> wan multifno 9 2
% Configured channel 9 uplink to WAN2
> wan multifno status
% Channel 4 uplink ifno: 3
% Channel 5 uplink ifno: 3
% Channel 6 uplink ifno: 3
% Channel 7 uplink ifno: 3
% Channel 8 uplink ifno: 3
% Channel 9 uplink ifno: 4
```

Telnet Command: wan vlan

This command allows you to tag packets on WAN VLAN with specified number.

Syntax

```
wan vlan wan [#] tag [value]
wan vlan wan [#] [enable|disable]
wan vlan wan [#] pri [value]
wan vlan wan [#] adsl tag [value]
wan vlan wan [#] adsl [enable|disable]
wan vlan wan [#] adsl pri[value]
wan vlan wan [#] vdsl tag [value]
wan vlan wan [#] vdsl [enable|disable]
wan vlan wan [#] vdsl pri[value]
wan vlan stat
```

Syntax Description

Parameter	Description
<i>#</i>	It means the number of WAN interface. 1: means WAN1 2: means WAN2.
<i>value</i>	It means the number to be tagged on packets. The range of the value is between 32 ~ 4095.
<i>enable disable</i>	It means to enable or disable the WAN interface for VLAN.
<i>pri[value]</i>	It means to set priority of data transmission via 802.1q. The range of the value is between 0 ~ 7.
<i>stat</i>	It means to display the table of WAN VLAN status.

Example

```
> wan vlan stat
%Interface      Pri      Tag      Enabled
%=====
% WAN1 (ADSL)   0        0
% WAN1 (VDSL)   0        0
% WAN2          0        0
```

Telnet Command: wan phyvlan

This command is used to set VLAN tag insertion for outer tag (service) for WAN interface. WAN interfaces must be configured first before setting VLAN encapsulation.

Syntax

```
wan phyvlan wan <#> tag <value>
wan phyvlan wan <#> pri <value>
wan phyvlan wan <#> <enable/disable>
wan phyvlan stat
```

Syntax Description

Parameter	Description
<#>	It means WAN interface. 1 ~2- WAN1 ~ WAN2
tag <value>	It means to tag a value (1 to 4095) onto the selected WAN interface.
pri <value>	It means to set value (0 to 7) for priority for such VLAN tag.
<enable/ disable>	It means to enable / disable the VLAN tag.
stat	Display the setting status.

Example

```

> wan phyvlan wan 1 tag 22
% Set physical port tag to 22 for WAN1
% Set physical port tag to 22 for WAN1
% You need to reboot router making config effective
> wan phyvlan wan 1 enable
% Set physical port tag to 22 for WAN1
% Set physical port tag to 22 for WAN1
% You need to reboot router making config effective
> wan phyvlan stat ?

% Interface      Pri      Tag      Enabled
% =====
% WAN1 (ADSL)    --      --      --
% WAN1 (VDSL)     0       22
% 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 <#> custom_mode <0/ 1>
wan budget wan <#> custom_mode_reset_hour <hour>
wan budget wan [#] action [action bit map]
wan budget status

```

Syntax Description

Parameter	Description
wan[#]	Specify the WAN interface.
rdate	Specify the WAN budget refresh time. day - Available settings are from 1 to 30.

	hour - Available settings are from 1 to 23. E.g., wan budget wan 1 rdate 5 10 If 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)
<i>gthres[budget limit (GB)]</i>	Specify the maximum value of wan budget limit. (Unit: GB)
<i>mode</i> <i>[monthly periodic none]</i>	Specify the calculation mode (monthly, periodically, or none) for WAN budget.
<i>psday [th day in periodic]</i>	It is used only when mode is set with “periodic”. Specify the order of “today” in the cycle. E.g., wan budget wan 5 psday → It means “today” is the 5th day in the billing cycle.
<i>custom_mode <0/ 1></i>	Set the custom mode (cycle in hours or in days). 0: cycle_in_hours 1: cycle_in_days
<i>custom_mode_reset_hour</i> <i><hour></i>	Set the reset hour value. hour: Enter 1 to 23.
<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. If 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 [host/ IPv6 address] -s [base_size]*

Syntax Description

Parameter	Description
<i>-w [number]</i>	Specify the WAN interface number: Type the number of WAN interface. 1: WAN1; 2:WAN2....and etc.
<i>-i [host/ IPv6 address]</i>	Specify the IPv6 target to detect. It must be an IPv6 IP address or host name. IPv6 address: Type the IPv6 address of the target.
<i>-s [base_size]</i>	Specify the size of MTU. base_size: Available setting is 1280 ~ 1500.

Example

```
> wan detect_mtu6 -w 1 -i 2404:6800:4008:c06::5e -s 1500
>
```

Telnet Command: wan failover

This command is used to configure failover WAN.

Syntax

wan failover off *<index>*

wan failover on *<1><2><3><4><5><6>*

wan failover show *<index>*

Syntax Description

Parameter	Description
<i>failover off <index></i>	Set specified WAN interface to always on. index - Ranges from 1 to 3.
<i>failover on <1><2><3><4><5><6></i>	There are six fields which represent different options. Field 1 - Specify WAN interface as failover WAN by typing 1 to 4. Field 2 - Enable / disable the action for the failover WAN. Such action is "Active When selected WAN [disconnect/reached traffic threshold]".

	0 - Disable 1 - Enable Field 3 - Enable / disable the action for the failover WAN. Such action is "Active When [any/all] of selected WAN disconnect or reached traffic threshold". 0 - Disable 1 - Enable Field 4 - Specify main WAN by typing 1 to 4. The main WAN will be set to always on. Field 5 - Specify traffic threshold [Download threshold(Kbps)]. Field 6 - Specify traffic threshold [Upload threshold (Kbps)]. For example, WAN 2 will be set as failover, and will be active when any of selected WANs has reached traffic threshold. WAN 4 is the selected WAN. Download threshold : 50 Kbps; Upload threshold : 20 Kbps. You can type as follows: <i>wan failover on 2 1 0 4 50 20</i>
<i>show <index></i>	Display parameters settings for WAN interface. index - Ranges from 1 to 3.

Example

