

DrayTek

Vigor2133 Series Gigabit Broadband Router

Your reliable networking solutions partner



User's Guide

V1.2

Vigor2133 Series Gigabit Broadband Router

User's Guide

Version: 1.2

Firmware Version: V3.8.8

(For future update, please visit DrayTek web site)

Date: April 24, 2018

Copyrights

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

Trademarks

The following trademarks are used in this document:

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

Safety Instructions

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

Warranty

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

Be a Registered Owner

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

Firmware & Tools Updates

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

More update, please visit www.draytek.com.

Table of Contents

Part I Installation	i
I-1 Introduction	1
I-1-1 Indicators and Connectors	2
I-2 Hardware Installation	4
I-2-1 Installing Vigor Router	4
I-2-2 Wall-Mounted Installation	5
I-2-3 Installing USB Printer to Vigor Router	6
I-3 Accessing Web Page	13
I-4 Changing Password	15
I-5 Dashboard	16
I-5-1 Virtual Panel	17
I-5-2 Name with a Link	17
I-5-3 Quick Access for Common Used Menu	18
I-5-4 GUI Map	19
I-5-5 Web Console	20
I-5-6 Config Backup	20
I-5-7 Logout	21
I-5-8 Online Status	21
I-5-8-1 Physical Connection	21
I-5-8-2 Virtual WAN	23
I-6 Quick Start Wizard	24
I-7 Service Activation Wizard	33
I-8 Registering Vigor Router	35
Part II Connectivity	37
II-1 WAN	38
Web User Interface	39
II-1-1 General Setup	39
II-1-1-1 WAN1	39
II-1-1-2 WAN3 (USB)	42
II-1-2 Internet Access	43
II-1-2-1 Details Page for PPPoE	44
II-1-2-2 Details Page for Static or Dynamic IP	47
II-1-2-3 Details Page for PPTP/L2TP	50
II-1-2-4 Details Page for IPv6 - Offline	52
II-1-2-5 Details Page for IPv6 - PPP	52
II-1-2-6 Details Page for IPv6 - TSPC	53
II-1-2-7 Details Page for IPv6 - AICCU	55
II-1-2-8 Details Page for IPv6 - DHCPv6 Client	56
II-1-2-9 Details Page for IPv6 - Static IPv6	58
II-1-2-10 Details Page for IPv6 - 6in4 Static Tunnel	59
II-1-2-11 Details Page for IPv6 - 6rd	61
II-1-3 Multi-VLAN	63
II-1-4 WAN Budget	67

<i>II-1-4-1 General Setup</i>	67
<i>II-1-4-2 Status</i>	70
Application Notes	71
<i>A-1 How to configure IPv6 on WAN interface?</i>	71
II-2 LAN	76
Web User Interface	78
II-2-1 General Setup	78
<i>II-2-1-1 Details Page for LAN1 - Ethernet TCP/IP and DHCP Setup</i>	81
<i>II-2-1-2 Details Page for LAN2 ~ LAN4</i>	83
<i>II-2-1-3 Details Page for IP Routed Subnet</i>	85
<i>II-2-1-4 Details Page for LAN IPv6 Setup</i>	86
<i>II-2-1-5 Advanced DHCP Options</i>	90
II-2-2 VLAN	92
II-2-3 Bind IP to MAC	95
II-2-4 LAN Port Mirror	99
II-2-5 Wired 802.1x	100
II-3 Hardware Acceleration	101
II-4 NAT	103
Web User Interface	104
II-4-1 Port Redirection	104
II-4-2 DMZ Host	108
II-4-3 Open Ports	111
II-4-4 Port Triggering	114
II-4-5 ALG	116
II-5 Applications	117
Web User Interface	119
II-5-1 Dynamic DNS	119
II-5-2 LAN DNS / DNS Forwarding	123
II-5-3 DNS Security	126
<i>II-5-3-1 General Setup</i>	126
<i>II-5-3-2 Domain Diagnose</i>	126
II-5-4 Schedule	128
II-5-5 RADIUS	131
II-5-6 UPnP	132
II-5-7 IGMP	133
<i>II-5-7-1 General Setting</i>	133
<i>II-5-7-1 Working Group</i>	134
II-5-8 Wake on LAN	135
II-5-9 SMS / Mail Alert Service	136
<i>II-5-9-1 SMS Alert</i>	136
<i>II-5-9-2 Mail Alert</i>	137
II-5-10 Bonjour	138
Application Notes	141
<i>A-1 How to use DrayDDNS?</i>	141
<i>A-2 How to Configure Customized DDNS?</i>	146

II-6 Routing.....	150
Web User Interface	151
II-6-1 Static Route	151
II-6-2 Route Policy	155
II-6-2-1 General Setup	155
II-6-2-2 Diagnose	159
Application Notes	162
A-1 How to set up Address Mapping with Route Policy?	162
Part III Wireless LAN.....	165
III-1 Wireless LAN (2.4 GHz/5 GHz)	166
Web User Interface	170
III-1-1 Wireless Wizard.....	170
III-1-2 General Setup	174
III-1-3 Security.....	176
III-1-4 Access Control	178
III-1-5 WPS.....	179
III-1-6 WDS	181
III-1-7 Advanced Setting	184
III-1-8 Station Control.....	187
III-1-9 AP Discovery	187
III-1-10 Bandwidth Management.....	189
III-1-11 Airtime Fairness.....	190
III-1-12 Band Steering.....	192
III-1-13 Roaming	196
III-1-14 Station List.....	197
Part IV VPN	199
IV-1 VPN and Remote Access	200
Web User Interface	201
IV-1-1 VPN Client Wizard	201
IV-1-2 VPN Server Wizard	207
IV-1-3 Remote Access Control	211
IV-1-4 PPP General Setup.....	212
IV-1-5 IPsec General Setup	214
IV-1-6 IPsec Peer Identity	215
IV-1-7 Remote Dial-in User	217
IV-1-8 LAN to LAN	220
IV-1-9 Connection Management.....	230
Application Notes	231
A-1 How to Build a LAN-to-LAN VPN Between Remote Office and Headquarter via IPsec Tunnel (Main Mode)	231
IV-2 SSL VPN	236

Web User Interface	237
IV-2-1 General Setup	237
IV-2-2 User Account.....	238
IV-2-3 Online User Status	242
IV-3 Certificate Management.....	243
Web User Interface	244
IV-3-1 Local Certificate	244
IV-3-2 Trusted CA Certificate.....	248
IV-3-3 Certificate Backup.....	250
Part V Security	251
V-1 Firewall.....	252
Web User Interface	254
V-1-1 General Setup	254
V-1-2 Filter Setup.....	259
V-1-3 DoS Defense.....	270
V-1-4 Diagnose	274
Application Notes	277
<i>A-1 How to Configure Certain Computers Accessing to Internet</i>	<i>277</i>
V-2 Central Security Management (CSM).....	281
Web User Interface	282
V-2-1 APP Enforcement Profile	282
V-2-2 URL Content Filter Profile	286
V-2-3 Web Content Filter Profile.....	290
V-2-4 DNS Filter Profile	294
Application Notes	296
<i>A-1 How to Create an Account for MyVigor</i>	<i>296</i>
<i>A-2 How to Block Facebook Service Accessed by the Users via Web Content Filter / URL Content Filter</i>	<i>304</i>
Part VI Management	311
VI-1 System Maintenance	312
Web User Interface	313
VI-1-1 System Status.....	313
VI-1-2 TR-069	315
VI-1-3 Administrator Password	318
VI-1-4 User Password.....	320
VI-1-5 Login Page Greeting	323
VI-1-6 Configuration Backup.....	325
VI-1-7 Syslog/Mail Alert	329
VI-1-8 Time and Date.....	332
VI-1-9 SNMP	333
VI-1-10 Management	335

VI-1-11 Panel Control	339
VI-1-12 Self-Signed Certificate	343
VI-1-13 Reboot System.....	345
VI-1-14 Firmware Upgrade	346
VI-1-15 Activation.....	347
VI-2 Bandwidth Management.....	349
Web User Interface	351
VI-2-1 Sessions Limit.....	351
VI-2-2 Bandwidth Limit.....	353
VI-2-3 Quality of Service.....	355
VI-2-4 APP QoS.....	362
Application Notes	364
<i>A-1 How to Optimize the Bandwidth through QoS Technology</i>	<i>364</i>
VI-3 Hotspot Web Portal.....	368
Web User Interface	369
VI-3-1 Profile Setup.....	369
<i>VI-4-1-1 Login Modes</i>	<i>369</i>
<i>VI-4-1-2 Steps for Configuring a Web Portal Profile.....</i>	<i>372</i>
Application Notes	384
<i>A-1 How to create Facebook APP for Web Portal Authentication?</i>	<i>384</i>
<i>A-2 How to create Google APP for Web Portal Authentication?.....</i>	<i>390</i>
VI-4 Central Management (AP).....	392
Web User Interface	393
VI-4-1 Status	393
VI-4-2 WLAN Profile.....	395
VI-4-3 AP Maintenance.....	400
VI-4-4 Traffic Graph	401
VI-4-5 Load Balance	402
VI-4-6 Function Support List	403
VI-5 Central Management (External Devices)	404
VI-5-1 All Devices	404
Part VII Others	407
VII-1 Objects Settings.....	408
Web User Interface	409
VII-1-1 IP Object	409
VII-1-2 IP Group.....	413
VII-1-3 IPv6 Object.....	414
VII-1-4 IPv6 Group	416
VII-1-5 Service Type Object.....	417
VII-1-6 Service Type Group	419
VII-1-7 Keyword Object.....	421

VII-1-8 Keyword Group	423
VII-1-9 File Extension Object	424
VII-1-10 SMS/Mail Service Object	426
VII-1-11 Notification Object	431
VII-1-12 String Object	433
Application Notes	434
<i>A-1 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection</i>	434
VII-2 USB Application	438
Web User Interface	439
VII-2-1 USB General Settings	439
VII-2-2 USB User Management	440
VII-2-3 File Explorer	442
VII-2-4 USB Device Status.....	443
VII-2-5 Temperature Sensor	444
VII-2-6 Modem Support List.....	446
VII-2-7 SMB Client Support List.....	447
Application Notes	448
<i>A-1 How can I get the files from USB storage device connecting to Vigor router? ...</i>	448

Part VIII Troubleshooting451

VIII-1 Diagnostics	452
Web User Interface	453
VIII-1-1 Dial-out Triggering.....	453
VIII-1-2 Routing Table.....	454
VIII-1-3 ARP Cache Table	455
VIII-1-4 IPv6 Neighbour Table	456
VIII-1-5 DHCP Table	457
VIII-1-6 NAT Sessions Table	458
VIII-1-7 DNS Cache Table	459
VIII-1-8 Ping Diagnosis	460
VIII-1-9 Data Flow Monitor	461
VIII-1-10 Traffic Graph	463
VIII-1-11 Trace Route	464
VIII-1-12 Syslog Explorer	465
VIII-1-13 IPv6 TSPC Status	466
VIII-1-14 DoS Flood Table	467
VIII-1-15 Route Policy Diagnosis.....	469
VIII-2 Checking If the Hardware Status Is OK or Not.....	471
VIII-3 Checking If the Network Connection Settings on Your Computer Is OK or Not.....	472
VIII-4 Pinging the Router from Your Computer	475
VIII-5 Checking If the ISP Settings are OK or Not	477

VIII-6 Backing to Factory Default Setting If Necessary	478
VIII-7 Contacting DrayTek	479
Appendix I: VLAN Applications on Vigor Router	480
Part IX Telnet Commands.....	489
Accessing Telnet of Vigor2133	490
Index	688

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.

Vigor2133 series integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

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

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

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

With the 6-port Gigabit switch on the LAN side provides extremely high speed connectivity for the highest speed local data transfer of any server or local PCs. The tagged VLANs (IEEE802.1Q) can mark data with a VLAN identifier. This identifier can be carried through an onward Ethernet switch to specific ports. The specific VLAN clients can also pick up this identifier as it is just passed to the LAN. You can set the priorities for LAN-side QoS. You can assign each of VLANs to each of the different IP subnets that the router may also be operating, to provide even more isolation.








On the Wireless-equipped models each of the wireless SSIDs can also be grouped within one of the VLANs.

Vigor2133 series provides two-level management to simplify the configuration of network connection. The user mode allows user accessing into WEB interface via simple configuration. However, if users want to have advanced configurations, they can access into WEB interface through admin mode.

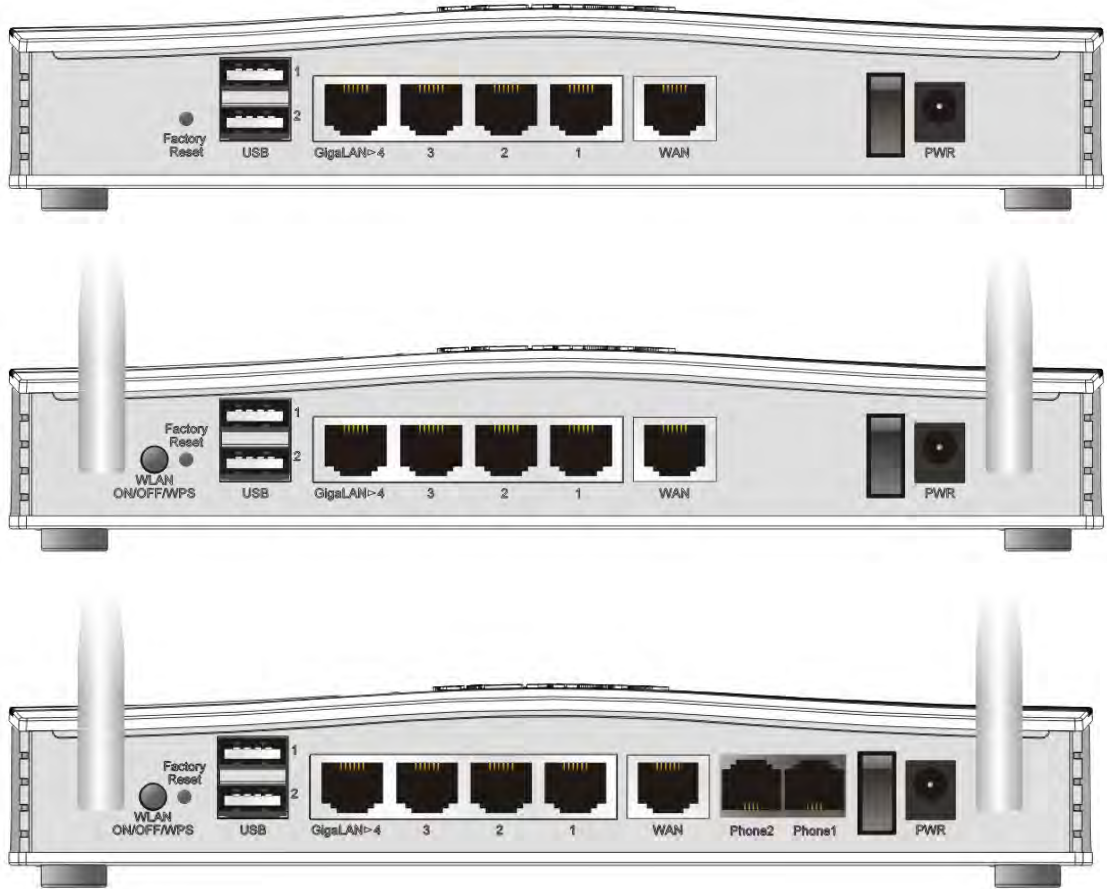
I-1-1 Indicators and Connectors

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



LED	Status	Explanation
 (Activity)	Blinking	The router is powered on and running normally.
	Blinking	When ACT and WLAN LEDs blink quickly and simultaneously is enabled and the system waits for wireless station of connection.
	Off	The router is powered off.
	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.
 USB	On	A USB device is connected and active.
	Blinking	The data is transmitting.
 WLAN	On	Wireless access point is ready.
	Blinking	Ethernet packets are transmitting over wireless LAN.
	Blinking	When ACT and WLAN LEDs blink quickly and simultaneously is enabled and the system waits for wireless station of connection.
	Off	The WLAN function is inactive.
 WAN	On	Internet connection is ready.
	Blinking	The data is transmitting.
	Off	Internet connection is not ready.
	On	The WAN port is connected with Ethernet cable.
	Blinking	The data is transmitting through WAN port.
	Off	The WAN port is disconnected.
	On	The LAN port is connected.
	Blinking	The data is transmitting.
	Off	The LAN port is disconnected.

LAN1/2/3/4



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

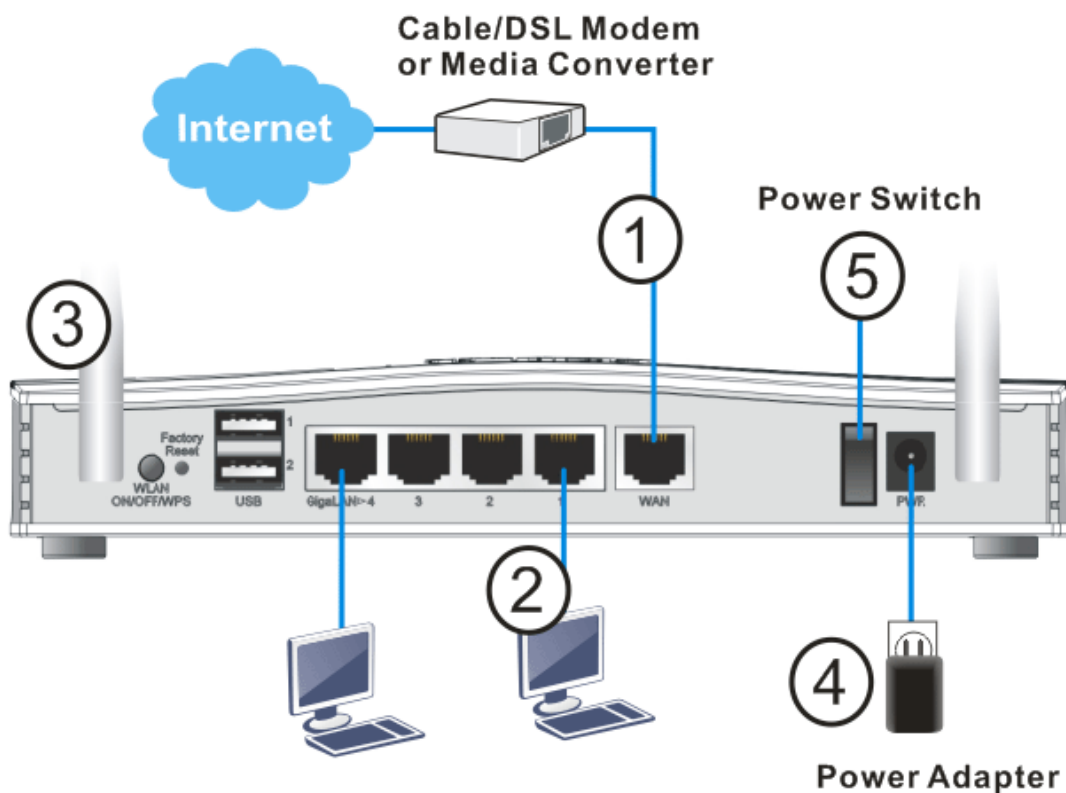
I-2 Hardware Installation

I-2-1 Installing Vigor Router

Before starting to configure the router, you have to connect your devices correctly. In this section, Vigor2133n is taken as an example.

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

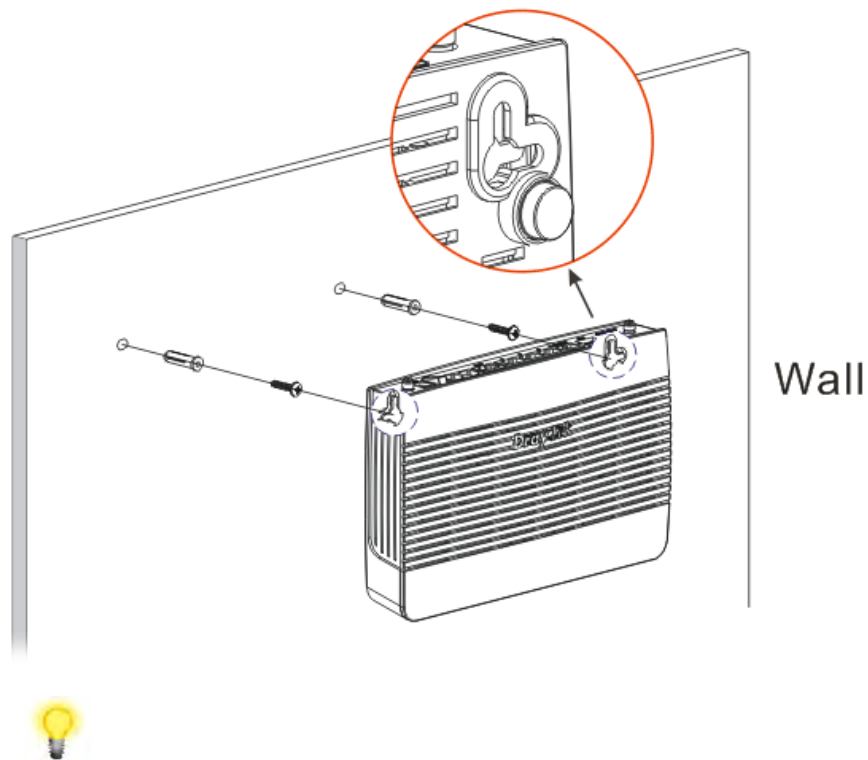
(For the hardware connection, we take “n” model as an example.)



I-2-2 Wall-Mounted Installation

Vigor2133 has keyhole type mounting slots on the underside.

1. A template is provided on the Vigor2133 packaging box to enable you to space the screws correctly on the wall.
2. Place the template on the wall and drill the holes according to the recommended instruction.
3. Fit screws into the wall using the appropriate type of wall plug.



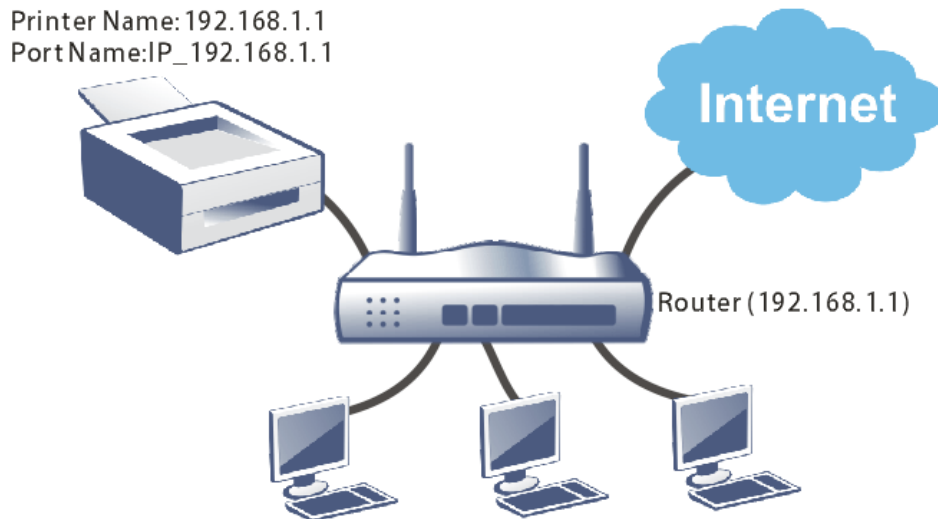
 Note

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

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

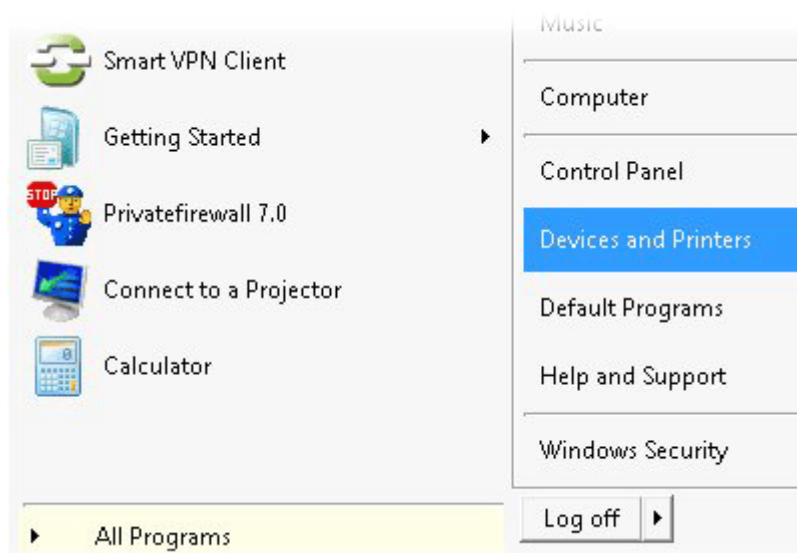
I-2-3 Installing USB Printer to Vigor Router

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

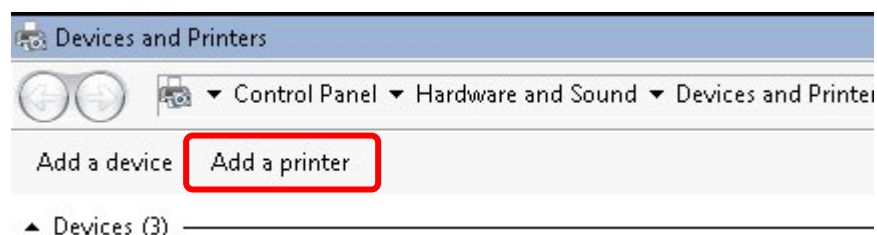


Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

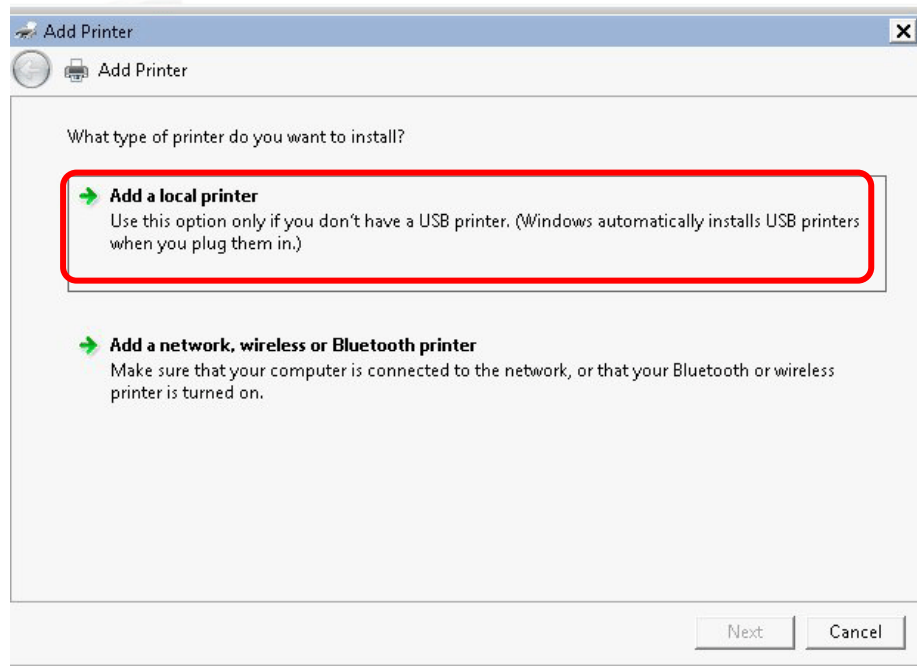
1. Connect the printer with the router through USB/parallel port.
2. Open All Programs>>Getting Started>>Devices and Printers.



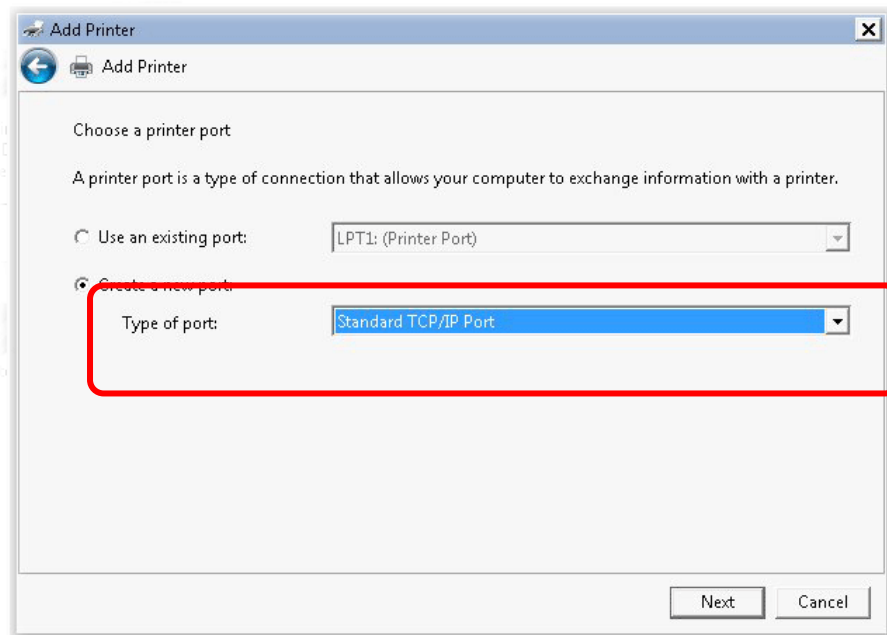
3. Click Add a printer.



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



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



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

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

- Device type: TCP/IP Device
- Hostname or IP address: 192.168.1.1
- Port name: 192.168.1.1

The checkbox 'Query the printer and automatically select the driver to use' is unchecked. The 'Next' and 'Cancel' buttons are located at the bottom right of the dialog.

7. Click Standard and choose Generic Network Card.

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

Additional port information required

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

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

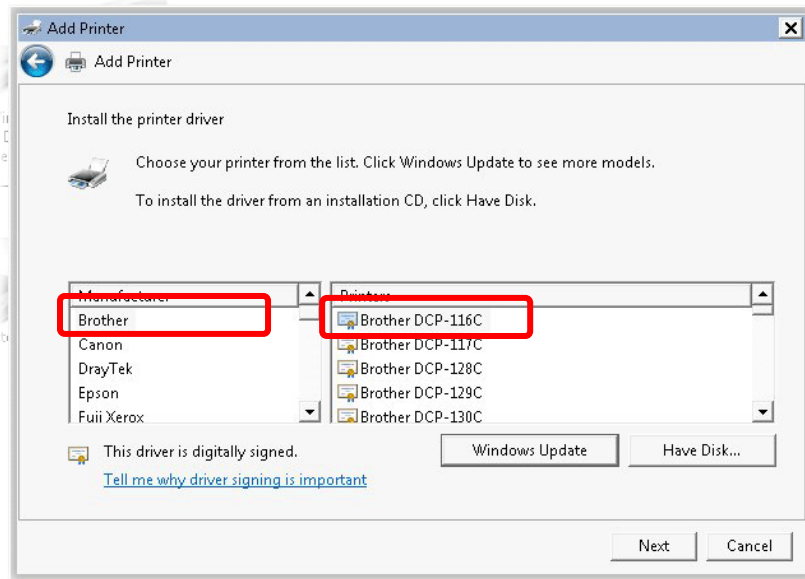
If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.

Device Type

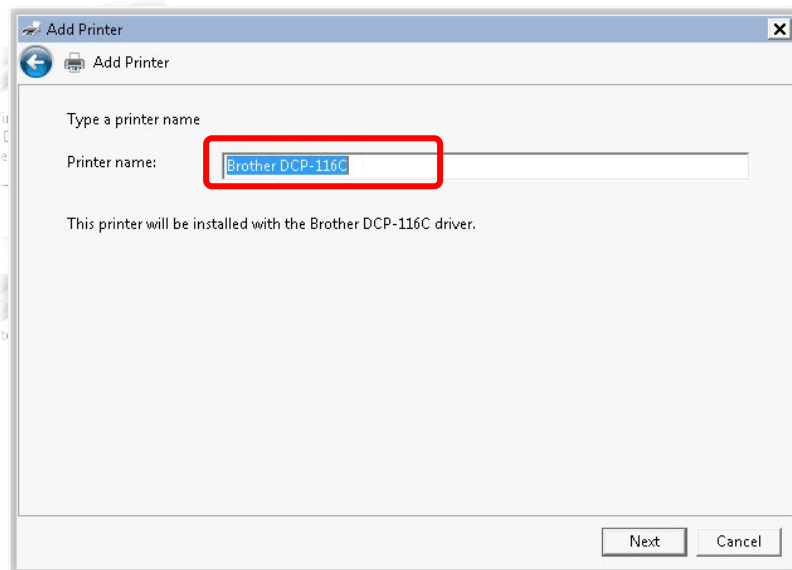
- Standard: Generic Network Card
- Custom: Settings...

The 'Standard' radio button and the 'Generic Network Card' dropdown menu are highlighted with a red box. The 'Next' and 'Cancel' buttons are at the bottom right.

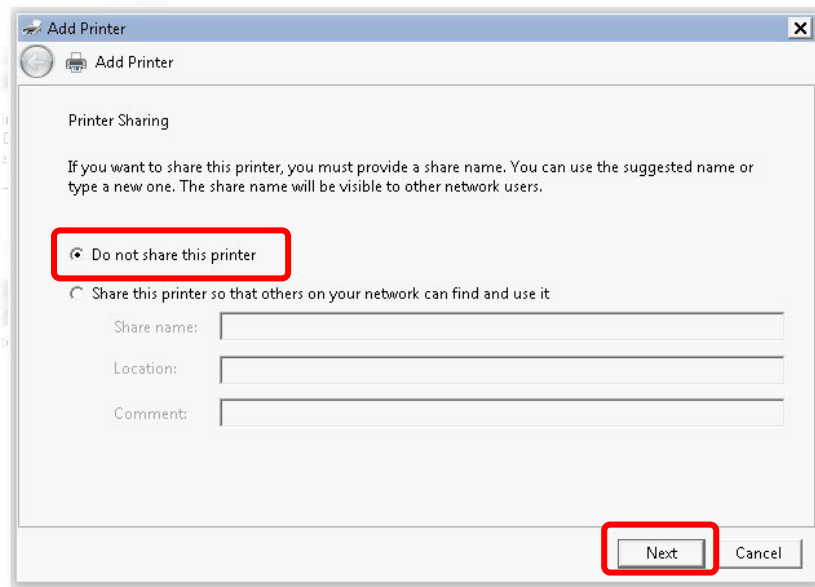
- Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.



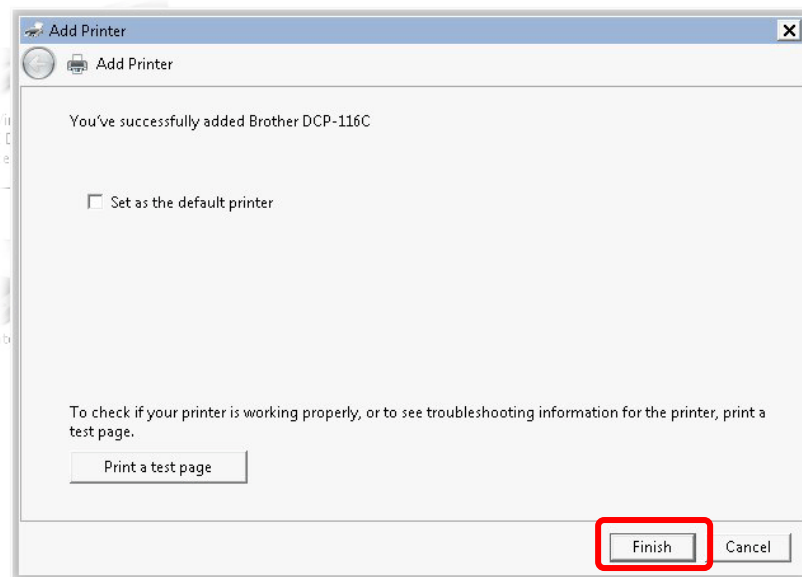
- Type a name for the chosen printer. Click **Next**.



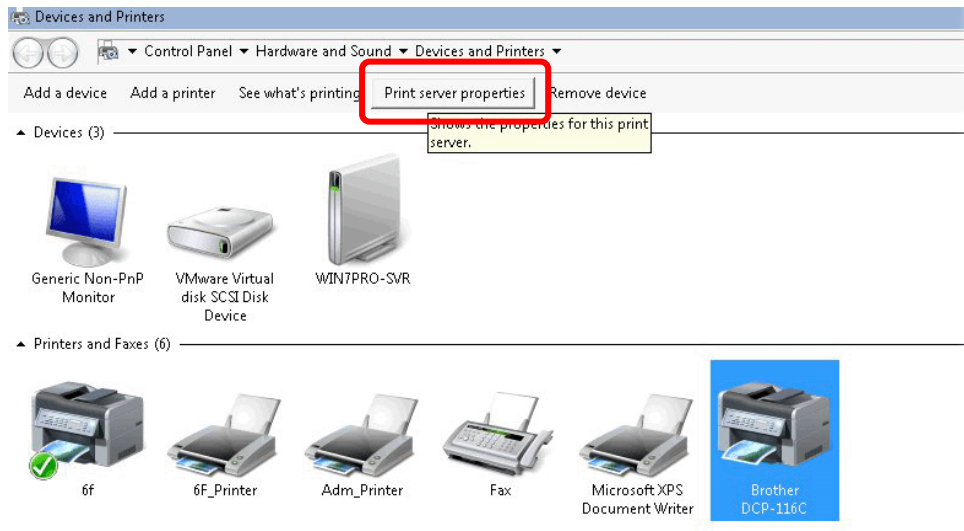
10. Choose **Do not share this printer** and click **Next**.



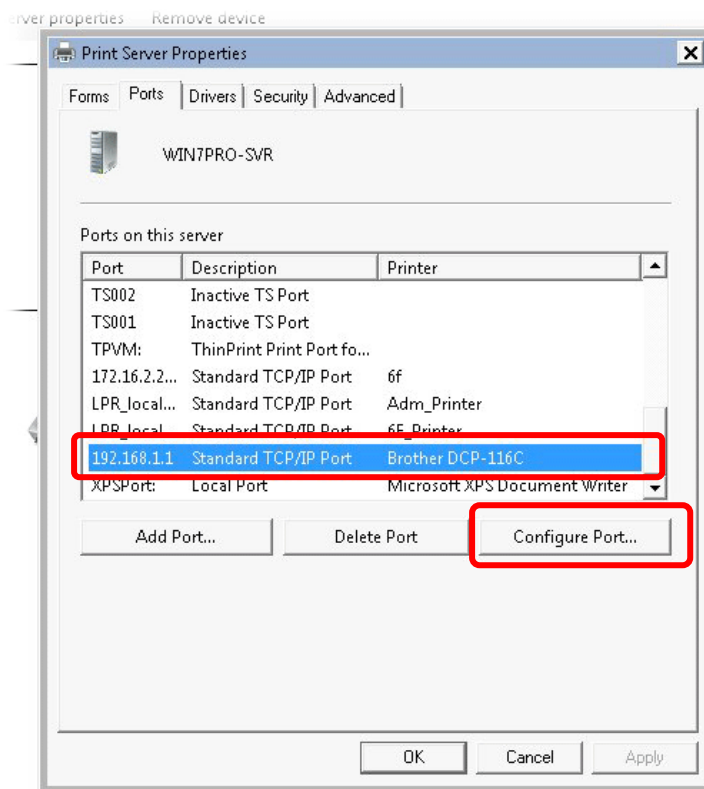
11. Then, in the following dialog, click **Finish**.



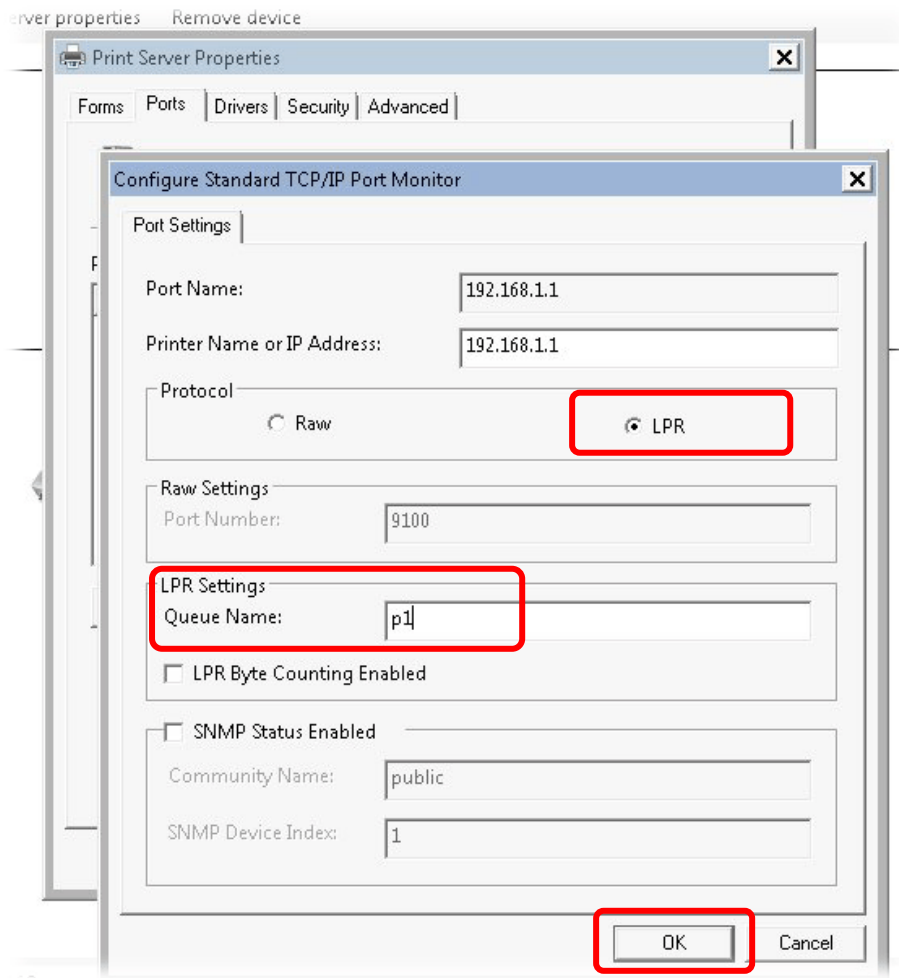
12. The new printer has been added and displayed under **Printers and Faxes**. Click the new printer icon and click **Printer server properties**.



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



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



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



Info

Some printers with the fax/scanning or other additional functions are not supported.

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

I-3 Accessing Web Page

1. Make sure your PC connects to the router correctly.
You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be the same subnet as the default IP address of Vigor router 192.168.1.1. For the detailed information, please refer to the later section - Trouble Shooting of the guide.
2. Open a web browser on your PC and type <http://192.168.1.1>. The following window will be open to ask for username and password.



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



Info

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

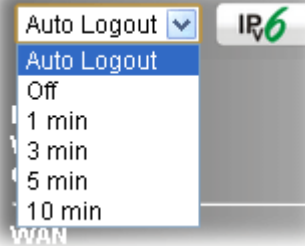
4. Now, the Main Screen will appear. Take Vigor2133Vac as an example.



Info

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

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



I-4 Changing Password

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

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

System Maintenance >> Administrator Password Setup

Administrator Password

Old Password	<input type="text"/>	
New Password	<input type="text"/>	(Max. 83 characters allowed)
Confirm Password	<input type="text"/>	(Max. 83 characters allowed)
Password Strength:	<input type="button" value="Weak"/> <input type="button" value="Medium"/> <input type="button" value="Strong"/>	
Strong password requirements:		
1. Have at least one upper-case letter and one lower-case letter.		
2. Including non-alphanumeric characters is a plus.		

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

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



Info

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

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



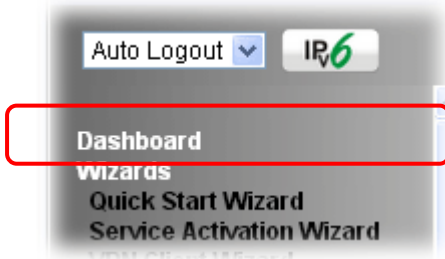
Info

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

I-5 Dashboard

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

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



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

Dashboard



System Information				Quick Access	
Model Name	Vigor2133Vac	System Up Time	0:1:48		
Router Name	DrayTek	Current Time	2000 Jan 1 Sat 0:1:40		
Firmware Version	3.8.8	Build Date/Time	Feb 27 2018 17:29:02		
LAN MAC Address	00-1D-AA-66-DF-F0				
IPv4 Internet Access					System Status
Line / Mode	IP Address	MAC Address	Up Time		
WAN1 Ethernet / DHCP Client	Disconnected	00-1D-AA-66-DF-F1	00:00:00		
WAN3 USB / ---	Disconnected	00-1D-AA-66-DF-F3	00:00:00		
Interface					
WAN	Connected: 0, <input type="radio"/> WAN1 <input type="radio"/> WAN3				
LAN	Connected: 0, <input type="radio"/> Port1 <input type="radio"/> Port2 <input type="radio"/> Port3 <input checked="" type="radio"/> Port4				
WLAN2.4G	Connected: 0				
WLAN5G	Connected: 0				
USB	Connected: 0, <input type="radio"/> USB 1 0, <input type="radio"/> USB 2				
Security					
VPN	Connected: 0 Remote Dial-in User / LAN to LAN				

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, or LAN1 - LAN4, related web setting page will be open for you to configure if required.

Dashboard



Port	Color	Description
LED (left side)	Black	It means the router or the function is not working.
	Green	It means the router or the function is working.
USB	Black	It means no USB device is connected.
	Green	It means a USB device is connected.
Ethernet Port (WAN/LAN)	Black	It means such port is disconnected.
	Green	It means such port is connected (with Giga transmission rate, 1Gbps) physically.
	Orange	It means such port is connected (with 10/100 Mbps) physically.

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](#) and etc.) below means you can click it to open the configuration page for modification.

System Information			
Model Name	Vigor2133Vac	System Up Time	0:1:48
Router Name	DrayTek	Current Time	2000 Jan 1 Sat 0:1:40
Firmware Version	3.8.8	Build Date/Time	Feb 27 2018 17:29:02
LAN MAC Address	00-1D-AA-66-DF-F0		

IPv4 Internet Access				
	Line / Mode	IP Address	MAC Address	Up Time
WAN1	Ethernet / DHCP Client	Disconnected	00-1D-AA-66-DF-F1	00:00:00
WAN3	USB / ---	Disconnected	00-1D-AA-66-DF-F3	00:00:00

I-5-3 Quick Access for Common Used Menu

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

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

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

The function links of System Status, Dynamic DDNS, 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	
WAN	Connected: 0, <input type="radio"/> WAN1
<input type="checkbox"/> LAN	Connected: 0, <input type="radio"/> Port1 <input type="radio"/> Port2 <input checked="" type="radio"/> Port3 <input type="radio"/> Port4
<input type="checkbox"/> WLAN5G	Connected: 0
USB	Connected: 0, <input type="radio"/> USB 1 0, <input type="radio"/> USB 2

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

System Resource	
Current Status :	CPU Usage: <div style="width: 1%; background-color: blue; height: 10px;"></div> 1%
	Memory Usage: <div style="width: 69%; background-color: blue; height: 10px;"></div> 69%

User Mode is **OFF** now.

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

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

WAN	Connected : 1, <input type="radio"/> WAN1 <input type="radio"/> WAN2 <input type="radio"/> WAN3						
LAN	Connected : 1, <input type="radio"/> LAN1 <input checked="" type="radio"/> LAN2 <input type="radio"/> LAN3 <input type="radio"/> LAN4 <input type="radio"/> LAN5						
	<table border="1"> <thead> <tr> <th>Host ID</th> <th>IP Address</th> <th>MAC</th> </tr> </thead> <tbody> <tr> <td>CARRIE-0C7CB251</td> <td>192.168.1.10</td> <td>E0-CB-4E-DA-48-79</td> </tr> </tbody> </table>	Host ID	IP Address	MAC	CARRIE-0C7CB251	192.168.1.10	E0-CB-4E-DA-48-79
Host ID	IP Address	MAC					
CARRIE-0C7CB251	192.168.1.10	E0-CB-4E-DA-48-79					
USB	Connected : 0, <input type="radio"/> USB 1						

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

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

I-5-4 GUI Map



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

GUI Map

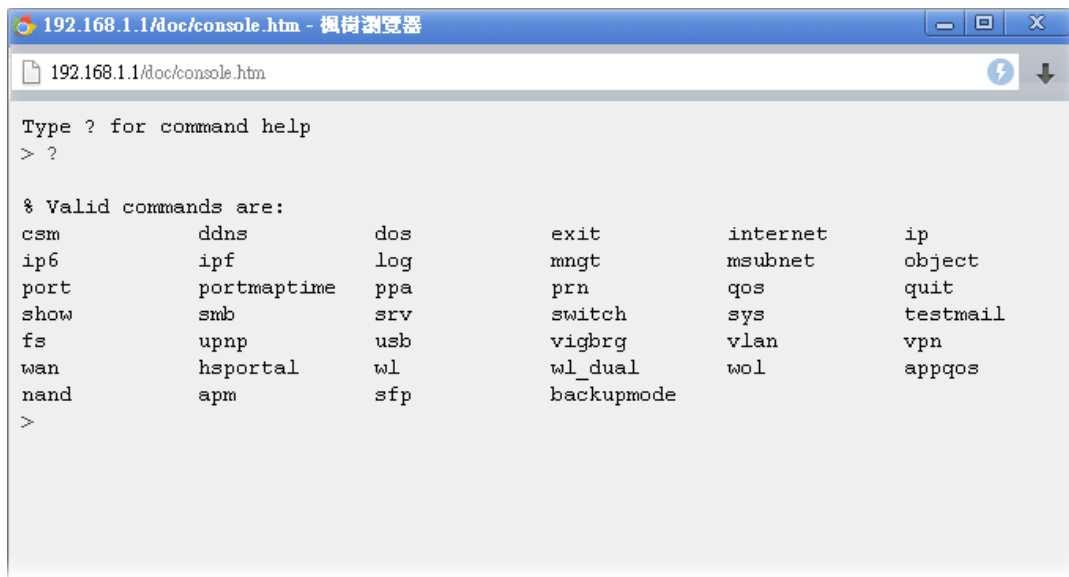
Dashboard		VPN and Remote Access	Remote Access Control
Wizards	Quick Start Wizard		PPP General Setup
	Service Activation Wizard		IPsec General Setup
	VPN Client Wizard		IPsec Peer Identity
	VPN Server Wizard		Remote Dial-in User
	Wireless Wizard		LAN to LAN
	VoIP Wizard		Connection Management
Online Status	Physical Connection	Certificate Management	Local Certificate
	Virtual WAN		Trusted CA Certificate
WAN	General Setup	VoIP	Certificate Backup
	Internet Access		General Settings
	Multi-VLAN	Wireless LAN (2.4 GHz)	General Setup
	WAN Budget		Security
LAN	General Setup		Access Control
	VLAN		WPS
	Bind IP to MAC		WDS
	LAN Port Mirror		Advanced Setting
	Wired 802.1X		Station Control
Hotspot Web Portal	Profile Setup		AP Discovery
			Band Steering
Routing	Static Route		Roaming
	Route Policy		Station List
NAT	Port Redirection	Wireless LAN (5 GHz)	Bandwidth Management
	DMZ Host		Airtime Fairness
	Open Ports		General Setup
	Port Triggering		Security
			Access Control

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 and a pop up dialog will appear.

Click **Save** to store the setting.

I-5-7 Logout



Click this icon to exit the web user interface.

I-5-8 Online Status

Online Status
Physical Connection
Virtual WAN

I-5-8-1 Physical Connection

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

Physical Connection for IPv4 Protocol

Online Status

Physical Connection		System Uptime: 0day 1:7:9			
IPv4		IPv6			
LAN Status					
IP Address	TX Packets	RX Packets	Router Primary DNS:	Router Secondary DNS:	
192.168.1.1	2676	2199	8.8.8.8	8.8.4.4	
WAN 1 Status >> Renew					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		DHCP Client	00:00:00	
IP	GW IP	TX Bytes	TX Rate(Bps)	RX Bytes	RX Rate(Bps)
---	---	0 (B)	0	0 (B)	0
WAN 3 Status					
Enable	Line	Name	Mode	Up Time	Signal
Yes	USB		---	00:00:00	-
IP	GW IP	TX Bytes	TX Rate(Bps)	RX Bytes	RX Rate(Bps)
---	---	0 (B)	0	0 (B)	0

Physical Connection for IPv6 Protocol

Online Status

Physical Connection		System Uptime: 0day 1:8:8	
IPv4	IPv6		
LAN Status			
IP Address FE80::21D:AFF:FE66:E010/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
23	11	1,802	858
WAN1 IPv6 Status			
Enable	Mode	Up Time	
No	Offline	---	
IP			Gateway IP
---			---
WAN3 IPv6 Status			
Enable	Mode	Up Time	
No	Offline	---	
IP			Gateway IP
---			---

Detailed explanation (for IPv4) is shown below:

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

Detailed explanation (for IPv6) is shown below:

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



Info

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

I-5-8-2 Virtual WAN

Such page displays the virtual WAN connection information.

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

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

I-6 Quick Start Wizard

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

Quick Start Wizard

Enter login password

Please enter an alpha-numeric string as your **Password**.

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.

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

Quick Start Wizard

Connect to Internet

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

- PPPoE
- PPTP
- L2TP
- Static IP
- DHCP

PPPoE

1. If you click **PPPoE** as the protocol, after clicking **Next**, you will get the following web page. Please manually enter the Username/Password provided by your ISP. Then click **Next**.

Quick Start Wizard

PPPoE Client Mode

WAN 1
Enter the user name and password provided by your ISP.

Service Name (Optional)	<input type="text" value="CHT"/>
Username	<input type="text" value="84005667@hinet.net"/>
Password	<input type="password" value="*****"/>
Confirm Password	<input type="password" value="*****"/>

Available settings are explained as follows:

Item	Description
Service Name (Optional)	Enter the description of the specific network service.
Username	Assign a specific valid user name provided by the ISP. Note: The maximum length of the user name you can set is 63 characters.
Password	Assign a valid password provided by the ISP. Note: The maximum length of the password you can set is 62 characters.
Confirm Password	Retype the password.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

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

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	PPPoE

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

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

Quick Start Wizard Setup OK!

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

PPTP/L2TP

1. Choose PPTP/L2TP as the WAN Interface and click the **Next** button.

Quick Start Wizard

Connect to Internet

WAN 1
Select one of the following Internet Access types provided by your ISP.

- PPPoE
- PPTP
- L2TP
- Static IP
- DHCP

2. The following page will be open for you to type in all the information originally provided by your ISP.

Quick Start Wizard

PPTP Client Mode

WAN 1
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

PPTP Server

Available settings are explained as follows:

Item	Description
Username	Assign a specific valid user name provided by the ISP. Note: The maximum length of the user name you can set is 63 characters.
Password	Assign a valid password provided by the ISP. Note: The maximum length of the password you can set is 62 characters.
Confirm Password	Retype the password.
WAN IP Configuration	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.
PPTP Server / L2TP Server	Type the IP address of the server.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

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

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	PPTP

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

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

Quick Start Wizard Setup OK!

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

Static IP

1. Click **Static IP** as the Internet Access type and click the **Next** button.

Quick Start Wizard

Connect to Internet

WAN 1
Select one of the following Internet Access types provided by your ISP.

- PPPoE
- PPTP
- L2TP
- Static IP
- DHCP

< Back Next > Finish Cancel

2. The following page will be open for you to type in the IP address information originally provided by your ISP.

Quick Start Wizard

Static IP Client Mode

WAN 1
Enter the Static IP configuration provided by your ISP.

WAN IP	<input type="text" value="192.168.3.100"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.3.1"/>
Primary DNS	<input type="text" value="8.8.8.8"/>
Secondary DNS	<input type="text" value="8.8.4.4"/> (optional)

< Back Next > Finish Cancel

Available settings are explained as follows:

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

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

- 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:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	Static IP

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

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

Quick Start Wizard Setup OK!

- Now, you can enjoy surfing on the Internet.

DHCP

- Click **DHCP** as the Internet Access type and click the **Next** button.

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

- The following page will be open for you to type in the IP address information originally provided by your ISP.

Quick Start Wizard

DHCP Client Mode

WAN 1
If your ISP requires you to enter a specific host name or specific MAC address, please enter it in.

Host Name (optional)

MAC (optional)

Available settings are explained as follows:

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

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

Quick Start Wizard

Please confirm your settings:

WAN Interface: WAN1
 Physical Mode: Ethernet
 Physical Type: Auto negotiation
 Internet Access: DHCP

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

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

Quick Start Wizard Setup OK!

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

I-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, please type "admin/admin" on Username/Password while Logging into the web user interface.

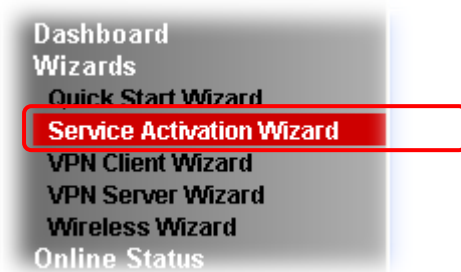
Service Activation Wizard is a tool which allows you to activate services without accessing into the server (**MyVigor**) located on <http://myvigor.draytek.com>.



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 and APPE Enforcement service at the same time or individually. When you finish the selection, please click Next.

Service Activation Wizard

Select the service type that you want to activate

Activation Date : 2017-08-03

Web Content Filter(WCF) Service :

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

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

APP Enforcement(APPE) Service :

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

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

Next >

Cancel



Info

BPjM is web content filter (WCF) for German Speaking users. It is ideal for your

family to provide more Internet security for youngsters.

Cryan 30-day trial is WCF which offers 30-day trial period. After trial, you can purchase DrayTek's prepared Cryan GlobalView WCF package from retailing outlets.

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

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 (Cyren / Commtouch)
APP Enforcement (DT-APPE)

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



Info

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

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

DrayTek Service Activation

Service Name	Start Date	Expire Date	Status
Web Content filter	2017-06-21	2017-07-21	Cyren
APP Enforcement	2017-06-21	2017-07-21	DT-APPE

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

Copyright © DrayTek Corp. All Rights Reserved.

I-8 Registering Vigor Router

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

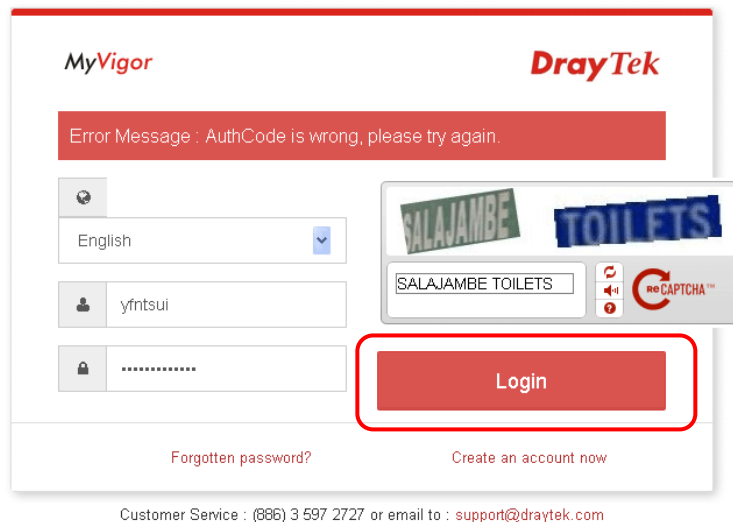
- 1 Please login the web configuration interface of Vigor router by typing "admin/admin" as User Name / Password.