```

> wan failover on 2 1 0 4 50 20
> wan failover show 2
  wan2 Active Mode : Failover
    Active when : Any of the selected WANs reached the Traffic Threshold
    Traffic Download Threshold : 50 Kbps
    Traffic Upload Threshold   : 20 Kbps
>

```

Telnet Command: hsportal

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

hsportal setup -p <profile> [-l <lan>] [-s <ssid>] ...

hsportal setup -p <profile> -c

Syntax Description

Parameter	Description
-p <profile>	Indicate available profile to be configured. <profile>: Enter the index number (1 to 4) of the profile.
-l	Apply to LAN interfaces (1 to 8). For example: hsportal setup -p 1 -l 1, 2 (apply LAN1 and LAN2)
-s	Apply to WLAN interfaces (1 to 4). For example: hsportal setup -p 1 -s 1, 2 (apply SSID1 and SSID2)
-a	Apply to WLAN5G interfaces (1 to 4). For example: hsportal setup -p 1 -a 1, 2 (apply SSID1 and SSID2)
-m	Select login mode. 0: skip 1: click 2: social

	3: pin 4: social or pin For example: hspportal setup -p 1 -m 0
-f <0/ 1>	It menas to enable or disable the function of Configure facebook login. 0: disable. 1: enable.
-g <0/ 1>	It menas to enable or disable the function of Configure google login. 0: disable. 1: enable.
-h <0/ 1>	It menas to enable or disable the function of HTTPS redirection. 0: disable. 1: enable.
-v <0/ 1>	It menas to enable or disable the function of portal detection. 0: disable. 1: enable.
-i <string>	It means to set APP ID. <string>: Enter a string as APP ID. For example, to configure facebook APP id, you can type: > hspportal set -p 1 -f 1 -i this_is_app_id Profile 1 set facebook login enabled ... [OK] Profile 1 set API ID ... [OK]
-k <string>	It means to set APP key. <string>: Enter a string as APP key. For example, to configure google APP key, you can type: > hspportal set -p 1 -g 1 -k keyforapp Profile 1 set google login enabled ... [OK] Profile 1 set API KEY ... [OK]
-r <0/ 1/ 2>	It means to set landing page mode. 0: fixed URL. 1: user request. 2: bulletin. For example, > hspportal set -p 1 -r 0 Profile 1 set landing page mode 0 ... [OK]
-e	Enable the specified profile.
-d	Disable the specified profile.
-c <1/ 2/ 3/ 4>	Reset the specified profile. <1/2/3/4>: Enter the index number of profile. For example, > hspportal set -p 1 -c Reset profile 1 ... [OK]
-o	Clear profiles for all clients.
-t <value>	Set the expire time for the specified profile. <value>: Enter a number of time period (unit: minutes). For example, k> hspportal setup -p 1 -t 300 Profile 1 set expire time 300 mins ... [OK]

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: hsportal level

This command allows the user to configure bandwidth and sessions quota which is only applicable to the web portal clients.

Syntax

hsportal level -p <index> [-e <enable>] [-t <mins>] ...

Syntax Description

Parameter	Description
-p <index>	It means to specify (add) a quota policy profile. <index>: Enter the index number (1 to 20) of the quota policy profile.
-e <0/ 1>	It means to enable or disable the quota policy profile. 0: disable. 1: enable.
-t <value>	It means to set expired time for quota policy. <value>: Enter a number (unit:minutes).
-i <0/ 1> -o <value>	It means to enable or disable the function of idle timeout 0: disable. 1: enable. If enabled, -o <value>: Set the idle timeout (unit:minutes) if idle timeout is enabled. For example: hsportal level -p 1 -e 1 -i 1 -o 300
-d <value>	It means to set the maximum number of devices that can be connected to the network using the same account. <value>: Enter a number (0 to 100). "0" means unlimited. For example: hsportal level -p 1 -e 1 -d 0
-ru <0/ 1>	It means to specify the bandwidth limit download unit. 0: kbps 1: mbps
-tu <0/ 1>	It means to specify the bandwidth limit upload unit. 0: kbps. 1: mbps.
-U <kbps/ mbps>	It means to specify the bandwidth upload limit. kbps mbps
-D <kbps/ mbps>	It means to specify the bandwidth download limit. kbps

	mbps
-c <index>	It means to delete a quota policy profile. <index>: Enter the index number (1 to 20) of the quota policy profile.
-r <0/ 1>	It means to enable or disable the function of reconnection time restriction. 0:disable. 1:enable.
-f <value>	It means to set a period of time to block the same user reconnecting to the network. <value>: Enter a number (1 to 1439 minutes). For example: hsportal level -p 1 -e 1 -r 1 -f 300
-g <value>	It means to set a reconnection time to block the same user from reconnecting before the set time. <value>: Enter the hour (01 to 23) and the minutes (0-59) (unit: minutes). For example: hsportal level -p 1 -e 1 -r 1 -f 23:15 (The same user can reconnect after 23:15 every day)

Example

```
> hsportal level -p 1 -e 1 -r 1 -f 30000
>
```

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]*

wl config dtim *<value>/ show*

wl config beaconperiod *<value> / show*

wl config radio *<1/ 0>/ show*

wl config frag *<value>/ show*

wl config rts <value> / show
wl config rate_alg <value> / show
wl config country <value> / show

Syntax Description

Parameter	Description
<i>mode</i> [value]	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</i> [number]	It means the channel of frequency of the wireless LAN. The available settings are 0,1,2,3,4,5,6,7,8,9,10,11,12 and 13. number=0, means Auto number=1, means Channel 1 number=13, means Channel 13.
<i>preamble</i> [enable]	It means to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. 0: disable to use long preamble. 1: enable to use long preamble.
<i>txburst</i> [enable]	It means to enhance the performance in data transmission about 40%* more (by enabling Tx Burst). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. 0: disable the function. 1: enable the function.
<i>ssid</i> [ssid_num enable ssid_name [hidden_ssid]]	It means to set the name of the SSID, hide the SSID if required. ssid_num: Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. ssid_name: Give a name for the specified SSID. hidden_ssid: Type 0 to hide the SSID or 1 to display the SSID
<i>Security</i> [SSID_NUMBER] [mode][key][index]	It means to configure security settings for the wireless connection. SSID_NUMBER: Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. mode: Available settings are: disable: No security. wpa1x: WPA/802.1x Only wpa21x: WPA2/802.1x Only wpamix1x: Mixed (WPA+WPA2/802.1x only) wep1x: WEP/802.1x Only wpapsk: WPA/PSK wpa2psk: WPA2/PSK wpamixpsk: Mixed (WPA+WPA2)/PSK wep: WEP key, index: Moreover, you have to add keys for wpapsk, wpa2psk, wpamixpsk and wep, and specify index number of schedule profiles to be followed by the wireless connection. WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8-63 ASCII text string or 64 Hexadecimal digit format.
<i>ratectl</i> [ssid_num enable	It means to set the rate control for the specified SSID.

<i>upload download]</i>	<i>ssid_num</i> : Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. <i>enable</i> : It means to enable the function of the rate control for the specified SSID. 0: disable and 1:enable. <i>upload</i> : It means to configure the rate control for data upload. The unit is kbps. <i>download</i> : It means to configure the rate control for data download. The unit is kbps.
<i>isolate [ssid_num lan member]</i>	It means to isolate the wireless connection for LAN and/or Member. <i>lan</i> - It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other. <i>member</i> - It can make the wireless clients (stations) with the same SSID not accessing for each other.
<i>dtim <value> / show</i>	Set the DTIM value. value: 1 to 255 show: Display the DTIM setting.
<i>beaconperiod <value> / show</i>	Set the beaconperiod value. value: 20 to 1023 (milli-second) show: Display the beaconperiod etting.
<i>radio <1/ 0>/ show</i>	Enble or disable the wireless radio. 1/0: Type 1 to enable; 0 to disable. show: Display the radio setting.
<i>frag<value>/ show</i>	Set the fragment value. value: 256 to 2346 show: Display the fragment setting.
<i>rts <value> / show</i>	Set the RTS value. value: 1 to 2347 show: Display the RTS setting.
<i>rate_alg <value>/ show</i>	Set the algorithm for ALG rate. value: 0 for old algorithm; 1 for new algorithm. show: Display the ALG rate setting.
<i>country <value>/ show</i>	Set the country code for a country. value: two capital letters, e.g., TW, UK show: Display the country cod setting.

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: wpalx
%% Wireless card must be reset for configurations to take effect
%% (Telnet Command: wl restart)
```

Telnet Command: wl set

This command allows users to configure basic wireless settings.

wl set [*SSID*] [*CHAN* [*En*]]

wl set txburst [*enable*]

Syntax Description

Parameter	Description
<i>SSID</i>	It means to type the SSID for the router. The maximum character that you can use is 32.
<i>CHAN</i> [<i>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</i> [<i>enable</i>]	It means to enhance the performance in data transmission about 40%* more (by enabling Tx Burst). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. 0: disable the function. 1: enable the function.

Example

```
> wl set MKT 2 on
% New Wlan Setting is:
% SSID=MKT
% Chan=2
% Wl is Enable
```

Telnet Command: wl act

This command allows users to activate wireless settings.

wl act [*En*]

Syntax Description

Parameter	Description
<i>En</i>	It means to enable or disable the function of VPN isolation. 0: diable 1: enable

Example

```
> wl act on
% Set Wlan to Enable.
```

Telnet Command: wl 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/ 4/ 5>

Syntax Description

Parameter	Description
<i>start</i>	It means to start AP scanning.
<i>set</i> <wlist/ blist/ stime> <MAC>	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., <i>wl scan set wlist 001122aabbcc</i> <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., <i>wl scan set time 5</i>
<i>del</i> <wlist/ blist><MAC>	Remove white list/block list. e.g., <i>wl scan del wlist 001122aabbcc</i>
<i>filter</i> <ssid/ channel/ mac>	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</i> <0/ 1/ 2/ 3/ 4/ 5>	It is used to show AP list. 0 - display white list 1 - display block list, 2 - display gray/unknown list, 3 - display all list 4. white list(in config) 5. block list(in config) Note : 0-3 is the list router scan, 4-5 is the list stored in config.

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.