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



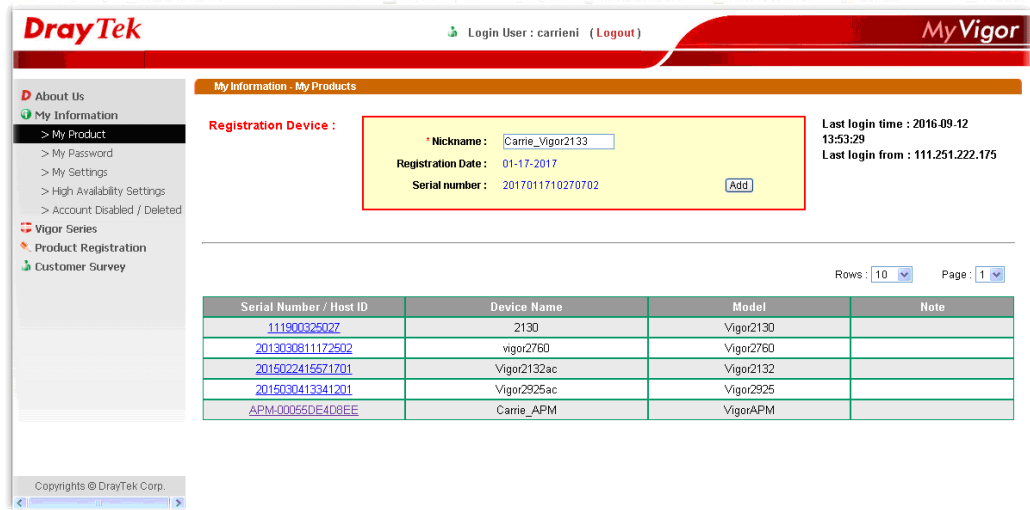
- 3 A **Login** page will be shown on the screen. Please type the account and password that you created previously. And click **Login**.



Info

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

- The following page will be displayed after you logging in MyVigor. When the following page appears, please type in Nickname (for the router) and choose the right registration date from the popup calendar (it appears when you click on the box of Registration Date). Click Add.

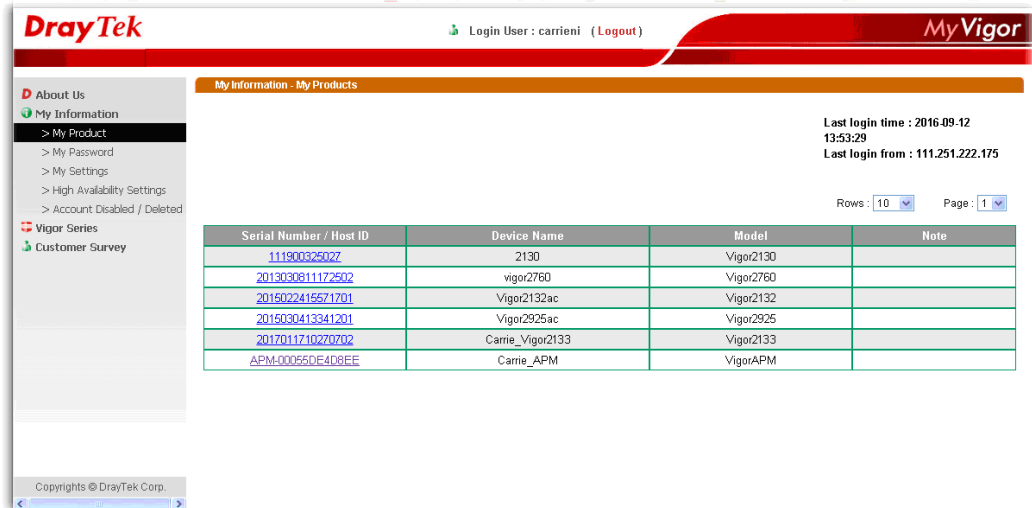


- When the following page appears, your router information has been added to the database.

Your device has been successfully added to the database.



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



Part II Connectivity



WAN

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



LAN

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



NAT

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



Applications

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



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.

Web User Interface



II-1-1 General Setup

This section will introduce some general settings of Internet and explain the connection modes for WAN in details.

II-1-1-1 WAN1

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

WAN >> General Setup

Setup	Index	Enable	Physical Mode/Type	Active Mode	Load Balance
	WAN1	V	Ethernet/Auto negotiation	Always On	V
	WAN3	V	USB/-	Failover(WAN1)	V

Note:

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

OK

Available settings are explained as follows:

Item	Description
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.
Load Balance	Display if Load Balance feature is enabled or disabled for such WAN interface.



Info

In default, each WAN port is enabled.

Click WAN1 link to get the following page:

WAN >> General Setup

WAN 1

Enable:	Yes
Display Name:	<input type="text"/>
Physical Mode:	Fiber
SFP Module:	
Vendor Name:	
Vendor PN:	
Physical Type:	1000M
VLAN Tag insertion :	Enable
Tag value:	0 (0~4095)
Priority:	0 (0~7)
Active Mode:	Always On

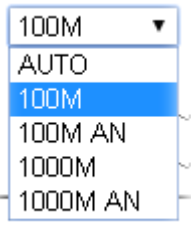
Or

WAN >> General Setup

WAN 1

Enable:	Yes
Display Name:	<input type="text"/>
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
VLAN Tag insertion :	Disable
Tag value:	0 (0~4095)
Priority:	0 (0~7)
Active Mode:	Always On

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	<p>You can change the physical type for WAN2 or choose Auto negotiation for determined by the system.</p> 
VLAN Tag insertion	<p>Enable - Enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the WAN while sending them out. Please type the tag value and specify the priority for the</p>

	packets sending by WAN interface. 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.
--	---

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

II-1-1-2 WAN3 (USB)

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

WAN >> General Setup

WAN 3

Enable:	<input type="button" value="Yes"/>
Display Name:	<input type="text"/>
Physical Mode:	USB
Active Mode:	<input type="button" value="Failover"/>
	<input checked="" type="checkbox"/> WAN 1

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.

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

II-1-2 Internet Access

This page allows you to set WAN configuration with different modes. Use the Connection Type drop down list to choose one of the WAN modes. The corresponding page will be displayed.

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode		
WAN1		Ethernet	Static or Dynamic IP	Details Page	IPv6
WAN3		USB	None	Details Page	IPv6

[DHCP Client Option](#)

Available settings are explained as follows:

Item	Description
Index	Display the WAN interface.
Display Name	It shows the name of the WAN1/WAN2/WAN3 /WAN4 that entered in general setup.
Physical Mode	It shows the physical connection for WAN (Ethernet or fiber) 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.
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.

WAN >> Internet Access

DHCP Client Options Status

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

Enable:

Interface: All WAN1 WAN5 WAN6

Option Number:

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

Data:

[Add](#) [Update](#) [Delete](#) [Reset](#)

Note:

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

[OK](#)

Enable - Check the box to enable the function of DHCP

	<p>Option. Each DHCP option is composed by an option number with data. For example,</p> <p>Option number: 100 Data: abcd</p> <p>When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets.</p> <p>Interface - Specify the WAN interface(s) that will be overwritten by such function. WAN5 ~ WAN6 can be located under WAN>>Multi-PVC/VLAN.</p> <p>Option Number - Type a number for such function.</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>Note: If you choose to configure option 61 here, the detailed settings in WAN>>Interface Access will be overwritten.</p> </div> <p>Data Type - Choose the type (ASCII or Hex) for the data to be stored.</p> <p>Data - Type the content of the data to be processed by the function of DHCP option.</p>
--	--

II-1-2-1 Details Page for PPPoE

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

WAN >> Internet Access

WAN 1

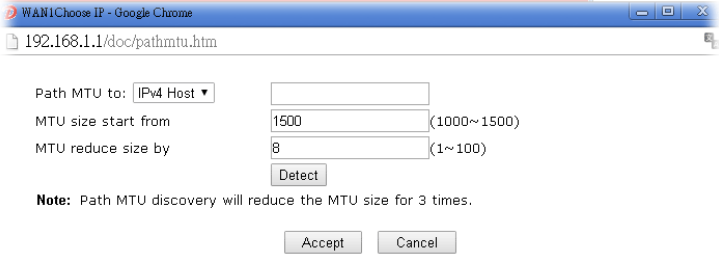
PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
ISP Access Setup Service Name (Optional) <input type="text" value="CHT"/> Username <input type="text" value="84005667@hinet.net"/> Password <input type="password" value="....."/> Index(1-15) in Schedule Setup: => <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>		PPP/MP Setup PPP Authentication <input type="text" value="PAP or CHAP"/> Idle Timeout <input type="text" value="-1"/> second(s)	
PPPoE Pass-through¹ <input type="checkbox"/> For Wired LAN <input type="checkbox"/> For Wireless LAN		IP Address Assignment Method (IPCP) <input type="text" value="WAN IP Alias"/> Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address <input type="text"/>	
WAN Connection Detection Mode <input type="text" value="PPP Detect"/>		<input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: <input type="text" value="00"/> <input type="text" value="1D"/> <input type="text" value="AA"/> <input type="text" value="66"/> <input type="text" value="DF"/> <input type="text" value="F1"/>	
MTU <input type="text" value="1500"/> (Max: 1500) Path MTU Discovery <input type="text" value="Detect"/>			
TTL Change the TTL value <input type="text" value="Enable"/>			

Note:

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

Available settings are explained as follows:

Item	Description
Enable/Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
ISP Access Setup	<p>Enter your allocated username, password and authentication parameters according to the information provided by your ISP.</p> <p>Service Name (Optional) - Enter the description of the specific network service.</p> <p>Username - Type in the username provided by ISP in this field. The maximum length of the user name you can set is 63 characters.</p> <p>Password - Type in the password provided by ISP in this field. The maximum length of the password you can set is 62 characters.</p> <p>Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page.</p>
PPPoE Pass-through	<p>The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction.</p> <p>For Wired LAN - If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet.</p> <p>For Wireless LAN - It is available for <i>n</i> model. If you check this box, PCs on the same wireless network can use another set of PPPoE session (different with the Host PC) to access into Internet.</p> <p>Note: To have PPPoA Pass-through, please choose PPPoA protocol and check the box(es) here. The router will behave like a modem which only serves the PPPoE client on the LAN. That's, the router will offer PPPoA dial-up connection.</p>
WAN Connection Detection	<p>Such function allows you to verify whether network connection is alive or not through PPP Detect or Ping Detect.</p> <p>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.</p> <ul style="list-style-type: none"> ● Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation. ● Ping Interval - Type the interval for the system to execute the PING operation.

	<ul style="list-style-type: none"> ● Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
<p>MTU</p>	<p>It means Max Transmit Unit for packet.</p> <p>Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path.</p> <p>Click Detect to open the following dialog.</p>  <ul style="list-style-type: none"> ● Path MTU to - Type the IP address as the specific transmit path. ● MTU size start from - Determine the starting point value of the packet. ● MTU reduce size by - It determines the decreasing size of MTU value. For example, the number specified in this field is "8". The maximum MTU size is "1500". After clicking the "detect" button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically. ● Detect - Click it to detect a suitable MTU value ● Accept - After clicking it, the detected value will be displayed in the field of MTU.
<p>TTL</p>	<p>Change the TTL value - Enable or disable the TTL (Time to Live) for a packet transmitted through Vigor router.</p> <p>Enable - TTL value will be reduced (-1) when it passes through Vigor router. It will cause the client, accessing Internet through Vigor router, be blocked by certain ISP when TTL value becomes "0".</p> <p>Disable - TTL value will not be reduced. Then, when a packet passes through Vigor router, it will not be cancelled. That is, the client who sends out the packet will not be blocked by ISP.</p>
<p>PPP/MP Setup</p>	<p>PPP Authentication - Select PAP only or PAP or CHAP for PPP.</p> <p>Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action.</p>
<p>IP Address Assignment Method (IPCP)</p>	<p>Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function.</p> <p>WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 32 public IP addresses other than the current one you are using. Type the additional WAN</p>

	<p>IP address and check the Enable box. Then click OK to exit the dialog.</p> <p>Fixed IP - Click Yes to use this function and type in a fixed IP address in the box of Fixed IP Address.</p> <p>Default MAC Address - You can use Default MAC Address or specify another MAC address by typing on the boxes of MAC Address for the router.</p> <p>Specify a MAC Address - Type the MAC address for the router manually.</p>
--	---

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

II-1-2-2 Details Page for Static or Dynamic IP

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 1

PPPoE
 Static or Dynamic IP
 PPTP/L2TP
 IPv6

Enable
 Disable

Keep WAN Connection

Enable PING to keep alive
PING to the IP:
PING Interval: minute(s)

WAN Connection Detection

Mode:

MTU

(Max: 1500)
Path MTU Discovery:

RIP Protocol

Enable RIP

TTL

Change the TTL value:

WAN IP Network Settings

Obtain an IP address automatically
Router Name: *
Domain Name: *
 DHCP Client Identifier *
Username:
Password:

Specify an IP address
IP Address:
Subnet Mask:
Gateway IP Address:

Default MAC Address
 Specify a MAC Address
MAC Address: · · : · ·

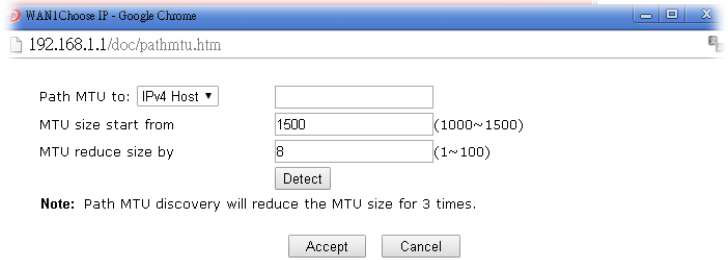
DNS Server IP Address

Primary IP Address:
Secondary IP Address:

*: Required for some ISPs

Available settings are explained as follows:

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

<p>Keep WAN Connection</p>	<p>Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time. Check Enable PING to keep alive box to activate this function.</p> <p>PING to the IP - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive.</p> <p>PING Interval - Enter the interval for the system to execute the PING operation.</p>
<p>WAN Connection Detection</p>	<p>Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.</p> <p>Mode - Choose ARP Detect, Ping Detect or Always On for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items.</p> <ul style="list-style-type: none"> ● Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation. ● Ping Interval - Type the interval for the system to execute the PING operation. ● Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
<p>MTU</p>	<p>It means Max Transmit Unit for packet.</p> <p>Path MTU Discovery - It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path.</p> <p>Click Detect to open the following dialog.</p>  <ul style="list-style-type: none"> ● Path MTU to - Choose the destination as the specific transmit path and type the IP address. ● MTU size start from - Determine the starting point value of the packet. ● MTU reduce size by - It determines the decreasing size of MTU value. For example, the number specified in this field is "8". The maximum MTU size is "1500". After clicking the "detect" button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically. ● Detect - Click it to detect a suitable MTU value ● Accept - After clicking it, the detected value will be

	displayed in the field of MTU.
RIP Protocol	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.
TTL	<p>Change the TTL value - Enable or disable the TTL (Time to Live) for a packet transmitted through Vigor router.</p> <p>Enable - TTL value will be reduced (-1) when it passes through Vigor router. It will cause the client, accessing Internet through Vigor router, be blocked by certain ISP when TTL value becomes "0".</p> <p>Disable - TTL value will not be reduced. Then, when a packet passes through Vigor router, it will not be cancelled. That is, the client who sends out the packet will not be blocked by ISP.</p>
WAN IP Network Settings	<p>This group allows you to obtain an IP address automatically and allows you type in IP address manually.</p> <p>WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 32 public IP addresses other than the current one you are using.</p> <p>Obtain an IP address automatically - Click this button to obtain the IP address automatically if you want to use Dynamic IP mode.</p> <ul style="list-style-type: none"> ● Router Name: Type in the router name provided by ISP. ● Domain Name: Type in the domain name that you have assigned. <p>DHCP Client Identifier</p> <ul style="list-style-type: none"> ● Enable: Check the box to specify username and password as the DHCP client identifier for some ISP. ● Username: Type a name as username. The maximum length of the user name you can set is 63 characters. ● Password: Type a password. The maximum length of the password you can set is 62 characters. <p>Specify an IP address - Click this radio button to specify some data if you want to use Static IP mode.</p> <ul style="list-style-type: none"> ● IP Address: Type the IP address. ● Subnet Mask: Type the subnet mask. ● Gateway IP Address: Type the gateway IP address. <p>Default MAC Address: Click this radio button to use default MAC address for the router.</p> <p>Specify a MAC Address: Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the Specify a MAC Address and enter the MAC address in the MAC Address field.</p>
DNS Server IP Address	Type in the primary IP address for the router if you want to use Static IP mode . If necessary, type in secondary IP address for necessity in the future.

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

II-1-2-3 Details Page for PPTP/L2TP

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

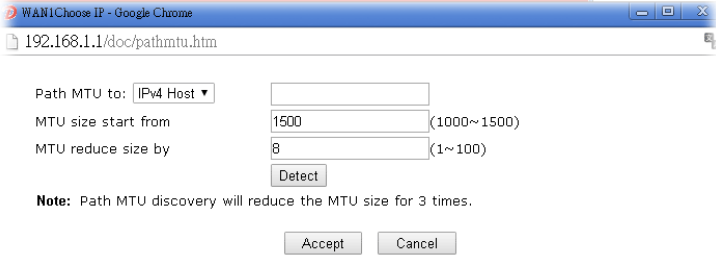
WAN >> Internet Access

WAN 1

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
<input type="radio"/> Enable PPTP <input type="radio"/> Enable L2TP <input checked="" type="radio"/> Disable Server Address <input type="text"/> Specify Gateway IP Address <input type="text"/>		PPP Setup PPP Authentication <input type="text" value="PAP or CHAP"/> Idle Timeout <input type="text" value="-1"/> second(s) IP Address Assignment Method (IPCP) <input type="button" value="WAN IP Alias"/> Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address <input type="text"/> WAN IP Network Settings <input checked="" type="radio"/> Obtain an IP address automatically <input type="radio"/> Specify an IP address IP Address <input type="text"/> Subnet Mask <input type="text"/>	
ISP Access Setup Username <input type="text" value="84005667@hinet.net"/> Password <input type="password" value="....."/> Index(1-15) in Schedule Setup: => <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>			
MTU <input type="text" value="1460"/> (Max: 1460) Path MTU Discovery <input type="button" value="Detect"/>			

Available settings are explained as follows:

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

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

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

II-1-2-4 Details Page for IPv6 – Offline

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

WAN >> Internet Access



WAN 1

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
Internet Access Mode			
Connection Type		Offline	

OK Cancel

II-1-2-5 Details Page for IPv6 – PPP

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	Static or Dynamic IP	PPTP/L2TP	IPv6
Internet Access Mode			
Connection Type		PPP	
WAN Connection Detection			
Mode		Ping Detect	
Ping IP/Hostname		<input type="text"/>	
TTL(1-255,0: Auto)		<input type="text" value="0"/>	
RIPng Protocol			
<input type="checkbox"/> Enable			

Note:

IPv4 WAN setting should be PPPoE / PPPoA client.

OK Cancel

Available settings are explained as follows:

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

	detection mode, you have to type TTL value.
RIPng Protocol	RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.

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

Online Status

Physical Connection		System Uptime: 0:2:32	
IPv4	IPv6		
LAN Status			
IP Address			
2001:8010:7300:201:21D:AFF:FEA6:2568/64 (Global)			
FE80::21D:AFF:FEA6:2568/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
7	4	690	328
WAN2 IPv6 Status >> Drop PPP			
Enable	Mode	Up Time	
Yes	PPP	0:02:08	
IP		Gateway IP	
2001:8010:7300:201:21D:AFF:FEA6:256A/128 (Global)		FE80::90:1A00:242:AD52	
FE80::1D:AFF:FEA6:256A/128 (Link)			
DNS IP			
2001:8000:168::1			
2001:8000:168::2			
TX Packets	RX Packets	TX Bytes	RX Bytes
7	9	544	1126



Info

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

II-1-2-6 Details Page for IPv6 – TSPC

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

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

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



WAN 1

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
<p>Internet Access Mode</p> <p>Connection Type <input type="text" value="TSPC"/></p> <p>TSPC Configuration</p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>Tunnel Broker <input type="text"/></p> <p>WAN Connection Detection</p> <p>Mode <input type="text" value="Always On"/></p>			

Available settings are explained as follows:

Item	Description
Username	Type the name obtained from the broker. It is suggested for you to apply another username and password for http://gogonet.gogo6.com/page/freenet6-account . The maximum length of the name you can set is 63 characters.
Password	Type the password assigned with the user name. The maximum length of the name you can set is 19 characters.
Tunnel Broker	Type the address for the tunnel broker IP, FQDN or an optional port number.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. Mode - Choose Always On or Ping Detect for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always. <ul style="list-style-type: none"> ● Ping IP/Hostname - If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. ● TTL (Time to Live) -If you choose Ping Detect as detection mode, you have to type TTL value.

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

II-1-2-7 Details Page for IPv6 – AICCU

WAN >> Internet Access



WAN 1

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
<p>Internet Access Mode</p> <p>Connection Type: AICCU</p> <p>AICCU Configuration</p> <p><input type="checkbox"/> Always On</p> <p>Username: <input type="text"/></p> <p>Password: <input type="text"/></p> <p>Tunnel Broker: tic.sixxs.net</p> <p>Tunnel ID: <input type="text"/></p> <p>Subnet Prefix: <input type="text"/> / <input type="text"/></p> <p>WAN Connection Detection</p> <p>Mode: Always On</p>			

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-1-2-8 Details Page for IPv6 – DHCPv6 Client

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

WAN >> Internet Access ?

WAN 1

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
Internet Access Mode			
Connection Type		DHCPv6 Client ▼	
DHCPv6 Client Configuration			
IAID (Identity Association ID)		44178339	
DUID (DHCP Unique ID)		00030001001daa000001	
Authentication Protocol		None ▼	
WAN Connection Detection			
Mode		NS Detect ▼	
RIPng Protocol			
<input type="checkbox"/> Enable			
Bridge Mode			
<input checked="" type="checkbox"/> Enable Bridge Mode			
<input type="checkbox"/> Enable Firewall			
Bridge Subnet		LAN 1 ▼	

Available settings are explained as follows:

Item	Description
DHCPv6 Client Configuration	<p>IAID - Type a number as IAID.</p> <p>DUID - Display the DHCP unique ID used by such WAN interface.</p> <p>Authentication Protocol - Such protocol will be used for the client to be authenticated by DHCPv6 server before accessing into Internet. There are three types can be specified, Reconfigure Key, Delayed and None. In general, the default setting is None.</p> <ul style="list-style-type: none"> ● Reconfigure Key - During the connection process, DHCPv6 server will authenticate the client automatically. ● Delayed - During the connection process, DHCPv6 server will authenticate and identify the client based on the key ID, realm and secret information specified in these fields. <p>Key ID - Type a value (range from 1 to 65535) which will be used to generate HMAC-MD5 value.</p> <p>Realm - The name (1 to 31 characters) typed here will identify the key which generates HMAC-MD5 value.</p>

	<p>Secret - Type a text (1 to 31 characters) as a unique identifier for each client on each DHCP server.</p>
WAN Connection Detection	<p>Such function allows you to verify whether network connection is alive or not through NS Detect or Ping Detect.</p> <p>Mode - Choose Always On, Ping Detect or NS Detect for the system to execute for WAN detection. With NS Detect mode, the system will check if network connection is established or not, like IPv4 ARP Detect. Always On means no detection will be executed. The network connection will be on always.</p> <ul style="list-style-type: none"> ● Ping IP/Hostname - If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. ● TTL (Time to Live) -If you choose Ping Detect as detection mode, you have to type TTL value.
Bridge Mode	<p>Enable Bridge Mode - If the function is enabled, the router will work as a bridge modem.</p> <p>Enable Firewall - It is available when Bridge Mode is enabled. When both Bridge Mode and Firewall check boxes are enabled, the settings configured (user profiles) under User Management will be ignored. And all of the filter rules defined and enabled in Firewall menu will be activated.</p> <p>Bridge Subnet - Make a bridge between the selected LAN subnet and such WAN interface.</p>

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

II-1-2-9 Details Page for IPv6 – Static IPv6

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

WAN >> Internet Access



WAN 1

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6			
Internet Access Mode						
Connection Type		Static IPv6				
Static IPv6 Address Configuration						
IPv6 Address		/ Prefix Length				
<input type="text"/>		/ <input type="text"/> <input type="button" value="Add"/> <input type="button" value="Update"/> <input type="button" value="Delete"/>				
Current IPv6 Address Table						
Index		IPv6 Address/Prefix Length	Scope			
<table border="1"><tr><td> </td><td> </td><td> </td></tr></table>						
Static IPv6 Gateway configuration						
IPv6 Gateway Address		<input type="text"/>				
WAN Connection Detection						
Mode		Ping Detect				
Ping IP/Hostname		<input type="text"/>				
TTL(1-255,0: Auto)		<input type="text"/>				
RIPng Protocol						
<input type="checkbox"/> Enable						
Bridge Mode						
<input checked="" type="checkbox"/> Enable Bridge Mode						
<input type="checkbox"/> Enable Firewall						
Bridge Subnet		LAN 1				

Available settings are explained as follows:

Item	Description
Static IPv6 Address configuration	IPv6 Address - Type the IPv6 Static IP Address. Prefix Length - Type the fixed value for prefix length. Add - Click it to add a new entry. 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	IPv6 Gateway Address - Type your IPv6 gateway address

Configuration	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 for the system to execute for WAN detection. Always On means no detection will be executed. The network connection will be on always. <ul style="list-style-type: none"> ● Ping IP/Hostname - If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. ● TTL (Time to Live) -If you choose Ping Detect as detection mode, you have to type TTL value.
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-1-2-10 Details Page for IPv6 – 6in4 Static Tunnel

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	Static or Dynamic IP	PPTP/L2TP	IPv6
Internet Access Mode			
Connection Type		6in4 Static Tunnel ▼	
6in4 Static Tunnel			
Remote Endpoint IPv4 Address		<input type="text"/>	
6in4 IPv6 Address		<input type="text"/>	/ 64 (default: 64)
LAN Routed Prefix		<input type="text"/>	/ 64 (default: 64)
Tunnel TTL		<input type="text" value="255"/>	(default: 255)
WAN Connection Detection			
Mode		Ping Detect ▼	
Ping IP/Hostname		<input type="text"/>	
TTL(1-255,0: Auto)		<input type="text" value="0"/>	

Available settings are explained as follows:

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

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

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

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

Online Status

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

II-1-2-11 Details Page for IPv6 – 6rd

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

WAN >> Internet Access



WAN 1

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
Internet Access Mode			
Connection Type		6rd ▼	
6rd Settings			
6rd Mode		<input type="radio"/> Auto 6rd <input checked="" type="radio"/> Static 6rd	
Static 6rd Settings			
IPv4 Border Relay:		<input type="text"/>	
IPv4 Mask Length:		<input type="text" value="0"/>	
6rd Prefix:		<input type="text"/>	
6rd Prefix Length:		<input type="text" value="0"/>	
WAN Connection Detection			
Mode		Ping Detect ▼	
Ping IP/Hostname		<input type="text"/>	
TTL(1-255,0:Auto)		<input type="text" value="0"/>	

Available settings are explained as follows:

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

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

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

Online Status

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

II-1-3 Multi-VLAN

Multi-VLAN allows users to create profiles for specific WAN interface and bridge connections for user applications that require very high network throughput. Simply go to **WAN** and select **Multi-VLAN**.

General

This page shows the basic configurations used by every channel. In which, **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).

WAN >> Multi-VLAN

Multi-VLAN

General

Channel	Enable	WAN Type	VLAN Tag	Port-based Bridge
1	<input checked="" type="checkbox"/>	Ethernet(WAN1)	None	
4. WAN4	<input type="checkbox"/>	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
5. WAN5	<input type="checkbox"/>	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
6. WAN6	<input type="checkbox"/>	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
7.	<input type="checkbox"/>	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
8.	<input type="checkbox"/>	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
9.	<input type="checkbox"/>	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
10.	<input type="checkbox"/>	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4

Note:

Channel 2~3 is reserved.

OK Cancel

Available settings are explained as follows:

Item	Description
Channel	Display the number of each channel. Channels 1 is used by the Internet Access web user interface and can not be configured here. Channels 4 ~ 10 are configurable.
Enable	Display whether the settings in this channel are enabled (Yes) or not (No).
WAN Type	Displays the physical medium that the channel will use.
VLAN Tag	Displays the VLAN tag value that will be used for the packets traveling on this channel.
Port-based Bridge	The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value. Enable - Check this box to enable the port-based bridge function on this channel. P1 ~ P4 - Check the box(es) to build bridge connection on LAN.

To configure a PVC channel, click its channel number.

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

WAN >> Multi-VLAN >> Channel 4

Multi-VLAN Channel 4: **Enable** **Disable**

General Settings

VLAN Header

VLAN Tag:

Priority: ▼

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.

Open Port-based Bridge Connection for this Channel

Physical Members

P1 P2 P3 P4

Note: P1 is reserved for NAT use, and cannot be configured for bridge mode.

Open WAN Interface for this Channel

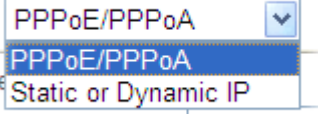
WAN Application: Management VoIP IPTV

WAN Setup: ▼

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

Available settings are explained as follows:

Item	Description
Multi-VLAN Channel 4/5/6	Enable - Select to enable this channel. Disable - Select to disable this channel.
General Settings	VLAN Tag - Type the value as the VLAN ID number. Valid settings are in the range from 1 to 4095. The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value. Priority - Choose the number to determine the packet priority for such VLAN. The range is from 0 to 7.
Open Port-based Bridge	The settings here will create a bridge between the LAN ports

Connection for this Channel	<p>selected and the WAN. The WAN interface of the bridge connection will be built upon the WAN type selected using the VLAN tag configured.</p> <p>Physical Members - Group the physical ports by checking the corresponding check box(es) for applying the port-based bridge connection.</p> <p>Note: LAN port P1 is reserved for NAT use and cannot be selected for bridging.</p>
Open WAN Interface for this Channel	<p>Check the box to enable relating function.</p> <p>WAN Application</p> <ul style="list-style-type: none"> ● Management can be specified for general management (Web configuration/telnet/TR069). If you choose Management, the configuration for this VLAN will be effective for Web configuration/telnet/TR069. ● IPTV - The IPTV configuration will allow the WAN interface to send IGMP packets to IPTV servers. <p>WAN Setup - Choose PPPoE/PPPoA or Static or Dynamic IP to determine what WAN settings must be configured.</p> 
ISP Access Setup, IP Address From ISP, WAN IP Network Settings, DNS Server IP Address	<p>For other settings, refer to Details Page for PPPoE in WAN1.</p>

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

Click any index (7, 8, 9 and 10) to get the following web page:

WAN >> Multi-VLAN >> Channel 8

Multi-VLAN Channel 8: Enable Disable

General Settings

VLAN Header

VLAN Tag:

Priority:

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

Note: P1 is reserved for NAT use, and cannot be configured for bridge mode.

Available settings are explained as follows:

Item	Description
Multi-VLAN Channel	Enable - Click it to enable the configuration of this channel.

7/8/9/10	Disable -Click it to disable the configuration of this channel.
General Settings	<p>VLAN Tag - Type the value as the VLAN ID number. Valid settings are in the range from 1 to 4095. The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value.</p> <p>Priority - Choose the number to determine the packet priority for such VLAN. The range is from 0 to 7.</p>
Bridge mode	<p>Enable - Click it to enable Bridge mode for such channel.</p> <p>Physical Members - Group the physical ports by checking the corresponding check box(es) for applying the bridge connection.</p>

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

II-1-4 WAN Budget

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

II-1-4-1 General Setup

WAN >> WAN Budget

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

Note:

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

OK Cancel

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/ WAN3 link to open the following web page.

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**

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

Data quota resets on day at

Note:

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

Available settings are explained as follows:

Item	Description
Enable	Check the box to enable such function.
Quota Limit	Type the data traffic quota allowed for such WAN interface. There are two unit (MB and GB) offered for you to specify.
When quota exceeded	<p>Check the box(es) as the condition(s) for the system to perform when the traffic has exceeded the budget limit.</p> <p>Shutdown WAN interface - All the outgoing traffic through such WAN interface will be terminated.</p> <ul style="list-style-type: none"> ● 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	<p>Some ISP might apply for the network limitation based on the traffic limit per month. This setting is to offer a mechanism of resetting the traffic record every month.</p> <p>Monthly Custom</p> <p>Select the day of a month when your (cellular) data resets.</p> <p>Data quota resets on day <input type="text" value="1"/> at <input type="text" value="00:00"/></p> <p>Data quota resets on day ... - You can determine the starting day in one month.</p>
Custom	<p>This setting allows the user to define the billing cycle according to his request. The WAN budget will be reset with an interval of billing cycle.</p> <p>Monthly is default setting. If long period or a short period is required, use Custom. The period of cycle duration is</p>

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

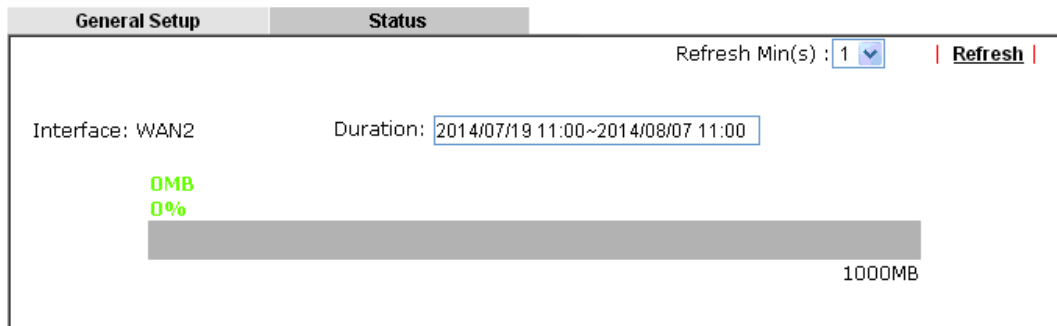
- **Cycle duration:** Specify the days to reset the traffic record. For example, 7 means the whole cycle is 7 days; 20 means the whole cycle is 20 days. When the time is up, the router will reset the traffic record automatically.
- **Today is day -** Specify the day and time for data quota rest in the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

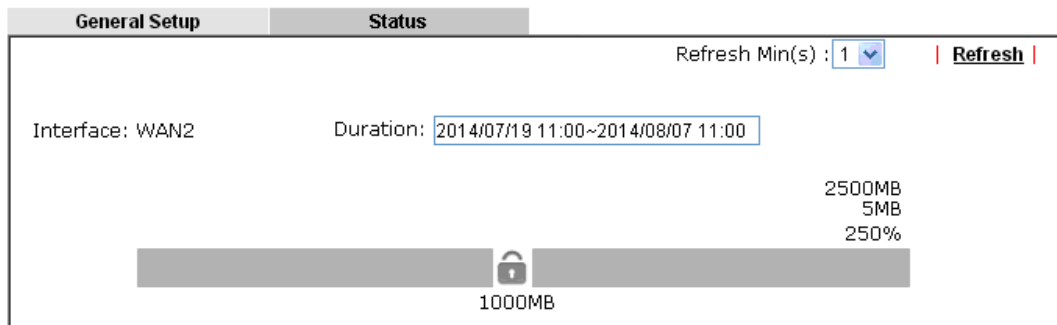
The status page displays the status WAN budget, including the duration and the usage.

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 **Mail Alert** is selected. Or, the system will send out SMS message to the administrator if **SMS message** is selected.

WAN >> WAN Budget



Application Notes

A-1 How to 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
Yes	ADSL		PPPoA
IP	GW IP	TX Packets	TX Rate(Bps)
---	---	0	0
WAN 2 Status			>> Drop PPPoE
Enable	Line	Name	Mode
Yes	Ethernet		PPPoE
IP	GW IP	TX Packets	TX Rate(Bps)
118.100.103.153	168.95.192.1	79	3
			Up Time
			0:03:20
		RX Packets	RX Rate(Bps)
		81	9

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

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode	
WAN1		Fiber	PPPoE	Details Page IPv6
WAN3		USB	None	Details Page IPv6

Advanced You can configure DHCP client options here.

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

WAN >> Internet Access ?

WAN 2

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

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

Online Status

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

IPv4 IPv6

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

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

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

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

Diagnostics >> Ping Diagnosis

Ping Diagnosis

IPV4 IPV6

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

Ping through:

Ping IPv6 Address:

Result |

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

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

PPP (Point-to-Point Protocol)

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

WAN >> Internet Access



WAN 2

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

Note:

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

OK

Cancel

TSPC (Tunnel Setup Protocol Client)

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

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

WAN >> Internet Access



WAN 2

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

OK

Cancel

Static IPv6

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

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

WAN >> Internet Access ?

WAN 2

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

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

WAN >> Internet Access ?

WAN 2

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

Static IPv6 Gateway configuration

IPv6 Gateway Address:

WAN Connection Detection

Mode: Always On

Bridge Mode

Enable Bridge Mode

Bridge Subnet: LAN 1

6in4 Static Tunnel

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

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

WAN >> Internet Access



WAN 2

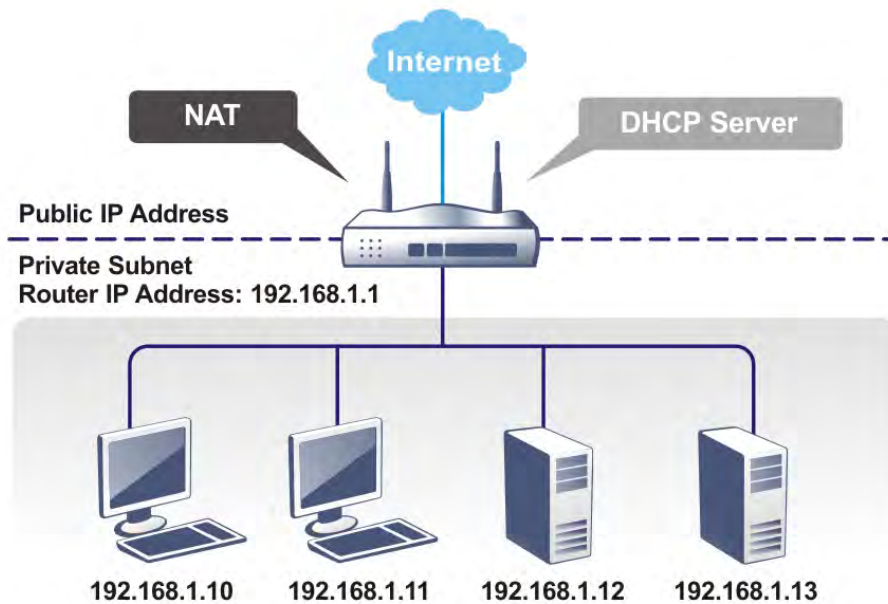
PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
Internet Access Mode			
Connection Type		6in4 Static Tunnel	
6in4 Static Tunnel			
Remote Endpoint IPv4 Address		216.211.221.16	
6in4 IPv6 Address		2001:47c:1b:836::2 / 64 (default:64)	
LAN Routed Prefix		2001:47c:1b:836:: / 64 (default:64)	
Tunnel TTL		255 (default:255)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

OK Cancel

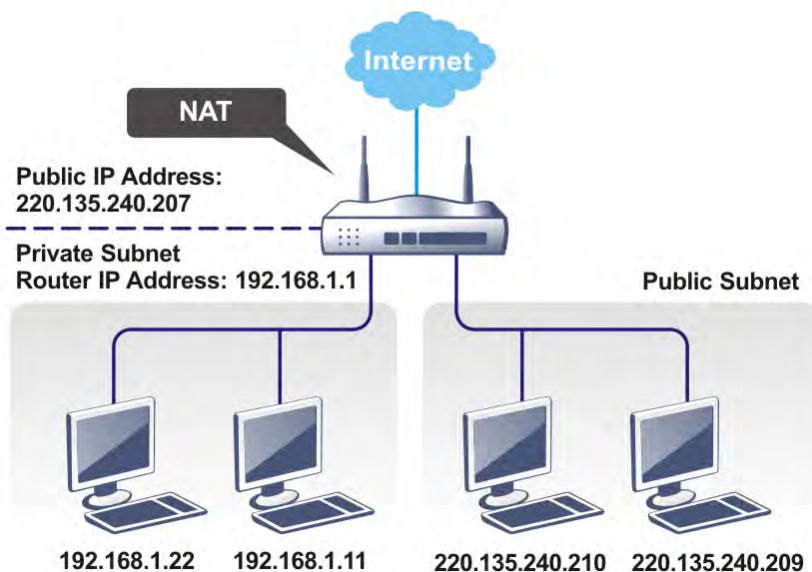
II-2 LAN

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

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



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



What is Routing Information Protocol (RIP)

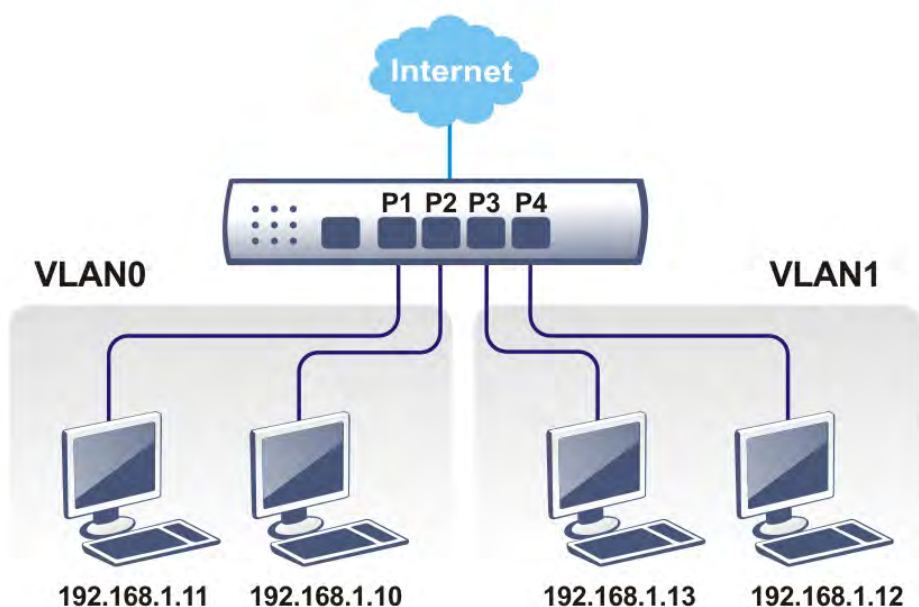
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

What is Static Route

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

What are Virtual LANs and Rate Control

You can group local hosts by physical ports and create up to 8 virtual LANs. To manage the communication between different groups, please set up rules in Virtual LAN (VLAN) function and the rate of each.



Web User Interface

A LAN comprises a collection of LAN clients, which are networked devices on your premises. A LAN client can be a computer, a printer, a Voice-over-IP (VoIP) phone, a mobile phone, a gaming console, an Internet Protocol Television (IPTV), etc, and can have either a wired (using Ethernet cabling) or wireless (using Wi-Fi) network connection.

LAN clients within the same LAN are normally able to communicate with one another directly, as they are peers to one another, unless measures, such as firewalls or VLANs, have been put in place to restrict such access. Nowadays the most common LAN firewalls are implemented on the LAN client itself. For example, Microsoft Windows since Windows XP and Apple OS X have built-in firewalls that can be configured to restrict traffic coming in and going out of the computer. VLANs, on the other hand, are usually set up using network switches or routers.

To communicate with the hosts outside of the LAN, LAN clients have to go through a network gateway, which in most cases is a router that sits between the LAN and the ISP network, which is the WAN. The router acts as a director to ensure traffic between the LAN and the WAN reach their intended destinations.



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

LAN >> General Setup

General Setup

Index	Enable	DHCP	DHCPv6	IP Address		
LAN 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.1.1	Details Page	IPv6
LAN 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.2.1	Details Page	IPv6
LAN 3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.3.1	Details Page	IPv6
LAN 4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.4.1	Details Page	IPv6
IP Routed Subnet	<input type="checkbox"/>	<input checked="" type="checkbox"/>		192.168.0.1	Details Page	

[DHCP Server Option](#)

Note:

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

Enable DMZ port will make the LAN Port 1 neglect the setting on VLAN page, LAN Port 1 will become the DMZ Port.

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

Inter-LAN Routing

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

[OK](#)

Available settings are explained as follows:

Item	Description
General Setup	<p>Allow to configure settings for each subnet respectively.</p> <p>Index - Display all of the LAN items.</p> <p>Status- Basically, LAN1 status is enabled in default. LAN2 -LAN4 and IP Routed Subnet can be observed by checking the box of Status.</p> <p>DHCP- LAN1 is configured with DHCP in default. If required, please check the DHCP box for each LAN.</p> <p>IP Address - Display the IP address for each LAN item. Such information is set in default and you can not modify it.</p> <p>Details Page - Click it to access into the setting page. Each LAN will have different LAN configuration page. Each LAN must be configured in different subnet.</p> <p>IPv6 - Click it to access into the settings page of IPv6.</p>
DHCP Server Option	<p>DHCP packets can be processed by adding option number and data information when such function is enabled.</p> <p>For detailed information, refer to later section.</p>
Force router to use "DNS server IP address"	<p>Force Vigor router to use DNS servers configured in LAN1/LAN2/LAN3/LAN4 instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).</p>
Inter-LAN Routing	<p>Check the box to link two or more different subnets (LAN and LAN).</p> <p>Inter-LAN Routing allows different LAN subnets to be interconnected or isolated.</p>

It is only available when the VLAN functionality is enabled. Refer to section II-2-2 VLAN on how to set up VLANs. In the Inter-LAN Routing matrix, a selected checkbox means that the 2 intersecting LANs can communicate with each other.
--

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



Info

To configure a subnet, select its Details Page button to bring up the LAN Details 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
<p>Network Configuration For NAT Usage</p> <p>IP Address <input type="text" value="192.168.1.1"/></p> <p>Subnet Mask <input type="text" value="255.255.255.0"/></p> <hr/> <p>RIP Protocol Control <input type="text" value="Disable"/></p>	<p>DHCP Server Configuration</p> <p><input type="radio"/> Disable <input checked="" type="radio"/> Enable Server <input type="radio"/> Enable Relay Agent</p> <p>Start IP Address <input type="text" value="192.168.1.10"/></p> <p>IP Pool Counts <input type="text" value="200"/> (max. 253)</p> <p>Gateway IP Address <input type="text" value="192.168.1.1"/></p> <p>Lease Time <input type="text" value="86400"/> (s)</p> <p><input checked="" type="checkbox"/> Clear DHCP lease for inactive clients periodically</p> <hr/> <p>DNS Server IP Address</p> <p>Primary IP Address <input type="text"/></p> <p>Secondary IP Address <input type="text"/></p>

Available settings are explained as follows:

Item	Description
Network Configuration	<p>For NAT Usage,</p> <p>IP Address - This is the IP address of the router. (Default: 192.168.1.1).</p> <p>Subnet Mask - The subnet mask, together with the IP Address field, indicates the maximum number of clients allowed on the subnet. (Default: 255.255.255.0/ 24).</p> <p>RIP Protocol Control,</p> <p>Enable - When Enabled, the router will attempt to exchange routing information with neighbouring routers using the Routing Information Protocol.</p>
DHCP Server Configuration	<p>DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatches related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.</p> <p>If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.</p> <p>Disable Server - Let you manually assign IP address to every host in the LAN.</p> <p>Enable Server - Let the router assign IP address to every host in the LAN.</p> <ul style="list-style-type: none"> ● Start IP Address - The beginning LAN IP address that is given out to LAN DHCP clients. ● IP Pool Counts - The maximum number of IP addresses to be handed out by DHCP. The default value is 200. Valid range is between 1 and 253. The actual number of IP addresses available for assignment is the IP Pool

Counts, or 253 minus the last octet of the Start IP Address, whichever is smaller.

- **Gateway IP Address** - The IP address of the gateway, which is the host on the LAN that relays all traffic coming into and going out of the LAN. The gateway is normally the router, and therefore the Gateway IP Address should be identical to the IP Address in the **Network Configuration** section above.
- **Lease Time** - The maximum duration DHCP-issued IP addresses can be used before they have to be renewed.
- **Clear DHCP lease for inactive clients periodically** - If selected, the router sends ARP requests recycles IP addresses previously assigned to inactive DHCP clients to prevent exhaustion of the IP address pool.

Note: When Clear DHCP lease for inactive clients periodically is enabled, router will do the following:

- Check activities of DHCP clients by ARP requests every minute when the available DHCP IP addresses are less than 30
- Clear DHCP lease when the client is not responding ARP replies.

Enable Relay Agent - When selected, all DHCP requests are forwarded to a DHCP server outside of the LAN subnet, and whose address is specified in the DHCP Server IP Address field.

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

DNS Server IP Address

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

Primary IP Address -You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server.

Secondary IP Address - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server.

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

Online Status

Physical Connection		System Uptime: 22:22:45	
IPv4	IPv6		
LAN Status	Primary DNS: 8.8.8.8	Secondary DNS: 8.8.4.4	
IP Address	TX Packets	RX Packets	
192.168.1.1	0	41533	

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

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

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

Private IP addresses can be assigned automatically to LAN clients using Dynamic Host Configuration Protocol (DHCP), or manually assigned. The DHCP server can either be the router (the most common case), or a separate server, that hands out IP addresses to DHCP clients.

Alternatively, static IP addresses can be manually configured on LAN clients as part of their network settings. No matter how IP addresses are configured, it is important that no two devices get the same IP address. If both DHCP and static assignment are used on a network, it is important to exclude the static IP addresses from the DHCP IP pool. For example, if your LAN uses the 192.168.1.x subnet and you have 20 DHCP clients and 20 static IP clients, you could configure 192.168.1.10 as the Start IP Address, 50 as the IP Pool Counts (enough for the current number of DHCP clients, plus room for future expansion), and use addresses greater than 192.168.1.100 for static assignment.

II-2-1-2 Details Page for LAN2 ~ LAN4

LAN >> General Setup

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

OK

Available settings are explained as follows:

Item	Description
Network Configuration	<p>Enable/Disable - Click Enable to enable such configuration; click Disable to disable such configuration.</p> <p>For NAT Usage - Click this radio button to invoke NAT function.</p> <p>For Routing Usage - Click this radio button to invoke this function.</p> <p>IP Address - This is the IP address of the router. (Default: 192.168.1.1).</p> <p>Subnet Mask - The subnet mask, together with the IP Address field, indicates the maximum number of clients allowed on the subnet. (Default: 255.255.255.0/ 24).</p>
DHCP Server Configuration	<p>DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.</p> <p>Disable Server - Let you manually assign IP address to every</p>

	<p>host in the LAN.</p> <p>Enable Server - Let the router assign IP address to every host in the LAN.</p> <ul style="list-style-type: none"> ● Start IP Address - The beginning LAN IP address that is given out to LAN DHCP clients. ● IP Pool Counts - The maximum number of IP addresses to be handed out by DHCP. The default value is 100. Valid range is between 1 and 253. The actual number of IP addresses available for assignment is the IP Pool Counts, or 253 minus the last octet of the Start IP Address, whichever is smaller. ● Gateway IP Address - The IP address of the gateway, which is the host on the LAN that relays all traffic coming into and going out of the LAN. The gateway is normally the router, and therefore the Gateway IP Address should be identical to the IP Address in the Network Configuration section above. ● Lease Time - The maximum duration DHCP-issued IP addresses can be used before they have to be renewed. ● Clear DHCP lease for inactive clients periodically - If selected, the router sends ARP requests recycles IP addresses previously assigned to inactive DHCP clients to prevent exhaustion of the IP address pool. <p>Note: When Clear DHCP lease for inactive clients periodically is enabled, router will do the following:</p> <ul style="list-style-type: none"> ■ Check activities of DHCP clients by ARP requests every minute when the available DHCP IP addresses are less than 30 ■ Clear DHCP lease when the client is not responding ARP replies. <p>Enable Relay Agent - When selected, all DHCP requests are forwarded to a DHCP server outside of the LAN subnet, and whose address is specified in the DHCP Server IP Address field.</p> <ul style="list-style-type: none"> ● DHCP Server IP Address - It is available when Enable Relay Agent is checked. Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.
<p>DNS Server IP Address</p>	<p>DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.</p> <p>Primary IP Address -You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server.</p> <p>Secondary IP Address - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server.</p> <p>The default DNS Server IP address can be found via Online Status:</p>

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

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

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

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

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

LAN >> General Setup

TCP/IP and DHCP Setup for IP Routed Subnet

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

Available settings are explained as follows:

Item	Description
Network Configuration	<p>Enable/Disable - Click Enable to enable such configuration; click Disable to disable such configuration.</p> <p>For Routing Usage,</p> <p>IP Address - This is the IP address of the router. (Default: 192.168.1.1).</p> <p>Subnet Mask - The subnet mask, together with the IP Address field, indicates the maximum number of clients allowed on the subnet. (Default: 255.255.255.0/ 24).</p> <p>RIP Protocol Control,</p> <p>Enable - When Enabled, the router will attempt to exchange routing information with neighbouring routers using the</p>

	Routing Information Protocol.
DHCP Server Configuration	<p>DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.</p> <p>If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.</p> <p>Start IP Address - The beginning LAN IP address that is given out to LAN DHCP clients.</p> <p>IP Pool Counts - The maximum number of IP addresses to be handed out by DHCP. The default value is 100. Valid range is between 1 and 253. The actual number of IP addresses available for assignment is the IP Pool Counts, or 253 minus the last octet of the Start IP Address, whichever is smaller.</p> <p>Gateway IP Address - The IP address of the gateway, which is the host on the LAN that relays all traffic coming into and going out of the LAN. The gateway is normally the router, and therefore the Gateway IP Address should be identical to the IP Address in the Network Configuration section above.</p> <p>Lease Time - The maximum duration DHCP-issued IP addresses can be used before they have to be renewed.</p> <p>Use LAN Port - Specify an IP for IP Route Subnet. If it is enabled, DHCP server will assign IP address automatically for the clients coming from P1 and/or P2. Please check the box of P1 and P2.</p> <p>Use MAC Address - Check such box to specify MAC address.</p> <ul style="list-style-type: none"> ● MAC Address: Enter the MAC Address of the host one by one and click Add to create a list of hosts which can be assigned, deleted or edited from above pool. Set a list of MAC Address for 2nd DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2nd subnet won't get an IP address belonging to 1st subnet. <p>Add - Type the MAC address in the boxes and click this button to add.</p> <p>Delete - Click it to delete the selected MAC address.</p> <p>Edit - Click it to edit the selected MAC address.</p> <p>Cancel - Click it to cancel the job of adding, deleting and editing.</p>

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

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

There are two configuration pages for each LAN. 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

Off ▾ / 64

Current IPv6 Address Table

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

DNS Server IPv6 Address Deploy when WAN is up ▾

Primary DNS Server

Secondary DNS Server

Management SLAAC(stateless) ▾

Other Option(O-bit)

DHCPv6 Server

Enable Server Disable Server

Auto IPv6 range

Start IPv6 Address

End IPv6 Address

Advance setting Edit

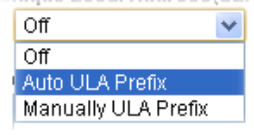
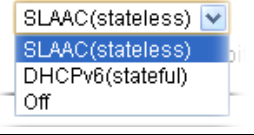
Advance setting
Edit

OK

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

Available settings are explained as follows:

Item	Description
Enable	Check the box to enable the configuration of LAN 1 IPv6 Setup.
WAN Primary Interface	Use the drop down list to specify a WAN interface for IPv6.
Static IPv6 Address configuration	IPv6 Address -Type static IPv6 address for LAN. Prefix Length - Type the fixed value for prefix length. Add - Click it to add a new entry.

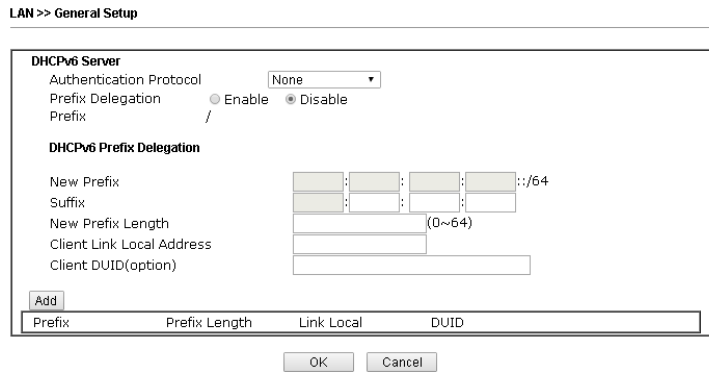
	Delete - Click it to remove an existed entry.
Unique Local Address (ULA) configuration	<p>Unique Local Addresses (ULAs) are private IPv6 addresses assigned to LAN clients.</p> <p>Off - ULA is disabled.</p> <p>Manually ULA Prefix - LAN clients will be assigned ULAs generated based on the prefix manually entered.</p> <p>Auto ULA Prefix - LAN clients will be assigned ULAs using an automatically-determined prefix.</p> 
Current IPv6 Address Table	Display current used IPv6 addresses.
DNS Server IPv6 Address	<p>Deploy when WAN is up - The RA (router advertisement) packets will be sent to LAN PC with DNS server information only when network connection by any one of WAN interfaces is up.</p> <p>Enable - The RA (router advertisement) packets will be sent to LAN PC with DNS server information no matter WAN connection is up or not.</p> <ul style="list-style-type: none"> ● Primary DNS Sever - Type the IPv6 address for Primary DNS server. ● Secondary DNS Server -Type another IPv6 address for DNS server if required. <p>Disable - DNS server will not be used.</p>
Management	<p>Configures the Managed Address Configuration flag (M-bit) in Route Advertisements.</p> <ul style="list-style-type: none"> ● Off - No configuration information is sent using Route Advertisements. ● SLAAC(stateless) - M-bit is unset. ● DHCPv6(stateful) - M-bit is set, which indicates to LAN clients that they should acquire all IPv6 configuration information from a DHCPv6 server. The DHCPv6 server can either be the one built into the Vigor2860, or a separate DHCPv6 server. 
Other Option(O-bit)	<p>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.</p> <p>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.</p>
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.

Disable Server -Click it to disable DHCPv6 server.

Auto IPv6 range - After check the box, Vigor router will assign the IPv6 range automatically.

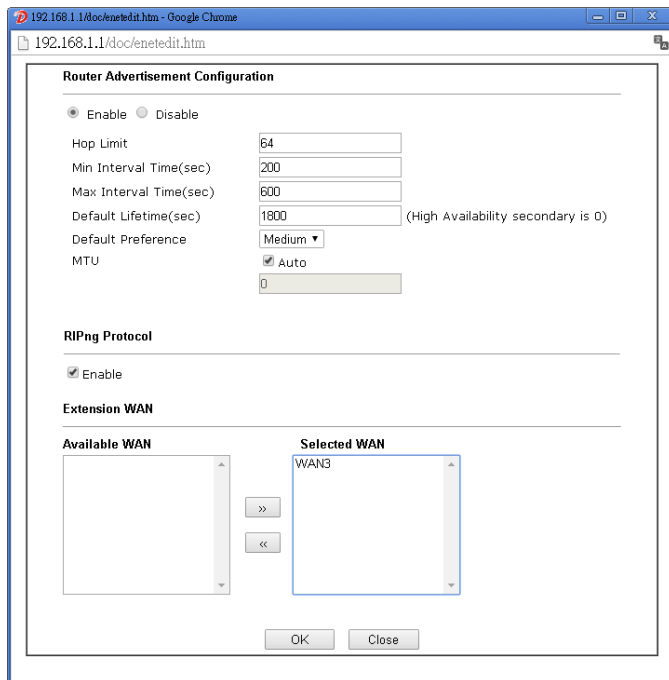
Start IPv6 Address / End IPv6 Address -Type the start and end address for IPv6 server.