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 wmm

This command allows users to set WMM for wireless connection. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs).

wl wmm ap *QueIdx Aifsn Cwmin Cwmax Txop ACM*

wl wmm bss *QueIdx Aifsn Cwmin Cwmax Txop ACM*

wl wmm ack *Que0_Ack Que1_Ack Que2_Ack Que3_Ack*

wl wmm enable *SSID0 SSID1 SSID2 SSID3*

wl wmm apsd *value*

wl wmm show

Syntax Description

Parameter	Description
<i>ap</i>	It means to set WMM for access point.
<i>bss</i>	It means to set WMM for wireless clients.
<i>ack</i>	It means to map to the Ack policy settings of AP WMM.
<i>enable</i>	It means to enable the WMM for each SSID. 0: disable 1: enable
<i>Apsd [value]</i>	It means to enable / disable the ASPD(automatic power-save delivery) function. 0: disable 1: enable
<i>show</i>	It displays current status of WMM.
<i>QueIdx</i>	It means the number of the queue which the WMM settings will be applied to. There are four queues, best effort, background, voice, and video.
<i>Aifsn</i>	It controls how long the client waits for each data transmission.
<i>Cwmin/ Cwmax</i>	CWMin means contention Window-Min and CWMax means contention Window-Max. Specify the value ranging from 1 to 15.
<i>Txop</i>	It means transmission opportunity. Specify the value ranging from 0 to 65535.
<i>ACM</i>	It can restrict stations from using specific category class if it is enabled. 0: disable 1: enable

Example

```
> wl wmm ap 0 3 4 6 0 0
  QueIdx=0: APAifsn=3,APCwmin=4,APCwmax=6, APTxop=0,APACM=0
> wl wmm enable 1 0 1 0
  WMM_SSID0 =1, WMM_SSID1 =0,WMM_SSID2 =1,WMM_SSID3 =0
> wl wmm show
  Enable WMM: SSID0 =1, SSID1 =0,SSID2 =1,SSID3 =0
  APSD=0
  QueIdx=0: APAifsn=3,APCwmin=4,APCwmax=6, APTxop=0,APACM=0
  QueIdx=1: APAifsn=7,APCwmin=4,APCwmax=10, APTxop=0,APACM=0
  QueIdx=2: APAifsn=1,APCwmin=3,APCwmax=4, APTxop=94,APACM=0
```

```

QueIdx=3: APAifsn=1,APCwmin=2,APCwmax=3, APTxop=47,APACM=0
QueIdx=0: BSSAifsn=3,BSSCwmin=4,BSSCwmax=10, BSSTxop=0,BSSACM=0
QueIdx=1: BSSAifsn=7,BSSCwmin=4,BSSCwmax=10, BSSTxop=0,BSSACM=0
QueIdx=2: BSSAifsn=2,BSSCwmin=3,BSSCwmax=4, BSSTxop=94,BSSACM=0
QueIdx=3: BSSAifsn=2,BSSCwmin=2,BSSCwmax=3, BSSTxop=47,BSSACM=0
AckPolicy[0]=0: AckPolicy[1]=0,AckPolicy[2]=0,AckPolicy[3]=0

```

Telnet Command: **wl ht**

This command allows you to configure wireless settings.

wl ht bw *value*

wl ht gi *value*

wl ht badecline *value*

wl ht autoba *value*

wl ht rdg *value*

wl ht msdu *value*

wl ht txpower *value*

wl ht antenna *value*

wl ht greenfield *value*

Syntax Description

Parameter	Description
<i>wl ht bw value</i>	The value you can type is 0 (for BW_20) and 1 (for BW_40).
<i>wl ht gi value</i>	The value you can type is 0 (for GI_800) and 1 (for GI_4001)
<i>wl ht badecline value</i>	The value you can type is 0 (for disabling) and 1 (for enabling).
<i>wl ht autoba value</i>	The value you can type is 0 (for disabling) and 1 (for enabling).
<i>wl ht rdg value</i>	The value you can type is 0 (for disabling) and 1 (for enabling).
<i>wl ht msdu value</i>	The value you can type is 0 (for disabling) and 1 (for enabling).
<i>wl ht txpower value</i>	The value you can type ranges from 1 - 6 (level).
<i>wl ht antenna value</i>	The value you can type ranges from 0-3. 0: 2T3R 1: 2T2R 2: 1T2R 3: 1T1R
<i>wl ht greenfield value</i>	The value you can type is 0 (for mixed mode) and 1 (for green field).

Example

```

> wl ht bw value 1
BW=0
<Note> Please restart wireless after you set new parameters.
> wl restart
Wireless restart.....

```

Telnet Command: wl restart

This command allows you to restart wireless setting.

Example

```
> wl restart
Wireless restart.....
```

Telnet Command: wl wds

This command allows you to configure WDS settings.

Syntax

wl wds mode *[value]*

wl wds security *[value]*

wl wds ap *[value]*

wl wds hello *[value]*

wl wds status

wl wds show

wl wds mac *[value]*

wl wds flush

Syntax Description

Parameter	Description
<i>mode [value]</i>	It means to specify connection mode for WDS. [value]: Available settings are : d: Disable b: Bridge r: Repeater
<i>security [value]</i>	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>
<i>ap [value]</i>	It means to enable or disable the AP function. Value: 1 - enable the function. 0 - disable the function.
<i>hello [value]</i>	It means to send hello message to remote end (peer). Value: 1 - enable the function.

	0 - disable the function.
<i>status</i>	It means to display WDS link status for 2.4GHz connection.
<i>show</i>	It means to display current WDS settings.
<i>mac add [index addr]</i>	add <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 specifed or all MAC entries in Repeater/Bridge WDS MAC table. e.g, <i>wl dual wds mac enable 1</i>
<i>flush</i>	It means to reset all WDS setting.