Advance setting - Click the Edit button to configure advanced IPv6 settings for DHCPv6 server.



Advance setting

The Advanced Settings page has additional settings for Router Advertisement and enabling multiple WANs for IPv6 traffic.



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

Disable - Click it to disable router advertisement server.

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

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

Default Lifetime (sec) -Within such period of time, Vigor2133 can be treated as the default gateway.

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

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

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

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

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

Selected WAN - Additional WANs selected to carry IPv6 traffic.

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

II-2-1-5 Advanced DHCP Options

DHCP Options can be configured by clicking the Advanced button on the LAN General Setup screen.

LAN >> General Setup

DHCP Server Customized Status

Customized List				
Enable	Interface	Option	Type	Data

Enable:

Interface: All LAN1 LAN2 LAN3 LAN4 IP Routed Subnet

Next Server IP Address/SIAddr :

Option Number:

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

Data:

Note:

1. Configuring options 44, 46 or 66 here will overwrite the settings by telnet command "msubnet".
2. Configuring option 3 here will overwrite the setting in "LAN >> General Setup" Details Page's "Gateway IP Address" field.
3. Configuring option 15 here will overwrite the setting in "WAN >> Internet Access >> Static or Dynamic IP" Detail Page's "Domain Name" field.

Available settings are explained as follows:

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

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

Virtual Local Area Networks (VLANs) allow you to subdivide your LAN to facilitate management or to improve network security.

Select LAN>>VLAN from the menu bar of the Web UI to bring up the VLAN Configuration page.

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 Vigor2133ac:

LAN >> VLAN Configuration

VLAN Configuration

Enable

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

Permit untagged device in P1 to access router

Note:

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

OK Clear Cancel

**Info**

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

Available settings are explained as follows:

Item	Description
Enable	Click it to enable VLAN configuration.
LAN	P1 - P4- Check the LAN port(s) to group them under the selected VLAN.
Wireless LAN (2.4GHz)	SSID1 - SSID4 - Check the SSID boxes to group them under the selected VLAN.
Wireless LAN (5GHz)	SSID1 - SSID4 - Check the SSID boxes to group them under the selected VLAN. This option is only available for Vigor2133ac.
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 form 0 to 4095. VIDs must be unique. Priority - Valid values are from 0 to 7, where 1 has the lowest priority, followed by 0, and finally from 2 to 7 in increasing order of priority.
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.

The Vigor router supports up to 8 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).

Inter-LAN Routing

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

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.

Vigor2133 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. Check the boxes according to the statement in step 1 and Step 2.

LAN >> VLAN Configuration

VLAN Configuration

Enable

	LAN				Wireless LAN(2.4GHz)				Wireless LAN(5GHz)				Subnet	VLAN Tag		
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	SSID1	SSID2	SSID3	SSID4		Enable	VID	Priority
VLAN0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LAN 2	<input type="checkbox"/>	0	0
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1 LAN 2	<input type="checkbox"/>	0	0
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 3 LAN 4	<input type="checkbox"/>	0	0
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0

Permit untagged device in P1 to access router

Note:

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

OK Clear Cancel

4. Click OK.

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

LAN >> General Setup

General Setup

Index	Status	DHCP	DHCPv6	IP Address		
LAN 1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	192.168.1.1	Details Page	IPv6
LAN 2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.2.1	Details Page	IPv6
LAN 3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.3.1	Details Page	IPv6
LAN 4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.4.1	Details Page	IPv6
IP Routed Subnet	<input type="checkbox"/>	<input checked="" type="checkbox"/>		192.168.0.1	Details Page	

Advanced You can configure DHCP server options here.

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

Inter-LAN Routing

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

Note:

LAN2/3/4 are available when VLAN is enabled.

OK

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



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. With the Bind IP to MAC feature you can reserve LAN IP addresses for LAN clients. Each reserved IP address is associated with a Media Access Control (MAC) address.

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

Bind IP to MAC

Enable Disable
 Strict Bind

Apply Strict Bind to Subnet:

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

IP Address	Mac Address	HOST ID
192.168.1.110	00-05-5D-E4-D8-EE	A1000351

IP Address:
 Mac Address: -----
 Comment:

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

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

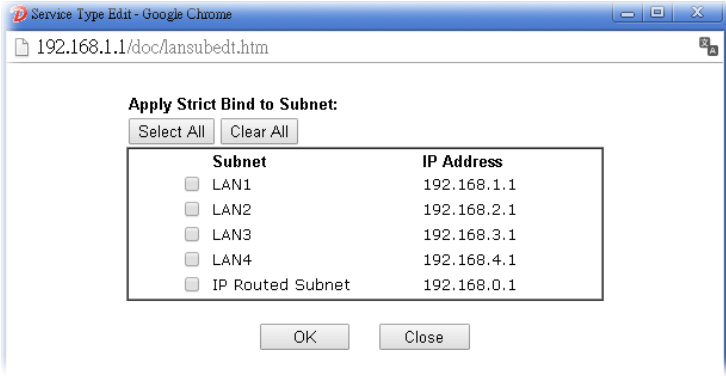
Backup IP Bind List :
 Upload From File: 未選擇任何檔案

Note:

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

Available settings are explained as follows:

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

<p>Strict Bind</p>	<p>Check the box to block the connection of the IP/MAC which is not listed in IP Bind List.</p> <p>LAN clients will be assigned IP addresses according to the MAC-to-IP address associations on this page. LAN client whose MAC address has not been bound to an IP address will be denied network access.</p> <p>Note: Before selecting Strict Bind, make sure at least one valid MAC address has been bound to an IP address. Otherwise no LAN clients will have network access, and it will not be possible to connect to the router to make changes to its configuration.</p> <p>Apply Strict Bind to Subnet – Choose the subnet(s) for applying the rules of Bind IP to MAC.</p> 
<p>ARP Table</p>	<p>This table is the LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking Add below.</p>
<p>Select All</p>	<p>Select all entries in the ARP Table for manipulation.</p>
<p>Sort</p>	<p>Reorder the entry based on the IP address.</p>
<p>Refresh</p>	<p>Refresh the ARP table listed below to obtain the newest ARP table information.</p>
<p>Add / Update to IP Bind List</p>	<p>IP Address – Type the IP address to be associated with a MAC address.</p> <p>Mac Address – Type the MAC address of the LAN client’s network interface.</p> <p>Comment – Type a brief description for the entry.</p> <p>Add - It allows you to add the one you choose from the ARP table or the IP/MAC address typed in Add and Edit to the table of IP Bind List.</p> <p>Update - It allows you to edit and modify the selected IP address and MAC address that you create before.</p> <p>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.</p>
<p>IP Bind List</p>	<p>It displays a list for the IP bind to MAC information.</p>
<p>Backup IP Bind List</p>	<p>Click Backup and enter a filename to back up IP Bind List to a file.</p>
<p>Upload From File</p>	<p>Click Browse... to select an IP Bind List backup file. Click Restore to restore the backup and overwrite the existing list.</p>



Info

Before you select Strict Bind, you have to bind one set of IP/MAC address for one PC. If not, no one of the PCs can access into Internet. And the web user interface of the router might not be accessed.

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

II-2-4 LAN Port Mirror

The LAN Port Mirror function allows network traffic of select LAN ports to be forwarded to another LAN port for analysis. This is useful for enforcing policies, detecting unauthorized access, monitoring network performance, etc.

Select LAN>>LAN Port Mirror from the menu bar of the Web UI to bring up the LAN Port Mirror configuration page.

LAN >> LAN Port Mirror

LAN Port Mirror

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

Note:

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

OK

Available settings are explained as follows:

Item	Description
Port Mirror	Enables or disables LAN Port Mirroring.
Mirror Port	One and only one port is selected as the mirror port, to which traffic is to be forwarded.
Mirrored Tx Port	Port(s) whose outbound traffic will be forwarded to the mirror port.
Mirrored Rx Port	Port(s) whose inbound traffic will be forwarded to the mirror port.

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

II-2-5 Wired 802.1x

Wired 802.1X provides authentication for clients wishing to connect to the LAN by Ethernet. Only one client can be authenticated on each LAN port.

Select **LAN>>Wired 802.1X** from the menu bar of the Web UI to bring up the **Wired 802.1X** configuration page.

LAN >> Wired 802.1X

Wired 802.1X

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

Note:

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

OK

Available settings are explained as follows:

Item	Description
Enable	Check the box to enable LAN 802.1x function.
802.1X ports	802.1X authentication will be available for the selected LAN ports.

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

II-3 Hardware Acceleration

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

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

Hardware Acceleration >> Setup

Mode: ▾

Protocol: TCP UDP

Option: Accelerate heaviest traffic sessions

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

Specific Hosts:

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

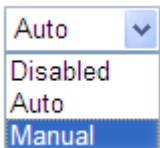
WAN Information:

	Status	TX	RX
WAN1-Ethernet	Enable	V	V

Note:

If Hardware Acceleration is enabled, then individual sessions processed by the accelerator will bypass the following features: Traffic Graph, WAN Budget.

Available settings are explained as follows:

Item	Description
Mode	<p>Disabled - The default setting.</p> <p>Auto - When the hardware acceleration is configured with the Auto mode, the sessions with the heaviest loading and the lower latency traffic will be added into PPA. However, the Auto mode does not support UDP protocol by designed.</p> <p>Manual - The Manual mode implements three sub-items-- <i>Accelerate most heavy traffic sessions</i>, <i>Apply the Class Rule in Quality of Service</i>, and <i>Specific Hosts</i>. Each of these sub-items can support TCP and UDP protocol.</p> 
Protocol	There are two types supported by this function, TCP and UDP.

<p>Option</p>	<p>Accelerate heaviest traffic sessions - Such option is available in Auto Mode, too. But the UDP protocol is only supported in this sub-item.</p> <p>Apply the <u>Class Rule</u> in Quality of Service - Users can apply the information provided by QoS in this sub-item.</p> <p>Please visit our website for referring the detailed configuration of QoS.</p> <p>Bandwidth Management >> Quality of Service</p> <hr/> <p>Rule Edit</p> <div style="border: 1px solid gray; padding: 5px;"> <input checked="" type="checkbox"/> ACT <input checked="" type="checkbox"/> Hardware Acceleration Ethernet Type <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 Local Address <input type="text" value="Any"/> Remote Address <input type="text" value="Any"/> </div> <p>Specific Hosts - This sub-item provides 5 hosts for adding NAT sessions into the PPA. For the PPA only supports 128 sessions, these hosts will share these sessions. Therefore, the performance will be lower than only one host.</p> <p>Choose this option to specify certain PCs on LAN to apply the hardware acceleration.</p> <ul style="list-style-type: none"> ● Enable - Check the box to make PC(s) specified in the selected index entry to be applied. ● Dest Port Start - Type the starting port for the PC(s) in LAN. ● Dest Port End - Type the ending port for the PC(s) in LAN. ● Private IP/Choose PC - Type the IP address as the selected host. Or click the Choose PC button to specify one IP address from the pop-up window.
---------------	--

Checking the PPA status

For checking whether the rule of PPA is working or not, a user can login to Vigor2133 series by using telnet. User can view how many sessions are transferring in each direction of PPA table after entering "ppa -v".

```

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

```

II-4 NAT

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

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

The benefit of the NAT includes:

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



Info

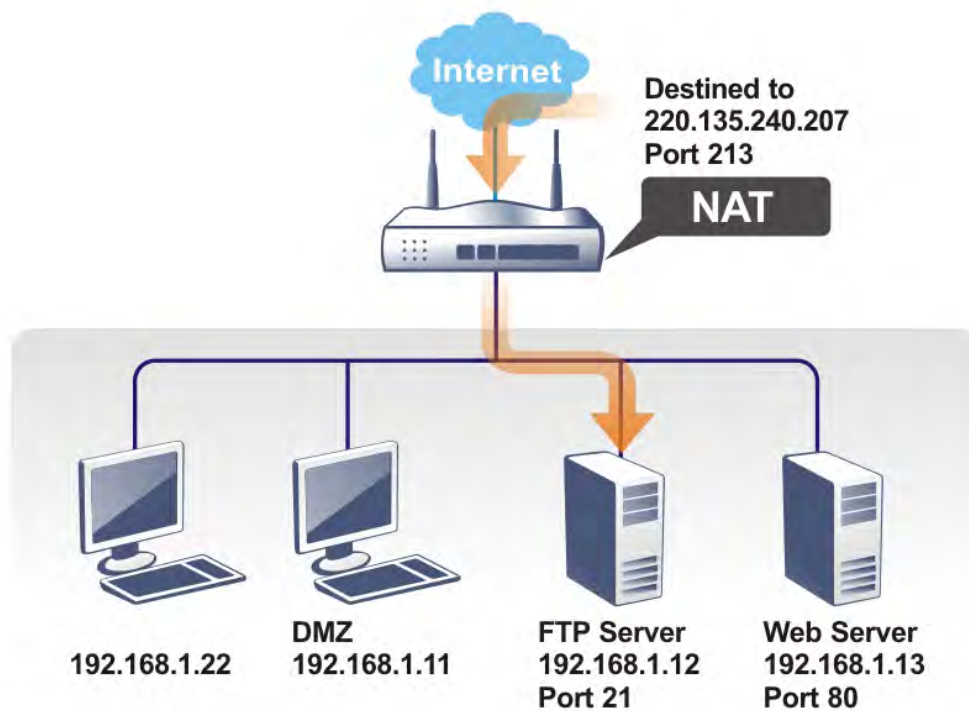
On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by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

Web User Interface



II-4-1 Port Redirection

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



The port redirection can only apply to incoming traffic.

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

NAT >> Port Redirection

Port Redirection							Set to Factory Default
Index	Service Name	WAN Interface	Protocol	Public Port	Source IP	Private IP	Status
1.		All			Any		x
2.		All			Any		x
3.		All			Any		x
4.		All			Any		x
5.		All			Any		x
6.		All			Any		x
7.		All			Any		x
8.		All			Any		x
9.		All			Any		x
10.		All			Any		x

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

Note:

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

Each item is explained as follows:

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

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

NAT >> Port Redirection

Index No. 1

<input type="checkbox"/> Enable	
Mode	Single ▾
Service Name	Single <input type="text"/>
Protocol	TCP ▾
WAN Interface	ALL ▾
Public Port	0 <input type="text"/>
Source IP	Any ▾ IP Object
Private IP	<input type="text"/>
Private Port	0 <input type="text"/>

Note:

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

Available settings are explained as follows:

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

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

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

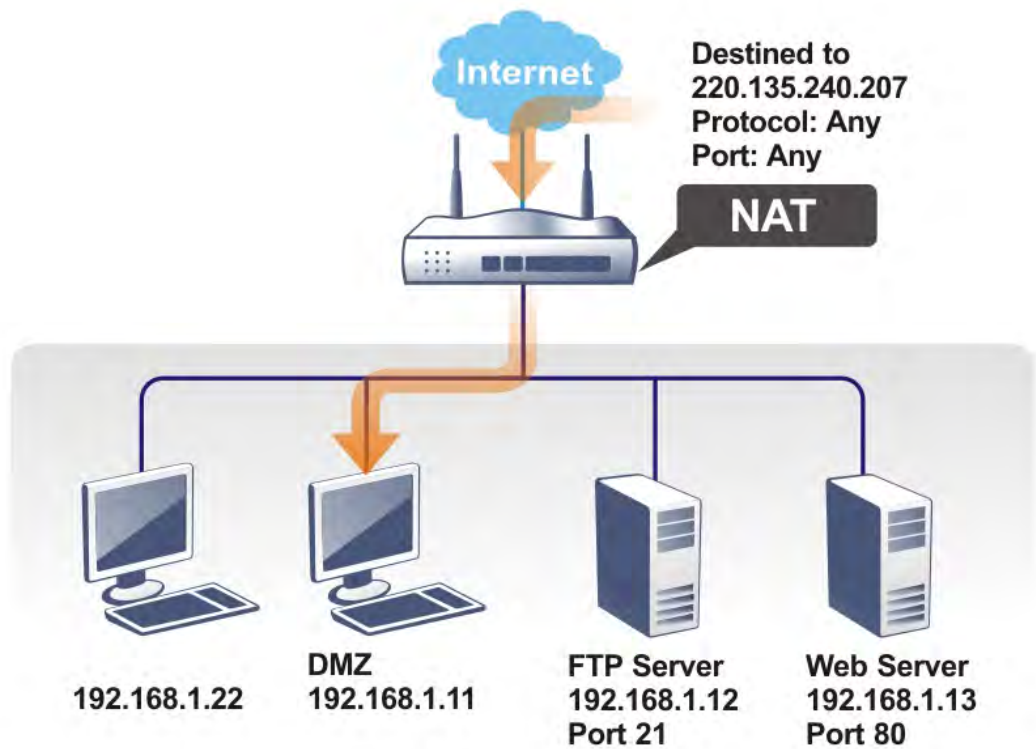
For example, the built-in web user interface in the router is with default port 80, which may conflict with the web server in the local network, `http://192.168.1.13:80`. Therefore, you need to **change the router's http port to any one other than the default port 80** to avoid conflict, such as 8080.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



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

II-4-2 DMZ Host

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



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

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

NAT >> DMZ Host Setup

DMZ Host Setup

WAN1

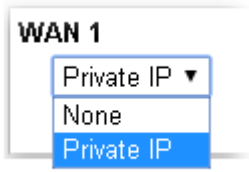
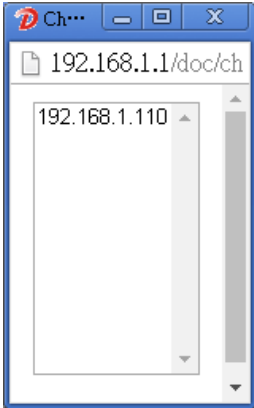
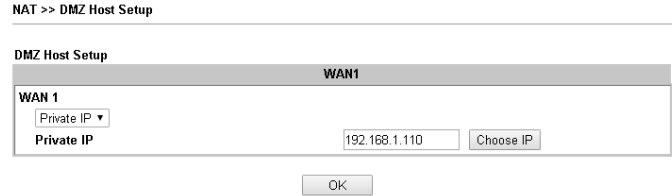
WAN 1

Private IP ▾

Private IP Choose IP

OK

Available settings are explained as follows:

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

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

NAT >> DMZ Host Setup

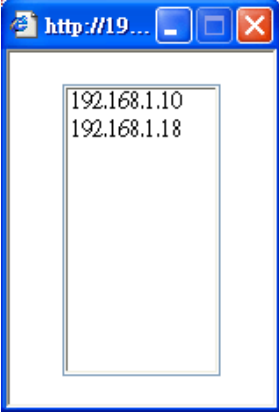
DMZ Host Setup

WAN1

WAN 1		Aux. WAN IP	Private IP	
Index	Enable			
1.	<input type="checkbox"/>	---	0.0.0.0	Choose IP
2.	<input type="checkbox"/>	192.168.1.56	0.0.0.0	Choose IP

Available settings are explained as follows:

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

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

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

II-4-3 Open Ports

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

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

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

NAT >> Open Ports

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

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

Note:

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

Available settings are explained as follows:

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

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

NAT >> Open Ports >> Edit Open Ports

Index No. 1

<input checked="" type="checkbox"/> Enable Open Ports							
Comment		<input type="text" value="TEST"/>					
WAN Interface		<input type="text" value="WAN1"/>					
WAN IP		<input type="text" value="192.168.1.56"/>					
Source IP		<input type="text" value="1 - CARRIE"/> IP Object					
Private IP		<input type="text"/> <input type="button" value="Choose IP"/>					
	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	<input type="text" value="TCP/UDP"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	2.	<input type="text" value="TCP/UDP"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
3.	<input type="text" value="TCP/UDP"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	4.	<input type="text" value="TCP/UDP"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
5.	<input type="text" value="TCP/UDP"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	6.	<input type="text" value="TCP/UDP"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
7.	<input type="text" value="TCP/UDP"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	8.	<input type="text" value="TCP/UDP"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
9.	<input type="text" value="TCP/UDP"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	10.	<input type="text" value="TCP/UDP"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

Available settings are explained as follows:

Item	Description
Enable Open Ports	Check to enable this entry.
Comment	Make a name for the defined network application/service.
WAN Interface	Specify the WAN interface that will be used for this entry.
WAN IP	Choose an IP address from the WAN IP alias.
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 IP to select one. Choose IP - Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select the appropriate IP address of the local host in the list.
Protocol	Specify the transport layer protocol. It could be TCP, UDP, or ----- (none) for selection.
Start Port	Specify the starting port number of the service offered by the local host.
End Port	Specify the ending port number of the service offered by the local host.

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

NAT >> Open Ports

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

Index	Comment	WAN Interface	Aux. WAN IP	Source IP	Local IP Address	Status
<u>1.</u>	TEST	WAN1	192.168.1.56		192.168.1.110	v
<u>2.</u>				Any		x
<u>3.</u>				Any		x
<u>4.</u>				Any		x
<u>5.</u>				Any		x
<u>6.</u>				Any		x
<u>7.</u>				Any		x
<u>8.</u>				Any		x
<u>9.</u>				Any		x
<u>10.</u>				Any		x

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

Note:

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

II-4-4 Port Triggering

Port Triggering is a variation of open ports function.

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

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

TCP: 86400 sec.

UDP: 180 sec.

IGMP: 10 sec.

TCP WWW: 60 sec.

TCP SYN: 60 sec.

NAT >> Port Triggering

Port Triggering							Set to Factory Default
Index	Comment	Triggering Protocol	Source IP	Triggering Port	Incoming Protocol	Incoming Port	Status
1.							x
2.							x
3.							x
4.							x
5.							x
6.							x
7.							x
8.							x
9.							x
10.							x

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

[Next](#) >>

Available settings are explained as follows:

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

Click the index number link to open the configuration page.

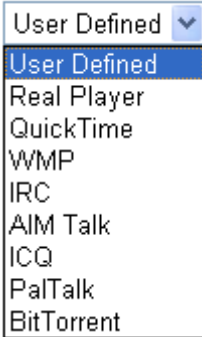
NAT >> Port Triggering

No. 1

<input type="checkbox"/> Enable	
Service	User Defined ▾
Comment	<input type="text"/>
Source IP	Any ▾ IP Object
Triggering Protocol	--- ▾
Triggering Port	<input type="text"/>
Incoming Protocol	--- ▾
Incoming Port	<input type="text"/>
Note: The Triggering Port and Incoming Port should be input like this : 123-456,777-789 (legal),123-456,789 (legal), but 123-456-789 (illegal).	

OK Clear Cancel

Available settings are explained as follows:

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

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

II-4-5 ALG

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

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

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

NAT >> ALG

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

Enable ALG

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

Available settings are explained as follows:

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

II-5 Applications

Dynamic DNS

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

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

LAN DNS / DNS Forwarding

The LAN DNS lets the network administrators host servers with privacy and security. When the network administrators of your office set up FTP, Mail or Web server inside LAN, you can specify specific private IP address (es) to correspondent servers. Thus, even the remote PC is adopting public DNS as the DNS server, the LAN DNS resolution on Vigor2133 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-5-1 Dynamic DNS

Enable the Function and Add a Dynamic DNS Account

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

Applications >> Dynamic DNS Setup

Dynamic DNS Setup | [Set to Factory Default](#) |

Enable Dynamic DNS Setup [View Log](#) [Force Update](#)

Auto-Update interval Min(s) (180~14400)

Accounts:

Index	Enable	Domain Name
<u>1.</u>	<input type="checkbox"/>	
<u>2.</u>	<input type="checkbox"/>	
<u>3.</u>	<input type="checkbox"/>	
<u>4.</u>	<input type="checkbox"/>	
<u>5.</u>	<input type="checkbox"/>	
<u>6.</u>	<input type="checkbox"/>	

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 this account.
Domain Name	Display the domain name that you set on the setting page of DDNS setup.

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

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

Index : 1

Enable Dynamic DNS Account

WAN Interface: WAN1 First

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

Service Type: Dynamic

Domain Name: chronic5563.dyndns.org dyndns.org

Login Name: chronic5563 (max. 64 characters)

Password:

Wildcards

Backup MX

Mail Extender: _____

Determine WAN IP: WAN IP

OK Clear Cancel

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

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

Index : 1

Enable Dynamic DNS Account

WAN Interface: WAN1 First

Service Provider: User-Defined ?

Provider Host: changeip.org

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

Auth Type: basic

Connection Type: Http

Server Response: _____

Login Name: chronic5563 (max. 64 characters)

Password:

Wildcards

Backup MX

Mail Extender: _____

Determine WAN IP: WAN IP

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
Service Provider	Select the service provider for the DDNS account.
Provider Host	Type the IP address or the domain name of the host which provides related service. Note that such option is available when Customized is selected as Service Provider.
Service API	Type the API information obtained from DDNS server. Note that such option is available when Customized is selected as Service Provider. (e.g: /dynamic/dns/update.asp?u=jo***&p=jo*****&hostname=j***.changeip.org&ip=###IP### &cmd=update&offline=0)
Auth Type	Two types can be used for authentication. Basic - Username and password defined later can be shown from the packets captured. URL - Username and password defined later can be shown in URL. (e.g. , http://ns1.vigorddns.com/ddns.php?username=xxxx&password=xxxx&domain=xxxx.vigorddns.com) Note that such option is available when Customized is selected as Service Provider.
Connection Type	There are two connection types (HTTP and HTTPS) to be specified. Note that such option is available when Customized is selected as Service Provider.
Server Response	Type any text that you want to receive from the DDNS server. Note that such option is available when Customized is selected as Service Provider.
Login Name	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.
Wildcard and Backup MX	The Wildcard and Backup MX (Mail Exchange) features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.
Mail Extender	If the mail server is defined with another name, please type the name in this area. Such mail server will be used as backup mail exchange.
Determine WAN IP	If a Vigor router is installed behind any NAT router, you can enable such function to locate the real WAN IP. When the WAN IP used by Vigor router is private IP, this function can detect the public IP used by the NAT router and use the detected IP address for DDNS update. There are two methods offered for you to choose: <ul style="list-style-type: none"> ● WAN IP - If it is selected and the WAN IP of Vigor router is private, DDNS update will take place right away. ● Internet IP - If it is selected and the WAN IP of Vigor router is private, it will be converted to public IP

	before DDNS update takes place.
--	---------------------------------

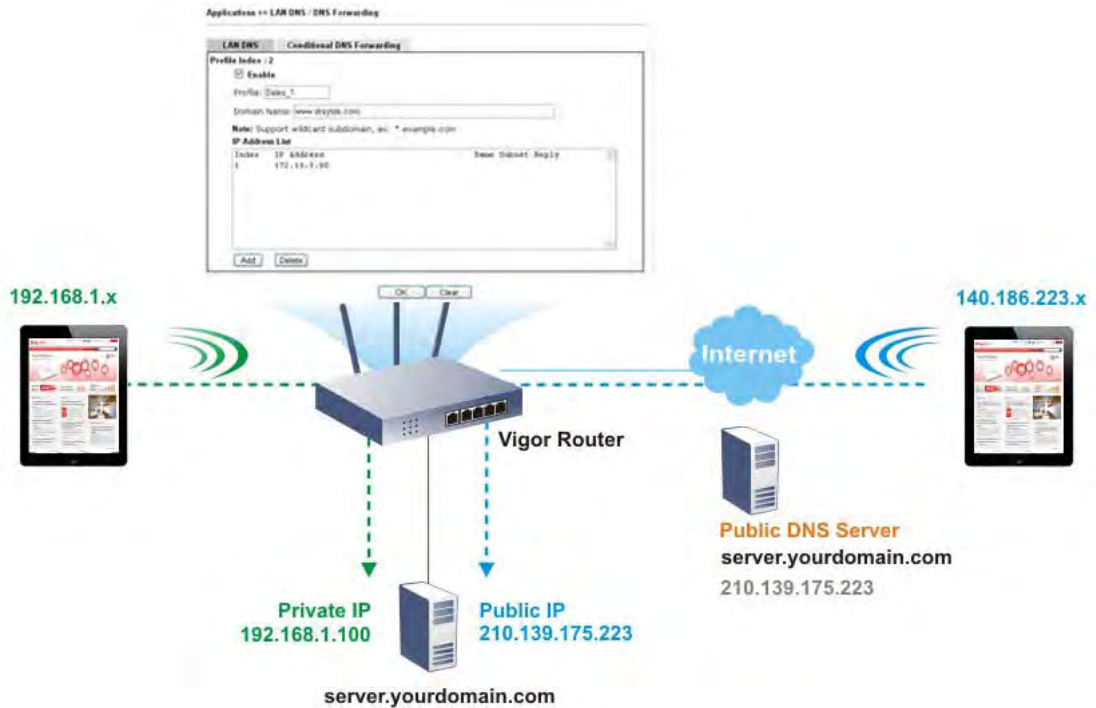
5. Click **OK** button to activate the settings. You will see your setting has been saved.

Disable the Function and Clear all Dynamic DNS Accounts

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

II-5-2 LAN DNS / DNS Forwarding

The LAN DNS lets the network administrators host servers with privacy and security. When the network administrators of your office set up FTP, Mail or Web server inside LAN, you can specify specific private IP address (es) to correspondent servers. Thus, even the remote PC is adopting public DNS as the DNS server, the LAN DNS resolution on Vigor2133 series will respond the specified private IP address.



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

Applications >> LAN DNS / DNS Forwarding

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

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

Each item is explained as follows:

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

Profile	Display the name of the LAN DNS profile.
Domain Name	Display the domain name of the LAN DNS profile.
Forwarding	Display that such profile is conditional DNS forwarding or not.
DNS Server	Display the IP adres of the DNS Server.

You can set up to 120 LAN DNS profiles.

To create a LAN DNS profile:

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

Applications >> LAN DNS / DNS Forwarding

LAN DNS
Conditional DNS Forwarding

Profile Index : 1

Enable

Profile:

Domain Name:

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

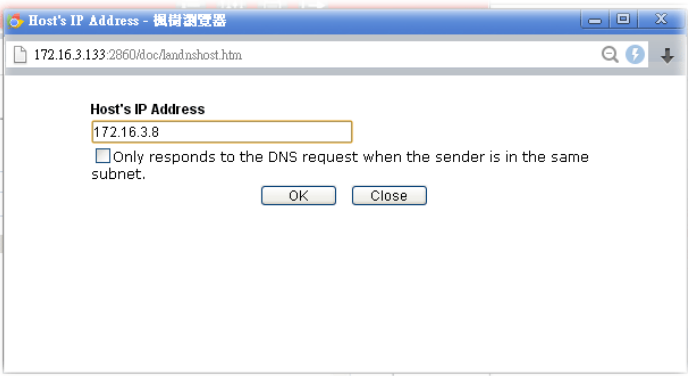
CNAME(Alias Domain Name):

IP Address List

Index	IP Address	Same Subnet	Reply

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable such profile.
Profile	Type a name for such profile. Note: If you type a name here for LAN DNS and click OK to save the configuration, the name also will be applied to conditional DNS forwarding automatically.
Domain Name	Type the domain name for such profile.
IP Address List	The IP address listed here will be used for mapping with the domain name specified above. In general, one domain name maps with one IP address. If required, you can configure two IP addresses mapping with the same domain name. Add - Click it to open a dialog to type the host's IP address.



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

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

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

Applications >> LAN DNS / DNS Forwarding

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

Available settings are explained as follows:

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

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

II-5-3 DNS Security

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

II-5-3-1 General Setup

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

Application >> DNS Security



DNS Security

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

Note:

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

OK

Available settings are explained as follows:

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

II-5-3-2 Domain Diagnose

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



DNS Security

General Setup	Domain Diagnose	DNS Cache
Domain:	<input type="text"/>	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Interface:	WAN1 ▾	
DNS Server:	<input type="text"/>	
<input type="button" value="Diagnose"/>		
Note: If the domain has not been queried before, it will take a few seconds to process.		
Result <input type="button" value="Clear"/>		
Domain Name	IP Address	Interface
-----	-----	-----
---		Verify Result

Available settings are explained as follows:

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

II-5-4 Schedule

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

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

Applications >> Schedule

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

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

Force on Force down

Available settings are explained as follows:

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

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

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

To add a schedule:

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

Applications >> Schedule

Index No. 1 Current System Time 2000 Jan 1 Sat 0 : 15 : 36 | **System time set** |

Enable Schedule Setup

Comment

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

Start Time (hh:mm) 0 : 0

Duration Time (hh:mm) 0 : 0

End Time (hh:mm) 00 : 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	Check to enable the schedule.
Comment	Type a short description for such schedule.
Start Date (yyyy-mm-dd)	Specify the starting date of the schedule.
Start Time (hh:mm)	Specify the starting time of the schedule.
Duration Time (hh:mm)	Specify the duration (or period) for the schedule.
End Time (hh:mm)	It will be calculated automatically when Start Time and Duration Time are configured well.

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

3. Click OK button to save the settings.

Example

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

Office
Hour:
(Force On)



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

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

II-5-5 RADIUS

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.

Applications >> RADIUS

RADIUS Setup

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

Note:

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

Available settings are explained as follows:

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

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

II-5-6 UPnP

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



Info

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

Applications >> UPnP

UPnP

- | |
|--|
| <input checked="" type="checkbox"/> Enable UPnP Service |
| <input type="checkbox"/> Enable Connection Control Service |
| <input type="checkbox"/> Enable Connection Status Service |

Note:

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

OK

Clear

Cancel

Available settings are explained as follows:

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

The reminder as regards concern about Firewall and UPnP:

Can't work with Firewall Software

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

Security Considerations

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

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

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

II-5-7 IGMP

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

II-5-7-1 General Setting

Applications >> IGMP

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

Available settings are explained as follows:

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

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

II-5-7-1 Working Group

Applications >> IGMP

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

Available settings are explained as follows:

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

II-5-8 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

Wake by:

IP Address:

MAC Address: : : : : :

Result

Note:

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

Available settings are explained as follows:

Item	Description
Wake by	Two types provide for you to wake up the binded IP. <ul style="list-style-type: none"> ● If you choose Wake by MAC Address, you have to type the correct MAC address of the host in MAC Address boxes. ● If you choose Wake by IP Address, you have to choose the correct IP address.
IP Address	The IP addresses that have been configured in Firewall>>Bind IP to MAC will be shown in this drop down list. Choose the IP address from the drop down list that you want to wake up.
MAC Address	Type any one of the MAC address of the bound PCs.
Wake Up	Click this button to wake up the selected IP. See the following figure. The result will be shown on the box.

II-5-9 SMS / Mail Alert Service

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

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

II-5-9-1 SMS Alert

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

Applications >> SMS / Mail Alert Service

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

Note:

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

Available settings are explained as follows:

Item	Description
Index	Check the box to enable such profile.
SMS Provider	Use the drop down list to choose SMS service provider. You can click SMS Provider link to define the SMS server.
Recipient 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-5-9-2 Mail Alert

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

Application >> SMS / Mail Alert Service

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

Note:

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

OK Cancel

Available settings are explained as follows:

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

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

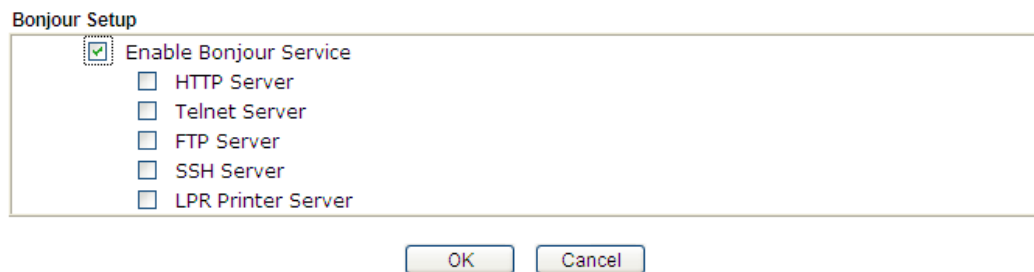
II-5-10 Bonjour

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.

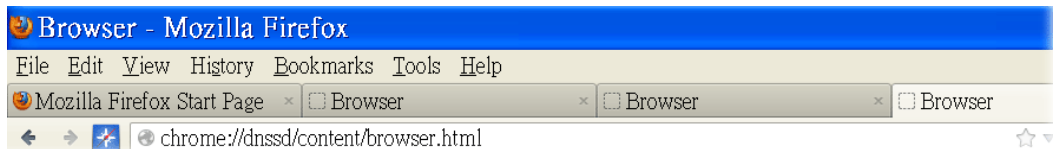
To enable the Bonjour service, click **Application>>Bonjour** to open the following page. Check the box(es) of the server service(s) that you want to share to the LAN clients.

Applications >> Bonjour

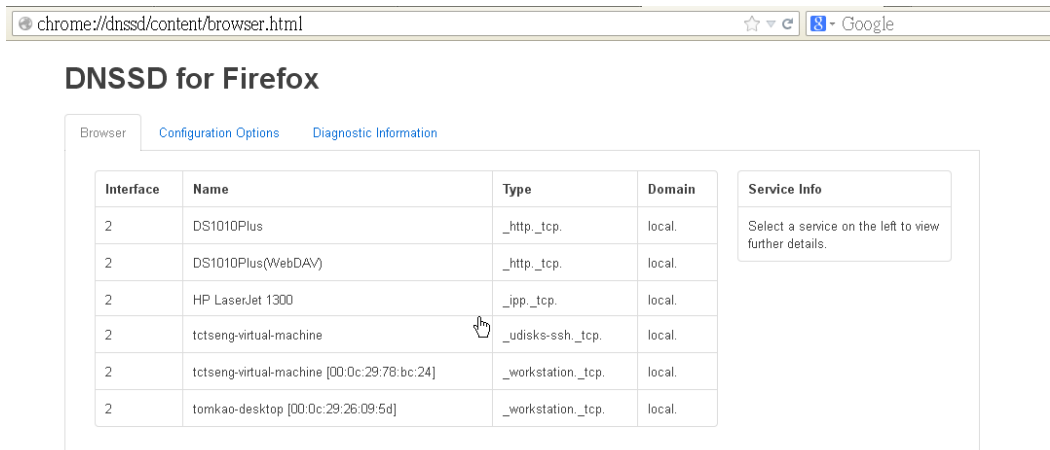


Below shows an example for applying the Bonjour feature that Vigor router can be used as the FTP server.

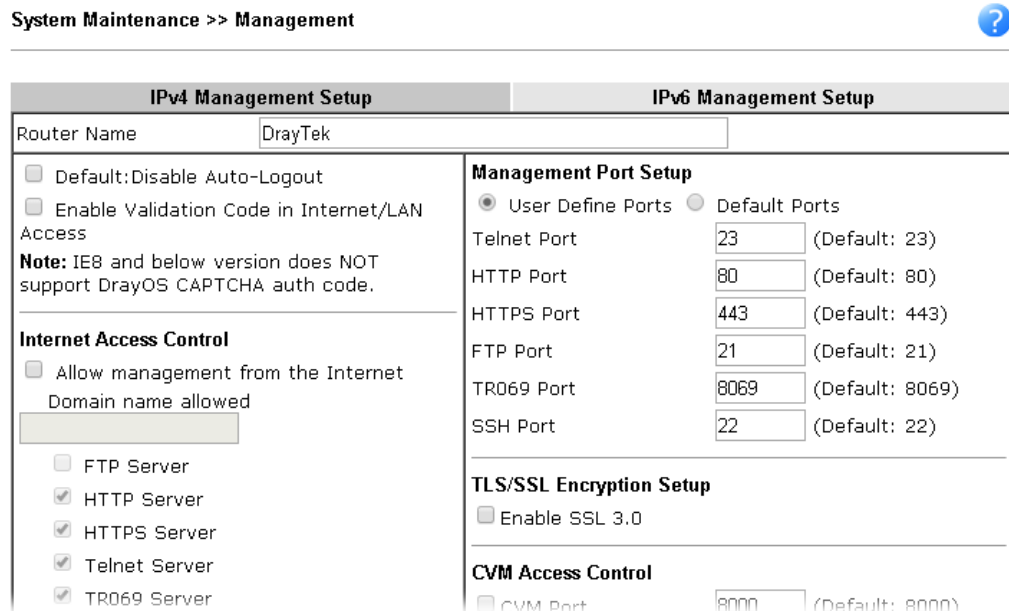
1. Here, we use Firefox and DNSSD to discover the service in such case. Therefore, just ensure the Bonjour client program and DNSSD for Firefox have been installed on the computer.



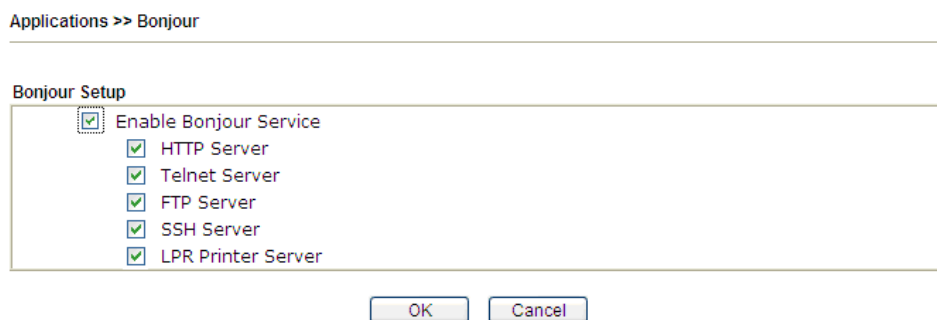
- Open the web browser, Firefox. If Bonjour and DNSSD have been installed, you can open the web page (DNSSD) and see the following results.



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



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



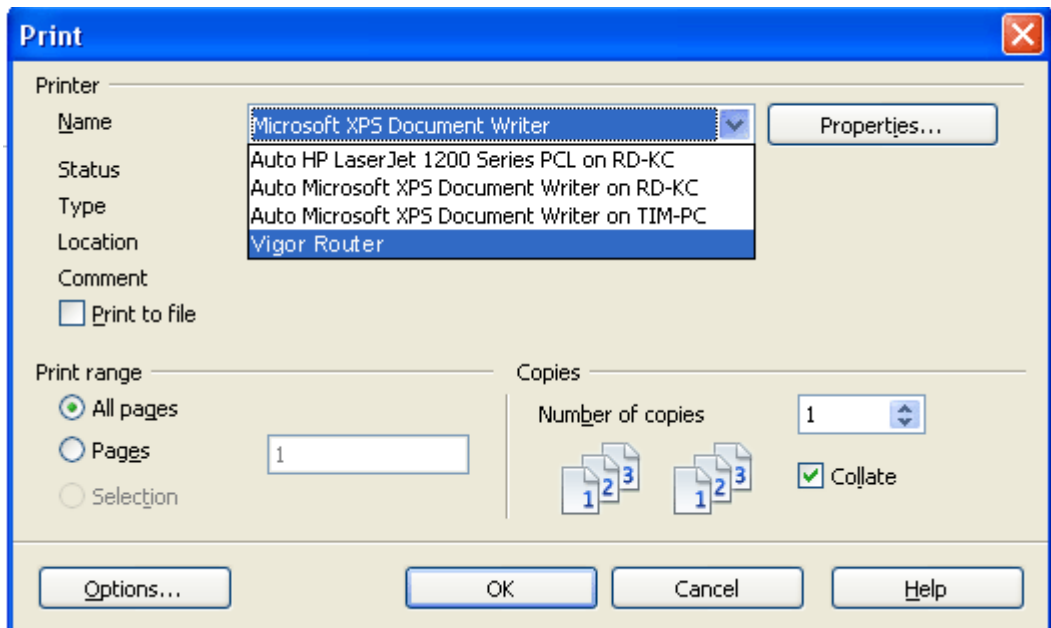
- Open the DNSSD page again. The available items will be changed as the follows. It means the Vigor router (based on Bonjour protocol) is ready to be used as a printer server, FTP server, SSH Server, Telnet Server, and HTTP Server.

DNSSD for Firefox

Browser Configuration Options Diagnostic Information

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

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



Application Notes

A-1 How to use DrayDDNS?

Vigor router supports various DDNS service providers, user can set up user-defined profile to update the DDNS even the service provider is not on the list. Now, DrayTek starts to support our own DDNS service - DrayDDNS. We will provide a domain name for each Vigor Router, this single domain name can record IP addresses of all WAN.

Activate DrayDDNS License

1. Go to **Wizards >> Service Activation Wizard**, wait for the router to connect to MyVigor server, then tick **DT-DDNS** and **I have read and accept the above Agreement**, click **Next**.

Service Activation Wizard

Select the service type that you want to activate

Activation Date : 2017-02-23

Web Content Filter(WCF) Service :

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

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

APP Enforcement(APPE) Service :

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

Dynamic DNS(DDNS) Service :

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

*** Please note that the DrayDDNS service is currently for internal use only.**

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

2. Confirm the information, then click **Activate**.

Service Activation Wizard

Please confirm your settings

Service Type : Trial version
Service Activated : Dynamic DNS (.draydns.com)

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

- MyVigor server will reply with the service activation information.

DrayTek Service Activation

Service Name	Start Date	Expire Date	Status
Web Content filter	---	---	Not Activated
APP Enforcement	---	---	Not Activated
DDNS	2017-02-23	2018-02-23	DT-DDNS

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

Configure DDNS Profile

- Go to Applications >> Dynamic DNS Setup,
 - Tick Enable Dynamic DNS Setup
 - Click an available profile index
 - Tick Enable Dynamic DNS Account
 - Select DrayTek Global (www.drayddns.com) as Service Provider
 - Select the WAN you would like to upload the IP to DDNS server
 - Click Get domain
 - Click OK on the pop up notification window

Applications >> Dynamic DNS Setup

Dynamic DNS Setup | Set to Factory Default |

Enable Dynamic DNS Setup View Log Force Update

Auto-Update interval 1440 Min(s) (180~14400)

Accounts:

Index	WAN Interface
1.	WAN1 Only
2.	WAN1 First
3.	WAN1 First
4.	WAN1 First
5.	WAN1 First
6.	WAN1 First

OK

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

Index : 2

Enable Dynamic DNS Account

Service Provider DrayTek Global (www.drayddns.com)

Status Activated [Start Date:2017-02-23 Expire Date:2018-02-23]

Domain Name .drayddns.com Get domain

Determine Real WAN IP WAN IP

Determine WAN IP

- WAN 1
- WAN 2
- WAN 3
- WAN 4

OK Clear Cancel

192.168.193.10 says:

Note: Router will automatically get the domain name from MyVigor server.
Please kindly wait for a while, then check the config again.

Prevent this page from creating additional dialogs.

OK

- Wait few seconds for router to get the domain name, then, we can click the profile to check the information of license and domain name.

Applications >> Dynamic DNS Setup

Dynamic DNS Setup | Set to Factory Default |

Enable Dynamic DNS Setup View Log Force Update

Auto-Update interval Min(s) (180~14400)

Accounts:

Index	WAN Interface	Domain Name	Active
1.	WAN1 Only	Customized	v
2.	WAN 1/2/3/4	115.100.154.drayddns.com	v
3.	WAN1 First		x
4.	WAN1 First		
5.	WAN1 First		
6.	WAN1 First		

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

Index : 2

Enable Dynamic DNS Account

Service Provider

Status **Activated** [Start Date:2017-02-23 Expire Date:2018-02-23]

Domain Name

Determine Real WAN IP

Determine WAN IP

OK Clear Cancel

Modify Domain Name

Currently, only the domain name is allowed to be modified MyVigor website. We will need to register the router to MyVigor server, and log in to MyVigor website to modify it.

- Please visit <https://myvigor.draytek.com/> or go to Applications >> Dynamic DNS Setup >> DrayDDNS profile and click Edit domain.

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

Index : 2

Enable Dynamic DNS Account

Service Provider

Status **Activated** [Start Date:2017-02-23 Expire Date:2018-02-23]

Domain Name

Determine Real WAN IP

Determine WAN IP

OK Clear Cancel

- Log in to MyVigor Website, choose the profile, then click Edit DDNS settings.

My Information - My Products

Device Information

Device Name: 115.100.154
Serial Number: 115.100.154
Model: Vigor2133 Series

Rename Transfer Back

Device's Service Expired License

Service	Provider	Action	Status	Start Date	Expired Date	Note
WCF	BPJM	Activate	On	-	-	-
WCF	Cyren	Trial	On	-	-	-
APPE	DT-APPE	Activate	On	-	-	-
DDNS	DT-DDNS	Renew	On	2017-02-23	2018-02-23	<input type="button" value="Edit DDNS settings"/>

3. Input the desired Domain name (e.g., XXXX25) and click Update.

Edit DDNS Settings

Please note that the DrayDDNS service is currently for internal use only.

Domain Name	<input type="text" value="XXXX25"/>	<input type="text" value=".draydns.com"/>
Current IP	<input type="text" value="192.168.39.44"/>	<input type="button" value="Get PC's Internet IP"/>
Last Update	2017/2/24 14:27:20	
Status	Update success	
	<input type="button" value="Update"/>	<input type="button" value="Delete"/> <input type="button" value="Reset"/>

4. Vigor router will get the modified domain name when the it performs next DDNS updating. We can click Sync domain to accelerate this process.

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

Index : 2

<input checked="" type="checkbox"/> Enable Dynamic DNS Account		
Service Provider	DrayTek Global (www.draydns.com) ▼	
Status	Activated [Start Date:2017-02-23 Expire Date:2018-02-23]	
Domain Name	<input type="text" value="XXXX25"/>	<input type="text" value=".draydns.com"/> <input type="button" value="Sync domain"/>
WAN Interfaces	WAN IP ▼	
	WAN 1 ▲	
	WAN 2	
	WAN 3	
	WAN 4 ▼	
Determine WAN IP		

After few seconds, the router will get the new domain name and print it on the profiles list.


Applications >> Dynamic DNS Setup

Dynamic DNS Setup | [Set to Factory Default](#) |

Enable Dynamic DNS Setup [View Log](#) [Force Update](#)

Auto-Update interval Min(s) (180~14400)

Accounts:

Index	WAN Interface	Domain Name	Active
1.	WAN1 Only	Customized	v
2.	WAN 1/2/3/4	 draydns.com	v
3.	WAN1 First		x
4.	WAN1 First		x
5.	WAN1 First		x
6.	WAN1 First		x


Applications >> Dynamic DNS Setup

Dynamic DNS Setup | [Set to Factory Default](#) |

Enable Dynamic DNS Setup [View Log](#) [Force Update](#)

Auto-Update interval Min(s) (180~14400)

Accounts:

Index	WAN Interface	Domain Name	Active
1.	WAN1 Only	Customized	v
2.	WAN 1/2/3/4	 25.draydns.com	v
3.	WAN1 First		x
4.	WAN1 First		x
5.	WAN1 First		x
6.	WAN1 First		x

A-2 How to Configure Customized DDNS?

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

Part A : Changeip.org

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

Note that,

Username: jo***

Password: jo*****

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

WAN IP address: 1.169.185.242

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



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

200 Successful Update (Address Used: 1.169.185.242)

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

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

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

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

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

Index : 1

Enable Dynamic DNS Account

Service Provider: User-Defined ?

Provider Host: ChangeIP.org

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

Auth Type: basic

Connection Type: Http

Server Response:

Login Name: chronic6633 (max. 64 characters)

Password: ***** (max. 64 characters)

Wildcards

Backup MX

Mail Extender:

Determine Real WAN IP: WAN IP

OK Clear Cancel

2. Set the Service Provider as **User-Defined**.
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

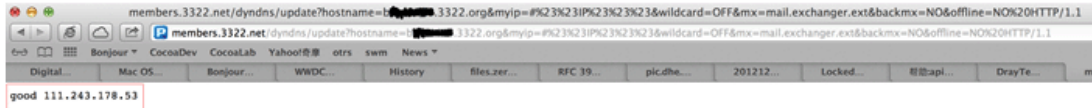
WAN 1	
Link Status	: Connected
MAC Address	: 00-50-7F-C8-C6-A1
Connection	: PPPoE
IP Address	: 111.243.178.53
Default Gateway	: 168.95.98.254
Primary DNS	: 168.95.192.1
Secondary DNS	: 168.95.1.1

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 User-Defined DDNS client.

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

Index : 1

Enable Dynamic DNS Account

Service Provider: User-Defined

Provider Host: member.3322.net

Service API: /dyndns/update?hostname=bi*****.3322.org&myip=###IP###&wildcard=OFF&mx=mail.exchanger.ext&backmx=NO&offline=NO

Auth Type: basic

Connection Type: Http

Server Response:

Login Name: chronic6633 (max. 64 characters)

Password: ***** (max. 64 characters)

Wildcards

Backup MX

Mail Extender:

Determine Real WAN IP: WAN IP

OK Clear Cancel

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

Part C : Extend Note

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



OK

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

Index : 1

Enable Dynamic DNS Account

Service Provider: User-Defined

Provider Host: member3322.net

Service API: /dyn dns/ update?
hostname=bi*****.3322.org&myip=###IP###&wildcard=OFF&mx=mail
.exchanger.ext&backmx= NO&offline=NO

Auth Type: basic

Connection Type: Http

Server Response:

Login Name: chronic6633 (max. 64 characters)

Password: ***** (max. 64 characters)

Wildcards

Backup MX

Mail Extender:

Determine Real WAN IP: WAN IP

OK Clear Cancel

II-6 Routing

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

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

Specify Interface

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

Address Mapping

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

Priority

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

Failover to/Failback

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

Other routing

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



Info

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

Web User Interface



II-6-1 Static Route

Static routing is an alternative to dynamic routing. It is a process that the system network administrator can configure network routers with all the required information for packet forwarding.

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

Static Route for IPv4

Routing >> Static Route Setup

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

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

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 30) under Index allows you to open next page to set up static route.
Enable	Check the box to enable such route.

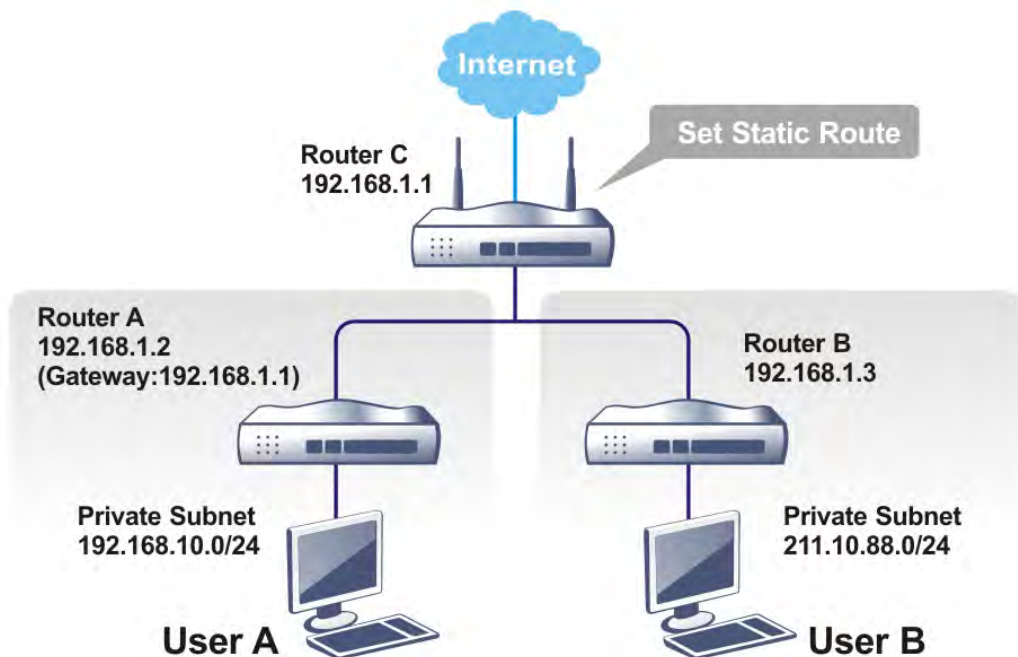
Destination Address	Displays the destination address of the static route.
---------------------	---

Add Static Routes to Private and Public Networks

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

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

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



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



Info

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

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

LAN >> Static Route Setup

Index No. 1

Enable

Destination IP Address: ???

Subnet Mask:

Gateway IP Address:

Network Interface: LAN1

OK Cancel Delete

Available settings are explained as follows:

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

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

LAN >> Static Route Setup

Index No. 1

Enable

Destination IP Address: 211.100.88.0

Subnet Mask: 255.255.255.0

Gateway IP Address: 192.168.1.3

Network Interface: LAN1

OK Cancel Delete

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

Diagnostics >> View Routing Table

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

Static Route for IPv6

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

Routing >> Static Route Setup

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

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

Available settings are explained as follows:

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

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

LAN >> Static Route Setup

Index No. 1

Enable

Destination IPv6 Address / Prefix Len: /

Gateway IPv6 Address:

Network Interface: ▼

Available settings are explained as follows:

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

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

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

II-6-2 Route Policy

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

II-6-2-1 General Setup

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

Routing >> Route Policy



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

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

OK

Available settings are explained as follows:

Item	Description
Index	Click the number of index to access into the configuration web page.
Enable	Check this box to enable this policy.
Comment	Display a brief explanation for this policy.
Protocol	Display the protocol used for this policy.
Interface	Display the interface to send packets to once the policy is matched.
Priority	Display the priority value for such route policy profile.
Src IP Start	Display the IP address for the start of the source IP.
Src IP End	Display the IP address for the end of the source IP.

Dest IP Start	Display the IP address for the start of the destination IP.
Dest IP End	Display the IP address for the end of the destination IP.
Dest Port Start	Display the IP address for the start of the destination port.
Dest Port End	Display the IP address for the end of the destination port.
Move UP/Move Down	Use Up or Down link to move the order of the policy.
Wizard Mode	Allow to configure frequently used (simple and basic) settings of route policy via three setting pages.
Advance Mode	Allow to configure detailed settings of route policy.

To use Wizard Mode, simple do the following steps:

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

Route Policy

Index: 1 Criteria

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

 192.168.1.6 ~ 192.168.1.66

Available settings are explained as follows:

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

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

Routing >> Route Policy

Index: 1 Interface

Route Policy directs the packets to the interface below

Interface

WAN4
LAN1
LAN2
LAN3
LAN4
IP Routed Subnet
WAN1
WAN4

< Back Next > Finish Cancel

Available settings are explained as follows:

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

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

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.

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

Route Policy

Index: 1 Configuration Summary

Criteria

Source IP Any
Destination IP 192.168.1.6 ~ 192.168.1.66

Interface

WAN1

More options

Force NAT

< Back Next > Finish Cancel

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

To use **Advance Mode**, do the following steps:

1. Click the **Advance Mode** radio button.
2. Click any **Index** number link (e.g., 1 in this case) to access into the following page.