Example

```
> wl wds status
Please enable WDS hello function first.

> wl wds hello 1
% <Note> Please restart router after you set the parameters.

> wl wds status
```

Telnet Command: wl btnctl

This command allows you to enable or disable wireless button control.

wl btnctl [*value*]

Syntax Description

Parameter	Description
<i>value</i>	0: disable 1: enable

Example

```
> wl btnctl 1
Enable wireless 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 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
<i>show</i>	Display current status for Band Steering function.
<i>enable</i> [1/0]	It means to enable wireless 2.4GHz AP client mode. 1 - enable 0 - disable
<i>chk_time</i> [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</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.

Example

```
> wl artfns enable 1
> wl artfns trg_num 3
> wl artfns show
airtime fairness: enable
trg_num: 3
>
```

Telnet Command: wl drayrs

This command allows the user to configure settings for Roaming for wireless clients.

Syntax

wl drayrs set <mode><rs_low><rs_low_security><delta>

wl drayrs restart

wl drayrs show

Syntax Description

Parameter	Description
<i>set</i> <mode> <rs_low> <rs_low_security><delta>	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.
<i>clear</i>	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 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 bw <0/ 1/ 2>
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
wl_dual config frag <value>
wl_dual config frag show
wl_dual config rts <value>
wl_dual config rts show
wl_dual config country <value>
wl_dual config txpower <value>
wl_dual config nss <value>

Syntax Description

Parameter	Description
<i>enable</i> <value>	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</i> <value>	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</i> <number>	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</i> <enable>	It means to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However,

	some original 11b wireless network devices only support long preamble. 0: disable to use long preamble. 1: enable to use long preamble.
<i>preamble show</i>	It means to display if preamble is enabled or not.
<i>bw <0/ 1/ 2></i>	It means to set channel bandwidth. 0: BW_20; 1:BW_20_40; 2:BW_20_40_80
<i>ssid <ssid_num enable ssid_name></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>ssid hide <ssid_num enable></i>	It means to hide the name of the SSID if required. <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.
<i>ssid show</i>	It means to display a table of SSID configuration.
<i>ratectl <ssid_num enable upload download></i>	It means to set the rate control for the specified SSID. <i>ssid_num</i>: Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. <i>enable</i>: It means to enable the function of the rate control for the specified SSID. 0: disable and 1:enable. <i>upload</i>: It means to configure the rate control for data upload. The unit is kbps. <i>download</i>: It means to configure the rate control for data download. The unit is kbps. (example: <i>wl dual config ratectl 1 1 25 25</i>)
<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>	It means to isolate the wireless connection from LAN. It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other. <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
<i>isolate member <ssid_num enable></i>	It means to isolate the wireless connection from Member. It can make the wireless clients (stations) with the same SSID not accessing for each other. <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.
<i>isolate vpn <ssid_num enable></i>	It means to isolate the wireless connection from VPN. <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.
<i>isolate show</i>	It means to display the status of wireless isolation.
<i>frag <value></i>	It means to set the fragment threshold. <i>value</i>: Enter a number (256 to 2346).
<i>frag show</i>	It means to display current value of fragment threshold.
<i>rts <value></i>	It means to set the RTS threshold. <i>value</i>: Enter a number (1 to 2347).
<i>rts show</i>	It means to display current value of RTS threshold.
<i>rate_alg<value></i>	It means to set the rate adaptation algorithm. <i>Value</i>: Enter 0 or 1. 0 - old algorithm; 1 - new algorithm.
<i>country <value></i>	It means to set the country code. Each country will be represented with two digits.

	value: Enter two capital letters (e.g., TW, UK, CN..)
<i>txpower <value></i>	It means to set TX power. Value: Enter a number (1 to 6).
<i>nss <value></i>	It means to set NSS. Value: Enter a number (0 to 4).

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> <SSID_NUMBER> <mode><key> <index>	<i>SSID_NUMBER</i> : Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. <i>mode</i> : Available settings are: disable: No security. wpa1x: WPA/802.1x Only wpa21x: WPA2/802.1x Only wpamix1x: Mixed (WPA+WPA2/802.1x only) wep1x: WEP/802.1x Only

	wpapsk: WPA/PSK wpa2psk: WPA2/PSK wpamixpsk: Mixed (WPA+WPA2)/PSK wep: WEP <i>key, index:</i> Moreover, you have to add keys for <i>wpapsk</i> , <i>wpa2psk</i> , <i>wpamixpsk</i> and <i>wep</i> , and specify index number of schedule profiles to be followed by the wireless connection. WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8-63 ASCII text string or 64 Hexadecimal digit format.
<i>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 show
wl_dual stalist num
wl_dual stalist neighbor
wl_dual stalist validtime <time>
wl_dual stalist maxnum <num>
```

Syntax Description

Parameter	Description
<i>validtime</i> <time>	Set the valid time of the neighbor station list. <time> - 0 to 300000.
<i>maxnum</i> <num>	Set the maximum number of neighbor station list. <value> - 10 to 512

Example

```
> wl_dual stalist neighbor
5G Wireless Neighbor Station List :
MAC Address      | Vendor Name      | RSSI (%) | RSSI (dbm) | SSID | time (ms)
F2:C6:DB:2B:25:E0 |                  | 24       | -84        | none | 20
D6:FC:CB:DC:C1:E8 |                  | 24       | -84        | none | 0
```

80:00:0B:04:CE:5A	Intel	11	-88	none	7230880
00:1D:AA:80:FE:D6	DrayTek	15	-87	none	7210610
A6:99:E2:27:7F:A0		50	-76	none	20
0A:32:AB:06:88:2C		40	-79	none	0
F8:63:3F:56:06:C6		15	-87	none	881950
1E:B9:C9:03:04:52		87	-62	none	20
8E:DF:E3:0A:F4:02		3	-92	none	20
E2:41:8F:4B:1A:11		50	-76	none	20
BA:96:81:7D:11:BD		24	-84	none	10
7C:2A:31:10:1B:11		2	-93	none	0

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
<i>mode <value></i>	It means to specify connection mode for WDS. [value]: Available settings are : d: Disable r: Repeater
<i>security <value></i>	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., <i>wl_dual wds security disable</i> <i>wl_dual wds security wep 12345</i> <i>wl_dual wds security wpa2psk 12345678</i>
<i>ap <value></i>	It means to enable or disable the AP function. Value: 1 - enable the function. 0 - disable the function.
<i>hello <value></i>	It means to send hello message to remote end (peer).