Routing >> Route Policy

Index: 1

Enable

Comment

Criteria

Protocol

Source

Destination

Destination Port

Send via if Criteria Matched

Interface WAN/LAN
 VPN

Gateway Default Gateway
 Specific Gateway

Packet Forwarding to WAN via Force NAT
 Force Routing

Failover to WAN/LAN
 VPN
 Route Policy

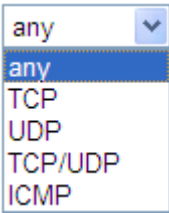
Gateway Default Gateway
 Specific Gateway

Priority

Note:

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

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable this policy.
Comment	Type a brief explanation for such profile.
Protocol	Use the drop-down menu to choose a proper protocol for the WAN interface. 
Source / Destination	<p>Any - Any IP can be treated as the source / destination IP.</p> <p>IP Range - Define a range of IP address as source / destination IP addresses.</p> <ul style="list-style-type: none"> ● Start - Type an address as the starting IP for such profile. ● End - Type an address as the ending IP for such profile.

	<p>IP Subnet - Define a subnet containing IP address and mask address.</p> <ul style="list-style-type: none"> ● Network - Type an IP address here. ● Mask - Use the drop down list to choose a suitable mask for the network. <p>IP Object / IP Group - Choose an IP object / IP group.</p>
Destination Port	<p>Any - Any port number can be treated as the destination port.</p> <p>Dest Port Range - A range of port number can be treated as the destination port.</p> <ul style="list-style-type: none"> ● Start - Type the destination port start for the destination IP. ● End - Type the destination port end for the destination IP. If this field is blank, it means that all the destination ports will be passed through the WAN interface.
Send to if criteria matched	<p>Interface - Use the drop down list to choose a WAN or LAN interface or VPN profile. Packets match with the above criteria will be transferred to the interface chosen here.</p> <p>Gateway IP - Specific gateway is used only when you want to forward the packets to the desired gateway. Usually, Default Gateway is selected in default.</p> <p>Packet Forwarding to WAN via - When you choose WAN (e.g., WAN1) as the Interface for packet transmission, you have to specify the way the packet forwarded to. Choose Force NAT or Force Routing.</p> <p>Failover to - Check this button to lead the data passing through specific interface (WAN/LAN/VPN/Route Policy) automatically when the selected interface (defined in Send via if criteria matched) is down.</p> <ul style="list-style-type: none"> ● WAN/LAN - Use the drop down list to choose an interface as an auto failover interface. ● VPN - Use the drop down list to choose a VPN tunnel as a failover tunnel. ● Route Policy - Use the drop down list to choose an existed route policy profile. <p>Gateway IP - Specific gateway is used only when you want to forward the packets to the desired gateway. Usually, Default Gateway is selected in default.</p>
Priority	<p>Packets will be transmitted based on all routes or Route Policy. Vigor router will determine which rule will be adopted for transmitting the packet according to the priority of Static Route and Route Policy.</p> <p>The greater the value is, the lower the priority is. Default value for route policy is "200" which means it has higher priority than the default route.</p>

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

II-6-2-2 Diagnose

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



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



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

Matched Route

Matched	Priority
N/A	N/A

Matched Policy

Matched	Priority	failovered
Route Policy 1	200	No

close

or

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 未選擇檔案

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

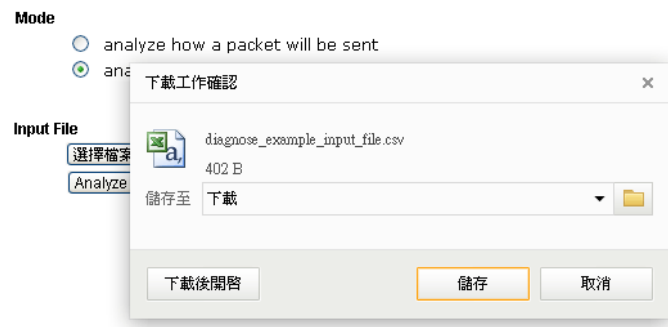
Analyze

Available settings are explained as follows:

Item	Description
Mode	<p>Analyze how a packet will be sent - Choose such mode to make Vigor router analyze how a single packet will be sent by a route policy.</p> <p>Analyze how multiple packets... - Choose such mode to make Vigor router analyze how multiple packets in a specified file will be sent by a route policy.</p>
Packet Information	<p>Specify the nature of the packets to be analyzed by Vigor router.</p> <p>Protocol - Specify a protocol for diagnosis.</p> <p>Src IP - Type an IP address as the source IP.</p> <p>Dst IP - Type an IP address as the destination IP.</p> <p>Dst Port - Use the drop down list to specify the destination port.</p>

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

Input File Select - Click the download link to get a blank example file. Then, click such button to select that blank ".csv" file for saving the result of analysis.



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

Load Balance/Route Policy >> Diagnose

Mode

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

Input File

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

[Analyze](#)

[export analysis](#)

Input Packet Information			Matched Route		Matched Policy		Final Result			
Profile	Proto	Src IP	Dst IP	Dst Port	Route	Priority	Policy	Priority	Interface	Reason
LA-branch	ICMP	192.168.1.10	10.10.10.10	N/A	No Match	N/A	No Match	N/A	N/A	The packet was dropped because neither "route" or "policy" was matched
HR-branch	TCP	192.168.1.20	20.20.20.20	8080	No Match	N/A	No Match	N/A	N/A	The packet was dropped because neither "route" or "policy" was matched
										The packet was dropped because

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

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, the administrator may specify the outgoing IP for certain internal IP address by a Route Policy.

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

192.168.1.1/doc/wipalias.htm

WAN1 IP Alias (Multi-NAT)

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

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

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 **Route Policy>>General Setup**. Create a Route Policy for specific IP address to send from specific WAN IP Address.

Route Policy

Index: 1

Enable

Criteria

Protocol: Any

Source: IP Range

Start: 192.168.1.20 End: 192.168.1.30

Destination: Any

Destination Port: Any

Send via if Criteria Matched

Interface: WAN/LAN (WAN1) VPN

Gateway: Default Gateway (2-172.17.1.1) Specific Gateway (VPN 1.???)

Packet Forwarding to WAN via: Force NAT Force Routing

Failover to: Failover to

WAN/LAN (Default WAN) VPN (VPN 1.???) Route Policy (Index 1)

Gateway: Default Gateway Specific Gateway (0.0.0.0)

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.

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 (2.4 GHz/5 GHz)

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 Vigor2133 wireless series router (with "n", or "ac" in model name) is designed for maximum flexibility and efficiency of a small office/home. Any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access.

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

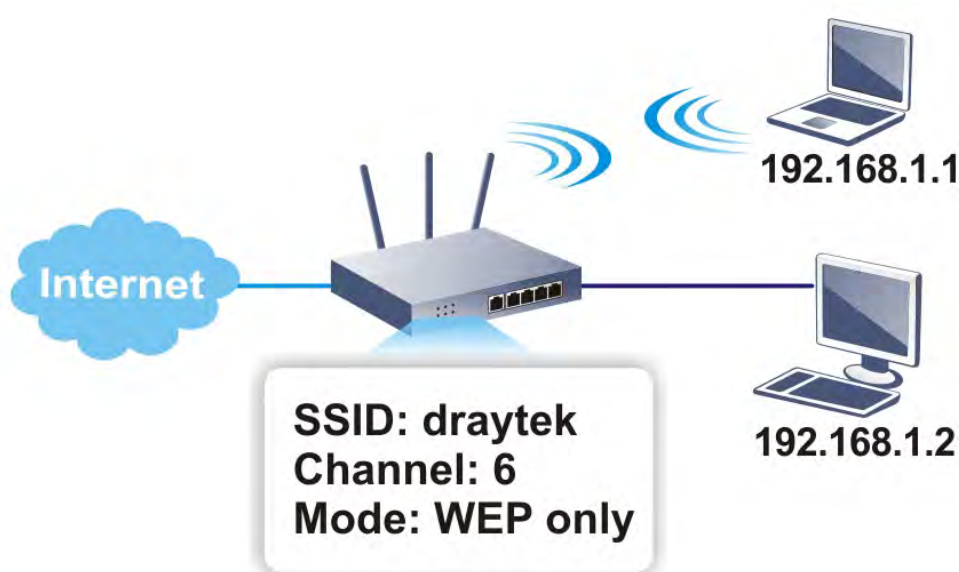
Vigor2133 wireless router is a highly integrated wireless local area network (WLAN) for 5 GHz 802.11ac or 2.4/5 GHz 802.11n WLAN applications. It supports channel operations of 20/40 MHz at 2.4 GHz and 20/40/80 MHz at 5 GHz. Vigor2133 "ac" series router can support data rates up to 1.3 Gbps in 802.11ac 80 MHz channels. Vigor2133 "n" series router supports 802.11n up to 300 Mbps for 40 MHz channel operations.



Info

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

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



Multiple SSIDs

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

Real-time Hardware Encryption

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

Complete Security Standard Selection

To ensure the security and privacy of your wireless communication, we provide several prevailing standards on market.

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

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

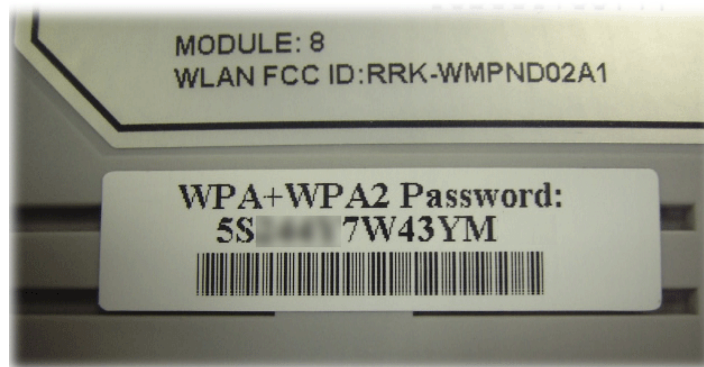
In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

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



Info

The password (PSK) of default security mode is provided and stated on the label pasted on the bottom of the router. For the wireless client who wants to access into Internet through such router, please input the default PSK value for connection.



Separate the Wireless and the Wired LAN- WLAN Isolation

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

Manage Wireless Stations - Station List

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

WPS

WPS (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point (vigor router) with the encryption of WPA and WPA2.



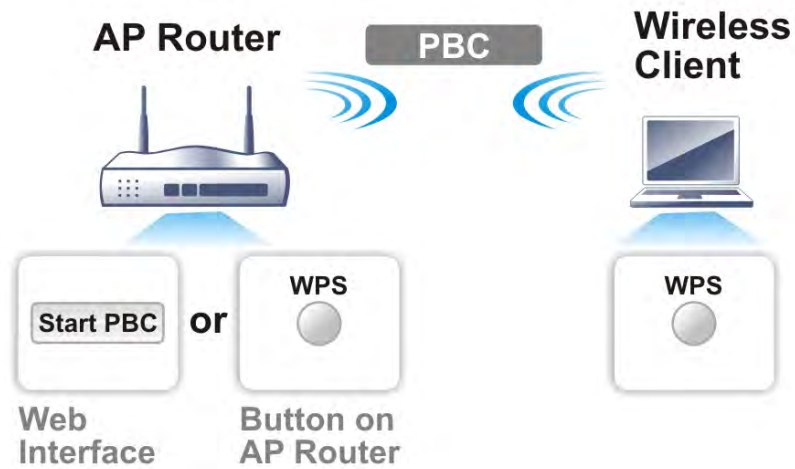
Info

WPS is available for the wireless station with WPS supported.

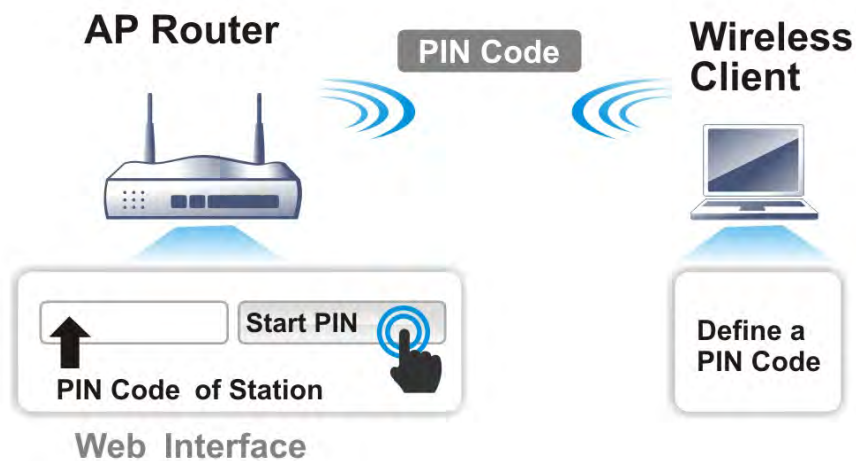
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for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

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

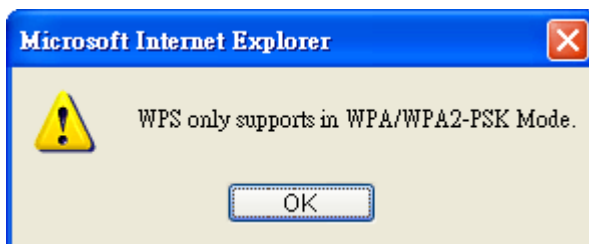
- On the side of Vigor2133 series which served as an AP, press WPS button once on the front panel of the router or click Start PBC on web configuration interface. On the side of a station with network card installed, press Start PBC button of network card.



- If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the vigor router.



For WPS is supported in WPA-PSK or WPA2-PSK mode, if you do not choose such mode in Wireless LAN>>Security, you will see the following message box.



Please click OK and go back Wireless LAN>>Security to choose WPA-PSK or WPA2-PSK mode and access WPS again.

Web User Interface

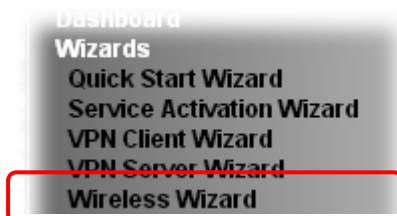


III-1-1 Wireless Wizard

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

Follow the steps listed below:

1. Open Wizards>>Wireless Wizard.



2. The screen of wireless wizard will be shown as follows. This page will be used for internal users in a company or your home. Besides, the settings will change based on different model of Vigor2133 series. In this case, Vigor2133ac is used as an example.

Wireless Wizard

Host AP Configuration

Wireless 2.4GHz Settings	
Name:	<input type="text" value="DrayTek_ian"/>
Mode:	<input type="text" value="Mixed(11b+11g+11n)"/>
Channel:	<input type="text" value="Channel 9, 2452MHz"/>
Security Key:	<input type="text" value="*****"/>
Wireless 5GHz Settings	
<input type="checkbox"/> Use the same SSID and Security Key as above	
Name:	<input type="text" value="DrayTek_5G_ian"/>
Mode:	<input type="text" value="Mixed (11a+11n+11ac)"/>
Channel:	<input type="text" value="Channel 36, 5180MHz"/>
Security Key:	<input type="text" value="*****"/>
Note: The host AP configured here will be used for home or internal company use.	

Available settings are explained as follows:

Item	Description
Name	Type the SSID name of this router for wireless connection. The default name is defined with DrayTek. Change the name if required.
Mode	At present, the router can connect to 11a Only, 11n Only, Mixed (11a+11n), and Mixed (11a+11n+11ac) stations simultaneously. Simply choose Mixed (11a+11n+11ac) mode. <div style="display: flex; justify-content: space-around; margin-top: 10px;"> <div style="border: 1px solid gray; padding: 5px;"> <p>Mixed(11b+11g+11n) ▾</p> <p>11g Only</p> <p>11n Only (2.4 GHz)</p> <p>Mixed(11b+11g)</p> <p>Mixed(11g+11n)</p> <p>Mixed(11a+11n 5 GHz)</p> <p>Mixed(11b+11g+11n)</p> </div> <div style="border: 1px solid gray; padding: 5px;"> <p>DrayTek_5G</p> <p>Mixed (11a+11n+11ac) ▾</p> <p>11a Only</p> <p>11n Only (5 GHz)</p> <p>Mixed (11a+11n)</p> <p>Mixed (11a+11n+11ac)</p> </div> </div>
Channel	Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.
Security Key	The wireless mode offered by this wizard is WPA2/PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
Next	Click it to get into the next setting page.
Cancel	Exit the wireless wizard without saving any changes.

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

Wireless Wizard

Guest AP Configuration

Wireless 2.4GHz Settings

Enable Disable

SSID:

Security Key:

Bandwidth Limit: Enable Total Upload kbps Total Download kbps

Wireless 5GHz Settings

Enable Disable

Use the same SSID and Security Key as above

SSID:

Security Key:

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

Available settings are explained as follows:

Item	Description
Enable/Disable	Click it to enable or disable settings in this page.
SSID	Type the SSID name of this router. (SSID1)
Security Key	The wireless mode offered by this wizard is WPA2/PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
Bandwidth Limit	It controls the data transmission rate through wireless connection. Total Upload - Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps. Total Download - Type the transmitting rate for data download. Default value is 30,000 kbps.
Use the same SSID and Security Key as above	Check the box to use the same settings configured above.
Next	Click it to get into the next setting page.
Cancel	Exit the wireless wizard without saving any changes.

- After typing the required information, click **Next**.

- The following page will display the configuration summary for wireless setting.

Wireless Wizard

Configuration Summary

Wireless 2.4GHz Settings	Wireless 5GHz Settings
Mode: Mixed(11b+11g+11n) Channel: Channel 9, 2452MHz	Mode: Mixed (11a+11n+11ac) Channel: Channel 36, 5180MHz
Host AP SSID Name: DrayTek_Ian Security Key: *****	Host AP SSID Name: DrayTek_5G_Ian Security Key: *****
Guest AP Status: Disabled SSID Name: DrayTek_Guest Security Key: ***** Bandwidth Limit: Disabled	Guest AP Status: Disabled SSID Name: DrayTek_5G_Guest Security Key: *****

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

III-1-2 General Setup

By clicking the **Wireless LAN>>General Setup**, a new web page will appear so that you could configure the SSID and the wireless channel. Please refer to the following figure for more information.

Wireless LAN(2.4 GHz) >> General Setup

General Setting (IEEE 802.11)

Enable Wireless LAN

Mode :

Channel:

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

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

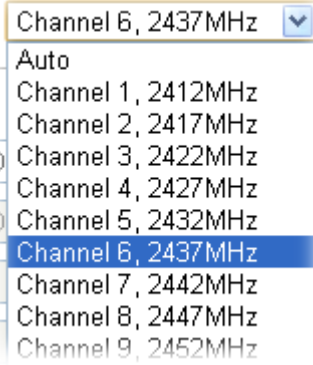
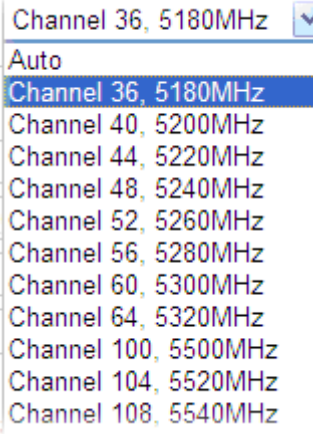
The isolate VPN configuration will isolate the wireless traffic from VPN connections and thus, wireless clients will not be able to access the VPN network under this setting.

Associated **Schedule** Profiles: , , ,

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

Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Mode	<p>For 2.4GHz: At present, the router can connect to 11b Only, 11g Only, 11n Only(2.4 GHz), Mixed (11b+11g), Mixed (11g+11n), and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.</p> <p>For 5GHz: At present, the router can connect to 11a Only, 11n Only (5 GHz), Mixed (11a+11n) and Mixed (11a+11n+11ac) stations simultaneously. Simply choose Mixed (11a+11n+11ac) mode.</p> <div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid gray; padding: 5px;"> <p>Mixed(11b+11g+11n) ▼</p> <p>11b Only</p> <p>11g Only</p> <p>11n Only (2.4 GHz)</p> <p>Mixed(11b+11g)</p> <p>Mixed(11g+11n)</p> <p>Mixed(11b+11g+11n)</p> </div> <div style="border: 1px solid gray; padding: 5px;"> <p>Mixed (11a+11n+11ac) ▼</p> <p>11a Only</p> <p>11n Only (5 GHz)</p> <p>Mixed (11a+11n)</p> <p>Mixed (11a+11n+11ac)</p> </div> </div> <p>Note: 802.11b/g operates on 2.4G band, 802.11a operates on 5G band, 802.11n operates on either 2.4G or 5G band, and 802.11ac operates on 5G band only.</p>

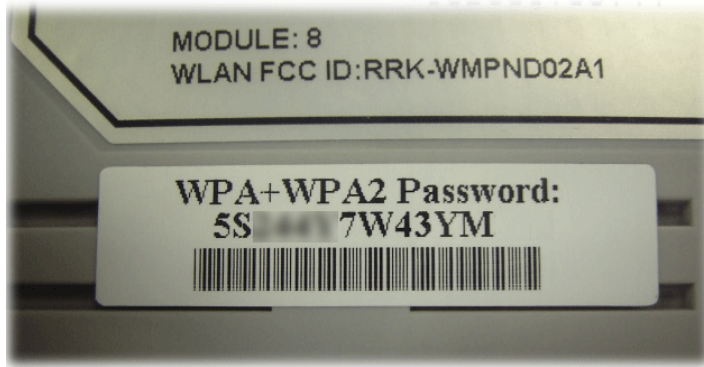
<p>Channel</p>	<p>Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.</p> <p>2.4GHz in "n" model:</p>  <p>5 GHz in "ac" model:</p> 
<p>Hide SSID</p>	<p>Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity.</p>
<p>SSID</p>	<p>Means the identification of the wireless LAN. SSID can be any text numbers or various special characters.</p>
<p>Isolate</p>	<p>Member -Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.</p> <p>VPN - Check this box to make the wireless clients (stations) with different VPN not accessing for each other.</p>
<p>Schedule</p>	<p>Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in Applications >> Schedule setup. The default setting of this field is blank and the function will always work.</p>

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

III-1-3 Security

This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click OK to save and invoke it.

The password (PSK) of default security mode is provided and stated on the label pasted on the bottom of the router. For the wireless client who wants to access into Internet through such router, please input the default PSK value for connection.



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

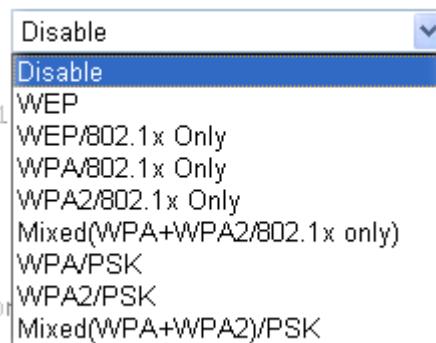
Wireless LAN(5GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
<p>Mode: Mixed(WPA+WPA2)/PSK ▼</p> <p><u>WPA</u></p> <p>Encryption Mode: TKIP for WPA/AES for WPA2</p> <p>Pre-Shared Key(PSK): <input type="text" value="*****"/></p> <p>Password Strength: Weak Medium Strong</p> <p>Strong password requirements:</p> <ol style="list-style-type: none"> 1. Have at least 7 characters, including numbers and letters. 2. Have at least one upper-case letter and one lower-case letter. 3. Including non-alphanumeric characters is a plus. <p>Type 8~63 ASCII character or 64 Hexadecimal digits leading by "0x", for example "cfgs01a2..." or "0x655abcd....".</p> <p><u>WEP</u></p> <p>Encryption Mode: 64-Bit ▼</p> <p><input checked="" type="radio"/> Key 1 : <input type="text" value="*****"/></p> <p><input type="radio"/> Key 2 : <input type="text" value="*****"/></p> <p><input type="radio"/> Key 3 : <input type="text" value="*****"/></p> <p><input type="radio"/> Key 4 : <input type="text" value="*****"/></p> <p>Note:</p> <p>Please configure the RADIUS Server if 802.1X is used.</p> <p>For 64 bit WEP key configurations, please insert 5 ASCII characters or 10 Hexadecimal digits leading by "0x". Examples are "AB312" or "0x4142333132".</p> <p>For 128 bit WEP key configurations, please insert 13 ASCII characters or 26 Hexadecimal digits leading by "0x".</p>			

Enable VigorAP AutoProvision for these settings

Available settings are explained as follows:

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



Info You should also set RADIUS Server simultaneously if 802.1x mode is selected.

Disable - Turn off the encryption mechanism.

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

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

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

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

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

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

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

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

WPA

The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either 8-63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

Pre-Shared Key (PSK) - Either 8-63 ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

Password Strength - The system will display the password strength (represented with the word of weak, medium or strong) of the PSK specified above.

WEP

64-Bit - For 64 bits WEP key, either 5 ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)

128-Bit - For 128 bits WEP key, either 13 ASCII characters,

	<p>such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D).</p> <p>Encryption Mode: 64-Bit ▼ 64-Bit 128-Bit</p> <p>All wireless devices must support the same WEP encryption bit size and have the same key. Four keys can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.</p>
--	---

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

III-1-4 Access Control

In the **Access Control**, the router may restrict wireless access to certain wireless clients only by locking their MAC address into a black or white list. The user may block wireless clients by inserting their MAC addresses into a black list, or only let them be able to connect by inserting their MAC addresses into a white list.

In the **Access Control** web page, users may configure the **white/black** list modes used by each SSID and the MAC addresses applied to their lists.

Wireless LAN(2.4 GHz) >> Access Control

Access Control

Enable Mac Address Filter SSID 1 White List ▼ SSID 2 White List ▼
 SSID 3 White List ▼ SSID 4 White List ▼

MAC Address Filter

Index	Attribute	MAC Address	Apply SSID
<div style="border: 1px solid black; min-height: 80px;"></div>			

Client's MAC Address : : : : : :

Apply SSID : SSID 1 SSID 2 SSID 3 SSID 4

Attribute : s: Isolate the station from LAN

Backup Access Control: Upload From File:

Note:
Support AP ACL configuration file restoration.

Available settings are explained as follows:

Item	Description
Enable Mac Address Filter	Select to enable the MAC Address filter for wireless LAN identified with SSID 1 to 4 respectively. All the clients (expressed by MAC addresses) listed in the box can be grouped under different wireless LAN. For example, they can be grouped under SSID 1 and SSID 2 at the same time if you

	check SSID 1 and SSID 2.
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Apply SSID	After entering the client's MAC address, check the box of the SSIDs desired to insert this MAC address into their access control list.
Attribute	s: Isolate the station from LAN - select to isolate the wireless connection of the wireless client of the MAC address from LAN.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.
OK	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.
Backup Access Control	Settings on this web page can be saved as a file which can be restored in the future by this device or other device.
Upload From File	Restore wireless access control settings and applied onto this device.

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

III-1-5 WPS

Below shows Wireless LAN>>WPS web page:

Wireless LAN(2.4GHz) >> WPS (Wi-Fi Protected Setup)

Enable WPS 

Wi-Fi Protected Setup Information

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


Device Configure


Configure via Push Button	<input type="button" value="Start PBC"/>
Configure via Client PinCode	<input type="text"/> <input type="button" value="Start PIN"/>

Status: Ready

Note:

WPS can help your wireless client automatically connect to the Access point.

: WPS is Disabled.

: WPS is Enabled.

: Waiting for WPS requests from wireless clients.

Available settings are explained as follows:

Item	Description
Enable WPS	Check this box to enable WPS setting.
WPS Status	Display related system information for WPS. If the wireless security (encryption) function of the router is properly

	configured, you can see 'Configured' message here.
SSID	Display the SSID1 of the router. WPS is supported by SSID1 only.
Authentication Mode	Display current authentication mode of the router. Only WPA2/PSK and WPA/PSK support WPS.
Configure via Push Button	Click Start PBC to invoke Push-Button style WPS setup procedure. The router will wait for WPS requests from wireless clients about two minutes. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Please input the PIN code specified in wireless client you wish to connect, and click Start PIN button. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)

III-1-6 WDS

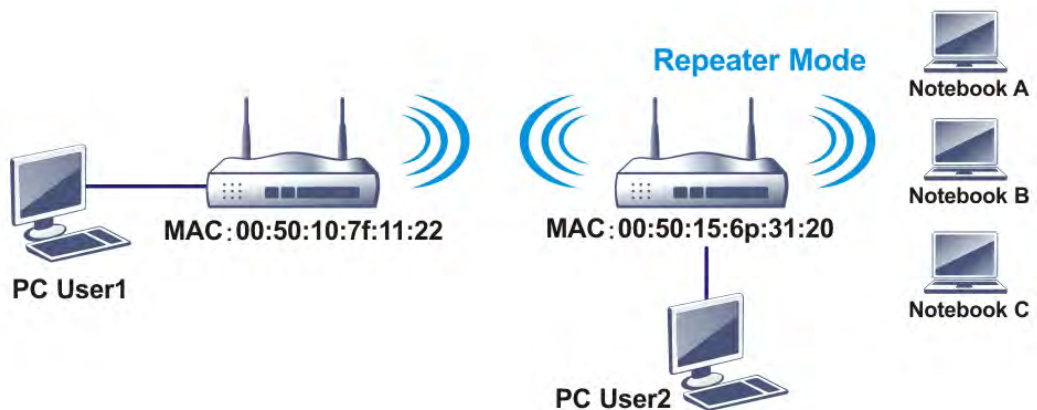
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

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

Refer to the following table:

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

The WDS - Repeater mode is implemented in Vigor router. The application for the WDS-Repeater mode is depicted as below:



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

WDS Settings
[Set to Factory Default](#)

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

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

OK Cancel

Available settings are explained as follows:

Item	Description
Mode	Choose the mode for WDS setting. Disable mode will not invoke any WDS setting. Repeater mode is for the second one.
Security	There are three types for security, Disable , WEP and Pre-shared key . The setting you choose here will make the following WEP or Pre-shared key field valid or not. Choose one of the types for the router.
Pre-shared Key	When Pre-Shared Key is selected as Security above, configure the following settings if required. Type - There are some types for you to choose. WPA and WPA2 are used for WDS devices (e.g.2925n wireless router, you can set the encryption mode as WPA or WPA2 to establish your WDS system between AP and the router. Key - Set the encryption key in this field. Type 8 ~ 63 ASCII characters or 64 hexadecimal digits leading by "0x".
Bridge	If you choose Bridge as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Yet please disable the unused link to get better performance. If you want to invoke the peer MAC address, remember to check Enable box in the front of the MAC

	address after typing.
Repeater	<p>If you choose Repeater as the connecting mode, please type in the peer MAC address (of VigorAP/Vigor router required to make connection with such Vigor router and used to extend the wireless signal) in these fields.</p> <p>Four peer MAC addresses are allowed to be entered in this page at one time. Similarly, if you want to invoke the peer MAC address, remember to check Enable box in the front of the MAC address after typing.</p>
Access Point Function	<p>Click Enable to make this router serve as an access point. When Repeater is set as WDS Mode, click Enable to use such function.</p> <p>Click Disable if Bridge is set as WDS Mode.</p>
Status	It allows user to send "hello" message to peers. Yet, it is valid only when the peer also supports this function.