	Value: 1 - enable the function. 0 - disable the function.
<i>status</i>	It means to display WDS link status for 5GHz 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 specied or all MAC entries in Repeater/Bridge WDS MAC table. e.g, <i>wl_dual wds mac enable 1</i>
<i>flush</i>	It means to reset all WDS setting.

Example

```
> wl_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 r
> wl_dual wds security wep
>
> wl_dual wds show
5G Wireless WDS Setting

Mode : Repeater
Security : WEP
AP Function : Enable
Send Hello Function : Enable

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
<i>enable <value></i>	It means to enable WPS. 1 - enable 0 - disable

<i>pbw</i>	It means to start WPS by pressing the WLAN ON/OFF WPS button on Vigor router.
<i>pin <code></i>	It means to start WPS by using client PIN code. [code]: Client PIN code (digit number).
<i>show</i>	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 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 <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.
<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</i> <mode> <rs_low> <rs_low_security> <delta>	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>	Dispaly 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 Minimun RSSI
% rs_low      : -68
% rs_low_secure : -66
% delta      : 2
```

Telnet Command: wol

This command allows you to set the white list of WAN IP addresses/Subnets, that the magic packet from these IP addresses/Subnets will be eligible to pass through NAT and wake up the LAN client. You also need to set NAT rule for LAN client.

Syntax

wol up [MAC Address]

wol fromWan [on/ off/ any]

wol fromWan_Setting [idx][ip address][mask]

Syntax Description

Parameter	Description
MAC Address	It means the MAC address of the host.
on/ off/ any	It means to enable or disable the function of WOL from WAN. on: enable off: disable

	any: It means any source IP address can pass through NAT and wake up the LAN client. This command will allow the user to choose whether WoL packets can be passed from the Internet to the LAN network from a specific WAN interface.
<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 *[-a/-b/-c/-d/-e/-l/-o/-q/-r/-s/-u]*

user edit *[PROFILE_IDX] [-a/-d/-e/-f/-i/-o/-m/-n/-p/-q/-r/-s/-t/-u/-v/-w/-x/-A/-H/-T/-P/-I/-L/-D]*

user account *[USER_NAME] [-t/-d/-q/-r/-w]*

user setdefault

Syntax Description

Parameter	Description
<i>set</i>	It means to configure general setup for the user management.
<i>edit</i>	It means to modify the selected user profile.
<i>account</i>	It means to set time and data quota for specified user account.
User Set	
<i>-a[Profile idx][User name][IP_Address]</i>	It means to pass an IP Address. <i>Profile idx</i>- Enter the index number of the selected profile. <i>User name</i>- Enter the user name that you want it to pass. <i>IP_Address</i>- Enter the IP address that you want it to pass.
<i>-c[user name]</i> <i>-c all</i>	Clear the user record. <i>user name</i> –Enter the user name that you want to get clear corresponding record. <i>all</i> –all of the records will be removed.
<i>-d</i>	Enable the User management in Rule-Based mode.
<i>-e</i>	Enable the User management in User-Based mode.
<i>-l all</i> <i>-l userl</i> <i>-l ip</i>	Show online user. <i>all</i> –all of the users will be displayed on the screen. <i>user name</i> –Enter the user name that you want to view on

	the screen. <i>ip</i> –Enter the IP address that you want to view on the screen.
<i>-o</i>	It means to show user account information. e.g., <i>-o</i>
<i>-q</i>	It means to trigger the alert tool to do authentication.
<i>-r [user name all]</i>	Remove the user record. <i>user name</i> –Enter the name of the user profile. <i>all</i> –all of the user profile settings will be removed.
<i>-s <0/ 1></i>	It means to set login service. 0:HTTPS 1:HTTP e.g., <i>-s 1</i>
<i>-b user [user name]</i> <i>-b ip [ip address]</i>	Block specifies user or IP address. <i>user name</i> –Enter the user name that you want to block. <i>ip address</i> –Enter the IP address that you want to block.
<i>-u user [user name]</i> <i>-u ip [ip address]</i>	Unblock specifies user or IP address. <i>user name</i> –Enter the user name that you want to unblock. <i>ip address</i> –Enter the IP address that you want to unblock.
User Edit	
<i>PROFILE_IDX</i>	Enter the index number of the profile that you want to edit.
<i>-a <0/ 1></i>	It means to enable /disable the internal RADIUS server for user profile. 0:Disable 1:Enable
<i>-d</i>	Disable User profile function.
<i>-e</i>	Enable User profile function.
<i>-f <0/ 1></i>	It means to enable /disable the Local 802.1x service for user profile. 0:Disable 1:Enable
<i>-i <0-255></i>	It means to set idle time. e.g., <i>-i 60</i>
<i>-o <0-65535></i>	It means to set auto-logout (from 0 to 65535, 0 means unlimited).
<i>-m <0-2000></i>	It means to set the maximum (from 0 to 2000) login user number. e.g., <i>-m 200</i>
<i>-n <param></i>	It means to set a user name for a profile. Param: Enter a string, e.g., <i>-n fortest</i> .
<i>-p <param></i>	It means to configure user password. Param: Enter a string, e.g., <i>-p 60fortest</i> .
<i>-q <param></i>	It means to set time quota (0-65535) of the user profile. Param: Enter a value, e.g., <i>-q 200</i> .
<i>-r <param></i>	It means to set data quota.

	Param: Enter a value, e.g., <i>-r 1000</i> .
<i>-s <sch_idx1, sch_idx2, sch_idx3, sch_idx4></i>	It means to specify schedule index number(from 1 to 15) for the profile. Four index number can be set at one time. e.g., <i>-s [1,2,3,4]</i>
<i>-t <0/ 1></i>	It means to enable /disable time quota limitation for user profile 0:Disable 1:Enable
<i>-u <0/ 1></i>	It means to enable /disable data quota limitation for user profile 0:Disable 1:Enable
<i>-v</i>	It means to view user profile(s).
<i>-w <MB/ GB></i>	It means to specify the data quota unit (MB/GB). e.g., <i>-w MB</i>
<i>-x <0/ 1/ 2/ 3></i>	It means to set external server authentication. 0: None 1: LDAP 2: Radius 3: TACAS e.g., <i>-x 2</i>
<i>-l <0/ 1/ 2/ 3></i>	It means to set log type. 0: None 1: Login 2: Event 3: All e.g., <i>-x 2</i>
<i>-P <0/ 1></i>	It means to pop the browser tracking window. 0:Disable 1:Enable
<i>-T <0/ 1></i>	It means to set user authentication by Telnet. 0:Disable 1:Enable
<i>-H <0/ 1></i>	It means to set user authentication by WEB. 0:Disable 1:Enable
<i>-A <0/ 1></i>	It means to set user authentication by Alert Tool. 0:Disable 1:Enable
<i>-O <0/ 1></i>	It means to reset the quota automatically. 0:Disable 1:Enable
<i>-Q <param></i>	It means to set the default time quota. param: Enter a number (1 to 65535).
<i>-R <param></i>	It means to set the default data quota.

	param: Enter a number (1 to 65535).
<i>-M <param></i>	It means to set the default quota type. 0: when login permission schedule expired. 1: at the start time of schedule.
<i>I <param></i>	It means to specify the default quota schedule index to perform the job at the start time.
<i>-S</i>	It means to display the reset default quota type and the schedule index.
User Account	
<i>USER_NAME</i>	It means to give a name of the user account.
<i>-d <0/ 1></i>	It means to enable /disable data quota limitation for user account. 0:Disable 1:Enable
<i>-q <1-65535></i>	It means to set account time quota (minutes). e.g., <i>-q 200</i>
<i>-r <1-65535></i>	It means to set account data quota (MB). e.g., <i>-r 1000</i>
<i>-t <0/ 1></i>	It means to enable /disable time quota limitation for user account. 0:Disable 1:Enable
<i>-w <MB/ GB></i>	It means to set data quota unit (MB/GB).
User setdefault	All user profiles will be set to factory default settings.

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

Syntax Description

Parameter	Description
<i>view</i>	It means to display current status of APP QoS.
<i>enable</i> [0/ 1]	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.

-v	It means to view the content of all traceable APs. Use “appqos traceable -v” to display all of the traceable APS with speficed index number. Use “appqos untraceable -v” to display all of the untraceable APS with speficed index number.
-e	It menas to enable QoS for application(s) and assign QoS class.
AP_INDEX	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 traceabel APPs. Index number: 0-49, 55-59, 61, 67, 69, and 70-123 are used for 125 untraceable AP.
CLASS	Specifies the QoS class of the application, from 1 to 4 1:Class 1, 2:Class 2, 3:Class 3, 4:Other Class
-d	It means to disable QoS for application(s).

Example

```
> appqos enable 1

APP QoS set to Enable.
> appqos traceable -e 68 2

TELNET: ENABLED, QoS Class 2.
```

Telnet Command: nand bad /nand usage

“NAND usage” is used to display NAND Flash usage; “nand bad” is used to display NAND Flash bad blocks.

nand bad

nand usage

Example

```
>nand usage
Show NAND Flash Usage:
Partition      Total          Used           Available      Use%
cfg            4194304        7920           4186384        0%
bin_web        33554432       11869493       21684939       35%
cfg-bak        4194304        7920           4186384        0%
bin_web-bak    33554432       11869493       21684939       35%
> nand bad
Show NAND Flash Bad Blocks:
Block  Address      Partition
1020   0x07f80000   unused
1021   0x07fa0000   unused
1022   0x07fc0000   unused
1023   0x07fe0000   unused
```

Telnet Command: apm enable/disable/show /clear/discover/query

The apm command(s) is use to display, remove, discover or query the information of VigorAP registered to Vigor2765.

Syntax

apm enable

apm disable

apm show

apm clear

apm discover

apm query

Syntax Description

Parameter	Description
<i>enable</i>	It means to enable APM function.
<i>disable</i>	It means to disable APM function.
<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 Vigor2765. Information related to the registered AP will be send back to Vigor2765 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 Vigor2765.
<i>clear</i>	It means to remove the information related to VigorAP registered Vigor2765.

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 1 - enable disassociation, 0 - disable disassociation. [8] - The eighth number means to enable or disable disassociation by signal strength. Type 1 - enable disassociation, 0 - disable disassociation. [9] - The ninth number means to determine the unit of traffic limit (for upload) 1 - Mbps 0 - kbps [10] - The tenth number means to determine the unit of traffic limit (for download) 1 - Mbps 0 - kbps

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: fw_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

fw_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.
-t <i>n</i>	Set the backup time. n : 1 ~ 168 hours
-m <i>n</i>	Set the firmware backup mode. 1: Backup after timeout. 0: Backup after upgrade.
-b	Backup the firmware manually and immediately.
-r	Set the firmware recovery mode. 1: the firmware will be recovered when the system crash. 0: No recovery.

Example

```
> fw_backupmode -b  
Do Firmware backup now!!!.
```

Telnet Command: service

This command is used to display information about Myvigor service. In addition, it allows to transfer MyVigor service from the original account to other account.

Syntax

service -s

service -r

service -l <account><password>

service -i <new_owner><new_owner_email>

service -t <yes>/<no>

service -c

Syntax Description

Parameter	Description
-s	Display the service status.
-r	Refresh the service status
-l <account><password>	Login to MyVigor server. Enter the account and password registered to MyVigor server account - Enter the name of the account. Password - Enter the password of the account.
-i <new_owner> <new_owner_email>	Enter the name and the e-mail address of the new owner for service transfer. New_owner - Enter the account name of the new owner. New_owner_email - Enter the e-mail address of the new owner.
-t <yes>/<no>	Transfer this Vigor device to a new owner.
-c	Clear current owner's account information.

Example

```
> service  
> service -l carrieni ttt0016ttt5  
Login Account:carrieni, Pw:ttt0016ttt5  
Login Success! Please check Service Status again!  
> service -s  
Show service status.  
Now state is [SS_STATE_REG_ACC_VALID]  
Service Status:  
Model Name : Vigor2765 Series  
Serial Number: 2019053108580701  
MAC Address : 00:1D:AA:73:4A:78  
Owner Account: carrieni  
E-mail : ca*****i@draytek.com  
  
Device service support status:  
Service WCF, ID = [1]  
Service Provider [Cyren]  
Licese Start_date [2019-09-26]  
Licese Exp_date [2019-10-26]  
  
Service APPE, ID=[4]  
Service Provider [Not Activated]  
Licese Start_date []  
Licese Exp_date []
```

```
Service DDNS, ID=[6]
Service Provider [Not Activated]
Licese Start_date []
Licese Exp_date []
```

Telnet Command: dmn

This command is used to set configuration related to mesh network, status display or trigger the mesh actions.

Syntax

```
dmn enable <1/0>
dmn reset_group
dmn loglevel <1/0>
dmn search <start/show>
dmn status
dmn mynode
dmn discover <start/show>
dmn acs
dmn table <0/1/2>
dmn set <rssi [1~100]/ timeout>
dmn disconnect
dmn auto_reselect
dmn refresh <index>
```

Syntax Description

Parameter	Description
<i>dmn enable <1/0></i>	Enable or disable the mesh function. 1 - Enable. 0 - Disable.
<i>dmn reset_group</i>	Reset the group list and group key.
<i>dmn loglevel <1/0></i>	Set the mesh log level. 1 - detailed information. 0 - basic information.
<i>dmn search start</i> <i>dmn search show</i>	Search for available mesh nodes in the environment to join the Mesh Network. start - Begin to search. show - Display the searching result.
<i>dmn status</i>	Display the group status.
<i>dmn mynode</i>	Display the local status of this device. For example, DrayTek> dmn mynode % [dmn_cmd] my node: Preferred Wireless Uplink : Auto Operation Mode : MeshNode(Wired) Root MAC : 00:00:00:00:00:00 Hop : 0 Uplink : none Downlink (0) : Model : Vigor2765

	Device Name : DrayTek MAC : 00:1D:AA:70:33:E0 State : Mesh Node (Wired Uplink) - Isolate Status : New
<i>dmn discover start</i> <i>dmn discover show</i>	Search for mesh devices (including mesh root and mesh node) around this router. start - Begin to search. show - Display the searching result.
<i>acs</i>	Obtain information by sending requests to Mesh auto-configuration server. Available sub-commands include: (g)et - get mynode and station list (s)et - set all parameter prin(t) - print all list (c)lear - clear all method (p)ause - pause acs (r)esume - resume acs st(a)tus - acs group status sta(l)ist - print all node station list (u)p_sta_status - print update station list status r(e)set - reset dmn acs
<i>table <0/ 1/ 2></i>	Display a device table of the mesh network. 0 - Originator table 1 - Local client table 2 - Remote client table
<i>set rssi <value></i> <i>set timeout</i> <i>set show</i>	When the RSSI value of the mesh node is less than the threshold, the network connection of the mesh node will be not allowed. Or, a mesh node will be disconnected if exceeding the timeout. rssi <value> - Set the threshold (1 to 100) value of the RSSI. timeout - Set the timeout level (unit is "second"). Show - Display current threshold (%) and timeout.
<i>disconnect <mac></i>	Disconnect an online wireless mesh node. In general, the mesh node will reconnect to Mesh Network later. <mac> - Enter the MAC address of the mesh node in a Mesh Group. (Ex. dmn disconnect 00:1d:aa:22:33:44)
<i>auto_reselect</i>	Enable (1) or disable (0) the auto reselection function. If enabled, the Mesh Root starts a Mesh Reselect automatically after the Mesh Network changed.
<i>reselect</i>	Start a Mesh Reselect immediately. An online Wireless Mesh Node may reconnect to a better Wireless uplink.

Example

```

> dmn refresh 2
% Delete [2] node and let it recover automatically
> dmn set rssi 50
> dmn

```