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

III-1-7 Advanced Setting

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

Wireless LAN(2.4 GHz) >> Advanced Setting

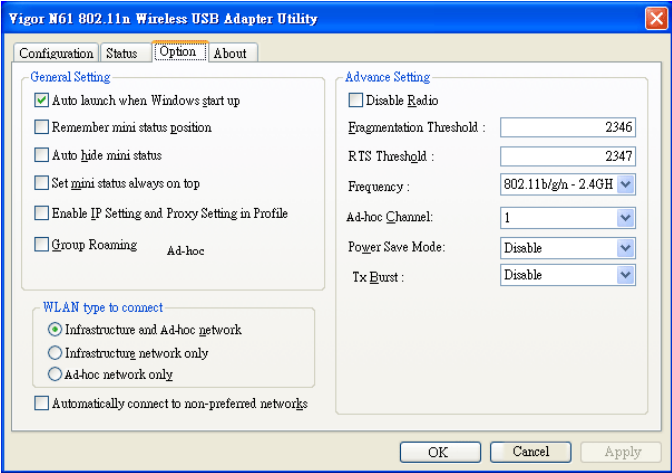
HT Physical Mode

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

OK

Available settings are explained as follows:

Item	Description
Operation Mode	<p>Mixed Mode - the router can transmit data with the ways supported in both 802.11a/b/g and 802.11n standards. However, the entire wireless transmission will be slowed down if 802.11g or 802.11b wireless client is connected.</p> <p>Green Field - to get the highest throughput, please choose such mode. Such mode can make the data transmission happen between 11n systems only. In addition, it does not have protection mechanism to avoid the conflict with neighboring devices of 802.11a/b/g.</p>
Channel Bandwidth	<p>Vigor router will use 20MHz/40MHz/80MHz for data transmission and receiving between the AP and the stations.</p> <p>20/40- Vigor Router will scan for nearby wireless AP, and then use 20MHz if the number of AP is more than 10, or use 40MHz if it's not.</p>
Guard Interval	<p>It is to assure the safety of propagation delays and reflections for the sensitive digital data. If you choose auto as guard interval, the AP router will choose short guard interval (increasing the wireless performance) or long guard interval for data transmit based on the station capability.</p>
Aggregation MSDU	<p>Aggregation MSDU can combine frames with different sizes. It is used for improving MAC layer's performance for some brand's clients. The default setting is Enable.</p>
Long Preamble	<p>This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. Click Enable to</p>

	use Long Preamble if needed to communicate with this kind of devices.
Packet-OVERDRIVE TX Burst	<p>This feature can enhance the performance in data transmission about 40%* more (by checking Tx Burst). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.</p> <p>Note: Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose Enable for TxBURST on the tab of Option).</p> 
TX Power	Set the power percentage for transmission signal of access point. The greater the value is, the higher intensity of the signal will be.
WMM Capable	<p>WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC_BE , AC_BK, AC_VI and AC_VO for WMM.</p> <p>To apply WMM parameters for wireless data transmission, please click the Enable radio button.</p>
APSD Capable	<p>APSD (automatic power-save delivery) is an enhancement over the power-save mechanisms supported by Wi-Fi networks. It allows devices to take more time in sleeping state and consume less power to improve the performance by minimizing transmission latency.</p> <p>The default setting is Disable.</p>
Rate Adaptation Algorithm	Wireless transmission rate is adapted dynamically. Usually, performance of "new" algorithm is better than "old".
Fragment Length (256 - 2346)	Set the Fragment threshold. Do not modify default value if you don't know what it is, default value is 2346.
RTS Threshold (1 - 2347)	<p>Minimize the collision (unit is bytes) between hidden stations to improve wireless performance.</p> <p>Set the RTS threshold. Do not modify default value if you don't know what it is, default value is 2347.</p>

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

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

III-1-8 Station Control

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

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

Wireless LAN(5GHz) >> Station Control

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

Note:

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

OK Cancel

Available settings are explained as follows:

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

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

III-1-9 AP Discovery

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

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

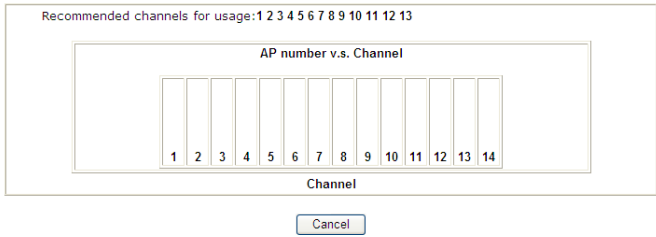
Access Point List

Index	BSSID	Channel	RSSI	SSID	Authentication
<input type="button" value="Scan"/>					
See Statistics .					
Add to WDS Settings :					
AP's MAC address		<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>			
<input type="button" value="Add to"/>		<input checked="" type="radio"/> Bridge <input type="radio"/> Repeater			

Note:

1. Wi-Fi will be temporarily off during AP Discovery (will take around 5 seconds).
2. AP Discovery can only support up to 32 APs displayed on the screen.

Available settings are explained as follows:

Item	Description
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button.
Statistics	It displays the statistics for the channels used by APs. Wireless LAN >> Site Survey Statistics 
Add to	If you want the found AP applying the WDS settings, please type in the AP's MAC address on the bottom of the page and click Repeater. Next, click Add to. Later, the MAC address of the AP will be added to Bridge or Repeater field of WDS settings page.

III-1-10 Bandwidth Management

The downstream or upstream from FTP, HTTP or some P2P applications will occupy large of bandwidth and affect the applications for other programs. Please use Bandwidth Management to make the bandwidth usage more efficient.

Wireless LAN >> Bandwidth Management

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

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

Available settings are explained as follows:

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

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

III-1-11 Airtime Fairness

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

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

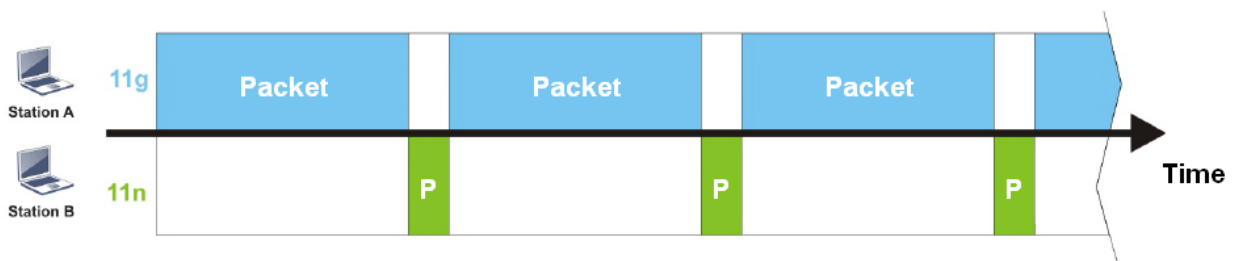
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

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

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

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

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



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



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

Suitable environment:

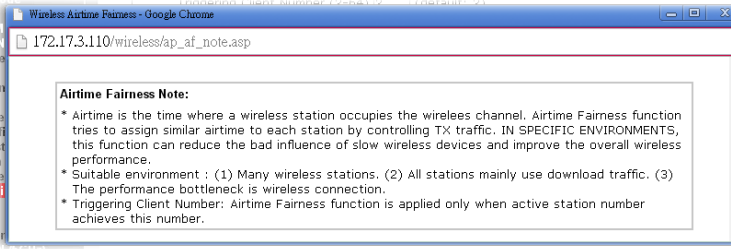
- (1) Many wireless stations.
- (2) All stations mainly use download traffic.
- (3) The performance bottleneck is wireless connection.

Wireless LAN(5GHz) >> Airtime Fairness

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

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

Available settings are explained as follows:

Item	Description
<p>Enable Airtime Fairness</p>	<p>Try to assign similar airtime to each wireless station by controlling TX traffic.</p> <p>Airtime Fairness - Click the link to display the following screen of airtime fairness note.</p> <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;">  </div> <p>Triggering Client Number -Airtime Fairness function is applied only when active station number achieves this number.</p>

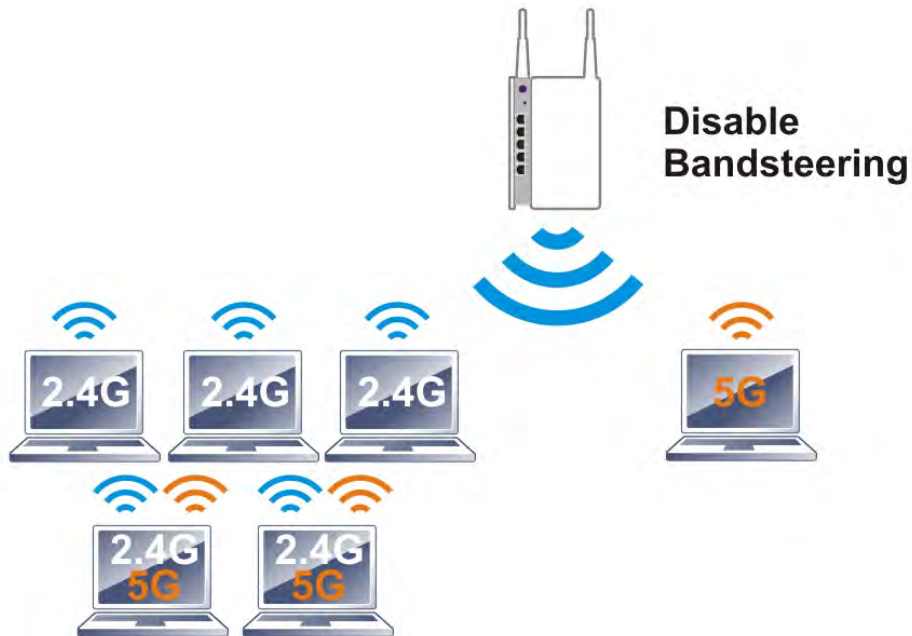
After finishing this web page configuration, please click OK to save the settings.



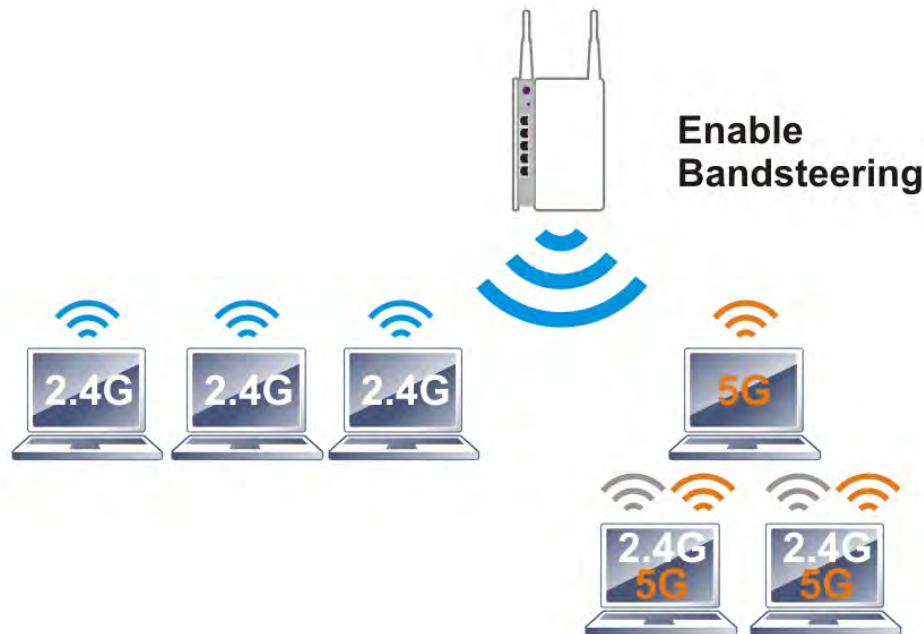
Info	Airtime Fairness function and Bandwidth Limit function should be mutually exclusive. So their webs have extra actions to ensure these two functions are not enabled simultaneously.
-------------	---

III-1-12 Band Steering

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



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



Info

To make Band Steering work successfully, SSID and security on 2.4GHz also MUST be broadcasted on 5GHz.

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

Wireless LAN(2.4 GHz) >> Band Steering

Enable **Band Steering**
 Check Time for WLAN Client 5G Capability second(s) (1 ~ 60) (Default: 15)

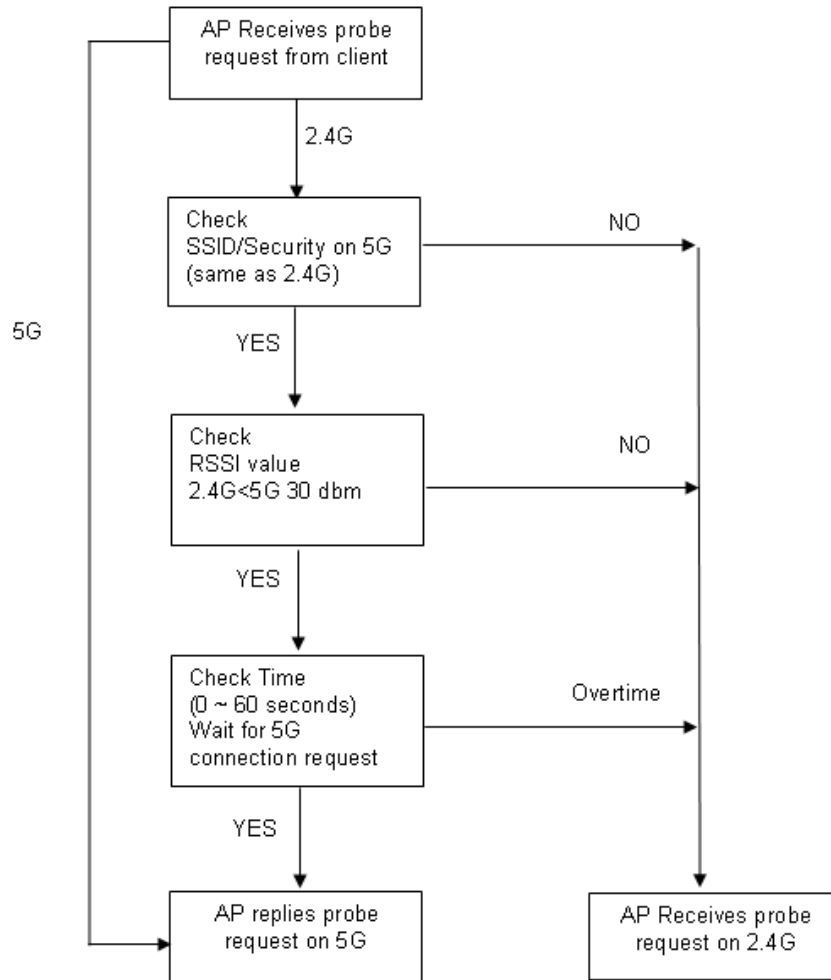
Note:
Please setup at least one pair of 2.4GHz and 5GHz Wireless LAN with the same SSID and security.

Available settings are explained as follows:

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

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

Below shows how Band Steering works.



How to Use Band Steering?

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

Wireless LAN(2.4 GHz) >> Band Steering

Enable **Band Steering**
 Check Time for WLAN Client 5G Capability second(s) (1 ~ 60) (Default: 15)

Note:

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

3. Click OK to save the settings.
4. Open **Wireless LAN (2.4GHz)>>General Setup** and **Wireless LAN (5GHz)>> General Setup**. Configure SSID as *DrayTek2862_BandSteering* for both pages. Click OK to save the settings.

Wireless LAN(2.4GHz) >> General Setup

General Setting (IEEE 802.11)

Enable Wireless LAN
 Mode :
 Channel:

Enable	Active	Hide SSID	SSID	Isolate Member	Isolate VPN
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	DrayTek2862_BandSteering	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DrayTek_Guest	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>

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

Wireless LAN(5GHz) >> General Setup

General Setting (IEEE 802.11)

Enable Wireless LAN
 Mode :
 Channel:

Enable	Active	Hide SSID	SSID	Isolate Member	Isolate VPN
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	DrayTek2862_BandSteering	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DrayTek_5G_Guest	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>

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

Same settings for 2.4GHz and 5GHz

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

Wireless LAN(2.4GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
Mode: Mixed(WPA+WPA2)/PSK			
<u>WPA</u>			
Encryption Mode: TKIP for WPA/AES for WPA2			
Pre-Shared Key(PSK): *****			
Password Strength: Weak Medium Strong			
Strong password requirements:			
1. Have at least 7 characters, including numbers and letters.			
2. Have at least one upper-case letter and one lower-case letter.			
3. Including non-alphanumeric characters is a plus.			
Type 8~63 ASCII character or 64 Hexadecimal digits leading by "0x", for example "cfigs01a2..." or "0x655abcd....".			
<u>WEP</u>			
Encryption Mode: 64-Bit			
<input checked="" type="radio"/> Key 1 : *****			
<input type="radio"/> Key 2 : *****			
<input type="radio"/> Key 3 : *****			

Same value for 2.4GHz and 5GHz

Wireless LAN(5GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
Mode: Mixed(WPA+WPA2)/PSK			
<u>WPA</u>			
Encryption Mode: TKIP for WPA/AES for WPA2			
Pre-Shared Key(PSK): *****			
Password Strength: Weak Medium Strong			
Strong password requirements:			
1. Have at least 7 characters, including numbers and letters.			
2. Have at least one upper-case letter and one lower-case letter.			
3. Including non-alphanumeric characters is a plus.			
Type 8~63 ASCII character or 64 Hexadecimal digits leading by "0x", for example "cfigs01a2..." or "0x655abcd....".			
<u>WEP</u>			
Encryption Mode: 64-Bit			
<input checked="" type="radio"/> Key 1 : *****			
<input type="radio"/> Key 2 : *****			
<input type="radio"/> Key 3 : *****			

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

III-1-13 Roaming

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

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

Wireless LAN(5GHz) >> Roaming

Router-assisted Client Roaming Parameters

Disable RSSI Requirement

Strictly Minimum RSSI -73 dBm (42%) (Default: -73)

Minimum RSSI -66 dBm (60%) (Default: -66)

with Adjacent AP RSSI over 5 dB (Default: 5)

Available settings are explained as follows:

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

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

III-1-14 Station List

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

Wireless LAN(2.4 GHz) >> Station List

Station List

Station List				
General				
Index	Status	IP Address	MAC Address	Associated with
<div style="text-align: center;">Refresh</div>				
<p>Status Codes : C: Connected, No encryption. E: Connected, WEP. P: Connected, WPA. A: Connected, WPA2. B: Blocked by Access Control. N: Connecting. F: Fail to pass WPA/PSK authentication.</p>				
<p>Add to Access Control :</p> <p>Client's MAC address <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/></p>				

Note:

After a station connects to the router successfully, it may be turned off without notice. In that case, it will still be on the list until the connection expires.

Add

Available settings are explained as follows:

Item	Description
Refresh	Click this button to refresh the status of station list.
Add	Click this button to add current typed MAC address into Access Control.

This page is left blank.

Part IV VPN



VPN



SSL VPN



Certificate
Management

A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link.

It is a form of VPN that can be used with a standard Web browser.

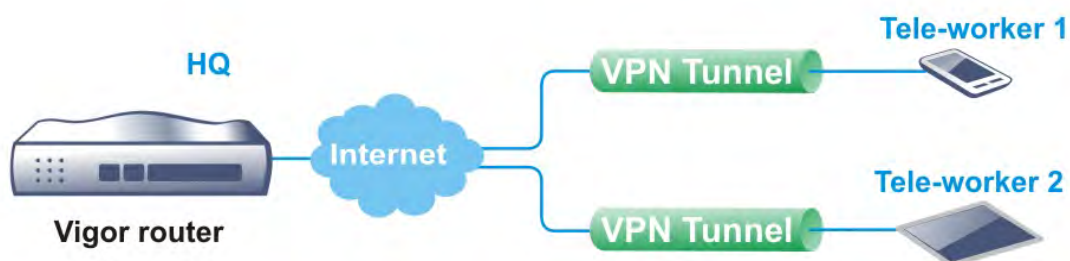
A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Here Vigor router support digital certificates conforming to standard X.509.

IV-1 VPN and Remote Access

A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link.

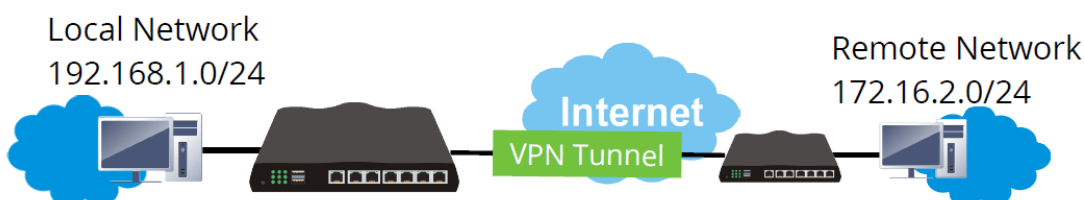
The VPN built is suitable for:

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



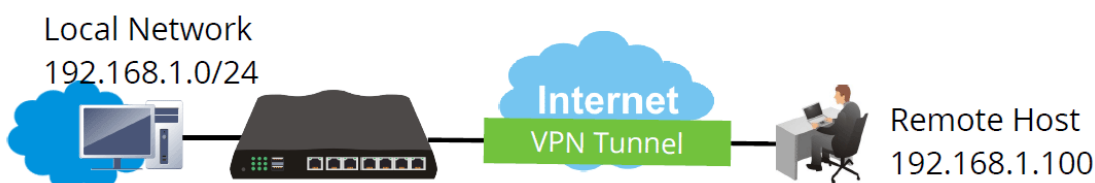
Site-to-Site (LAN-to-LAN)

- A connection between two router's LAN networks.
- Allows employees in branch offices and head office to share the same network resources.

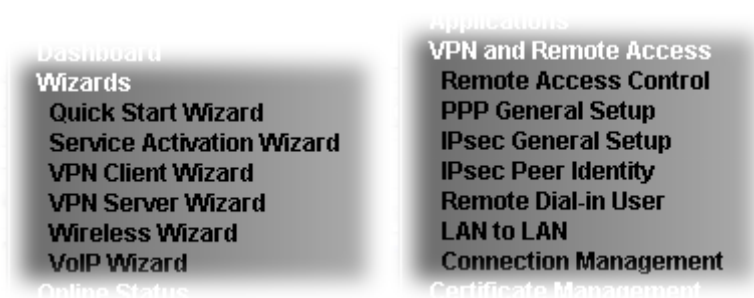


Remote Access (Remote Dial-in)

- A connection between the remote host and router's LAN network. The host will use an IP address in the local subnet.
- Allows employees to access the company's internal resources when they are traveling.



Web User Interface



IV-1-1 VPN Client Wizard

Such wizard is used to configure VPN settings for VPN client. Such wizard will guide to set the LAN-to-LAN profile for VPN dial out connection (from server to client) step by step.

1. Open Wizards>>VPN Client Wizard. The following page will appear.

VPN Client Wizard

Choose VPN Establishment Environment

LAN-to-LAN VPN Client Mode Selection:

Please choose a LAN-to-LAN Profile:

Note:

1. Please use Route Mode for typical LAN-to-LAN tunnels.
2. If the remote network is only expecting a single client or IP and is not configured to route the subnet then select NAT Mode.
3. If you are unsure of your configuration select Route Mode.

Available settings are explained as follows:

Item	Description
LAN-to-LAN Client Mode Selection	Choose the client mode. Route Mode/NAT Mode - If the remote network only allows you to dial in with single IP, please choose NAT mode, otherwise please choose Route Mode. <div style="border: 1px solid black; padding: 2px; margin-top: 5px;"> Route Mode ▾ Route Mode NAT Mode </div>
Please choose a LAN-to-LAN Profile	There are 32 VPN profiles for users to set.

[Index]	[Status]	[Name]
1	x	???
2	x	???
3	x	???
4	x	???
5	x	???
6	x	???
7	x	???

- When you finish the mode and profile selection, please click **Next** to open the following page.

VPN Client Wizard

VPN Connection Setting

<p>Security Ranking:</p> <p>Very High L2TP over IPSec</p> <p>High IPSec / SSL</p> <p>Medium PPTP (Encryption)</p> <p>Low L2TP / PPTP (None Encryption)</p>	<p>Throughput Ranking:</p> <p>Very High L2TP / PPTP (None Encryption)</p> <p>High IPSec</p> <p>Medium L2TP over IPSec / PPTP (Encryption)</p> <p>Low SSL</p>
<p>Select VPN Type:</p> <div style="border: 1px solid black; padding: 2px;"> <p>PPTP (Encryption) ▾</p> <p>PPTP (None Encryption)</p> <p style="background-color: #e0e0e0;">PPTP (Encryption)</p> <p>IPsec</p> <p>L2TP</p> <p>L2TP over IPsec (Nice to Have)</p> <p>L2TP over IPsec (Must)</p> <p>SSL</p> </div>	

In this page, you have to select suitable VPN type for the VPN client profile. There are six types provided here. Different type will lead to different configuration page. After making the choices for the client profile, please click **Next**. You will see different configurations based on the selection(s) you made.



Info

The following descriptions for VPN Type are based on the Route Mode specified in LAN-to-LAN Client Mode Selection.

When you choose **PPTP (None Encryption)** or **PPTP (Encryption)**, you will see the following graphic:

VPN Client Wizard

VPN Client PPTP None Encryption Settings

Profile Name	???
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	draytek.com
Username	marketing
Password	*****
Remote Network IP	192.168.1.6
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

When you choose IPsec, you will see the following graphic:

VPN Client Wizard

VPN Client IPsec Settings

Profile Name	???
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
IKE Authentication Method	
<input checked="" type="radio"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input type="radio"/> Digital Signature (X.509)	
Peer ID	None
Local ID	
<input checked="" type="radio"/> Alternative Subject Name First	
<input type="radio"/> Subject Name First	
Local Certificate	None
IPsec Security Method	
<input type="radio"/> Medium (AH)	
<input checked="" type="radio"/> High (ESP)	AES with Authentication
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

When you choose SSL, you will see the following graphic:

VPN Client Wizard

Profile Name	???
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
Server Port (for SSL Tunnel):	443
Username	???
Password	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

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

VPN Client Wizard

VPN Client L2TP over IPsec (Nice to Have) Settings

Profile Name	???
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
IKE Authentication Method	
<input checked="" type="radio"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input type="radio"/> Digital Signature (X.509)	
Peer ID	None
Local ID	
<input type="radio"/> Alternative Subject Name First	
<input type="radio"/> Subject Name First	
Local Certificate	None
IPsec Security Method	
<input type="radio"/> Medium (AH)	
<input checked="" type="radio"/> High (ESP)	AES with Authentication
Username	???
Password	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such profile. The length of the file is limited to 10 characters.
Always On	Check to enable router always keep VPN connection.
Server IP/Host Name	Type the IP address of the server or type the host name for

for VPN	such VPN profile.
IKE Authentication Method	<p>IKE Authentication Method usually applies to those are remote dial-in user or node (LAN to LAN) which uses dynamic IP address and IPsec-related VPN connections such as L2TP over IPsec and IPsec tunnel.</p> <p>Pre-Shared Key- Specify a key for IKE authentication.</p> <p>Confirm Pre-Shared Key-Confirm the pre-shared key.</p>
Digital Signature (X.509)	<p>Click Digital Signature to invoke this function.</p> <p>Peer ID - Choose the peer ID selection from the drop down list.</p> <p>Local ID - Choose Alternative Subject Name First or Subject Name First.</p> <p>Local Certificate - Use the drop down list to choose one of the certificates for using. You have to configure one certificate at least previously in Certificate Management >> Local Certificate. Otherwise, the setting you choose here will not be effective.</p>
IPsec Security Method	<p>Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.</p> <p>High - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.</p>
User Name	<p>This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above.</p> <p>The length of the user name is limited to 11 characters.</p>
Password	<p>This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above.</p> <p>The length of the password is limited to 11 characters.</p>
Remote Network IP	<p>Please type one LAN IP address (according to the real location of the remote host) for building VPN connection.</p>
Remote Network Mask	<p>Please type the network mask (according to the real location of the remote host) for building VPN connection.</p>

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

VPN Client Wizard

Please confirm your settings

LAN-to-LAN Index: 3
Profile Name: VPN_2R
VPN Connection Type: PPTP (None Encryption)
Always on: Yes
Server IP/Host Name: 123.45.67.89
Remote Network IP: 192.168.1.98
Remote Network Mask: 255.255.255.0

Click **Back** to modify changes if necessary. Otherwise,click **Finish** to save the current settings and proceed to the following action:

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

< Back

Next >

Finish

Cancel

Available settings are explained as follows:

Item	Description
Go to the VPN Connection Management	Click this radio button to access VPN and Remote Access>>Connection Management for viewing VPN Connection status.
Do another VPN Server Wizard Setup	Click this radio button to set another profile of VPN Server through VPN Server Wizard.
View more detailed configuration	Click this radio button to access VPN and Remote Access>>LAN to LAN for viewing detailed configuration.

IV-1-2 VPN Server Wizard

Such wizard is used to configure VPN settings for VPN server. Such wizard will guide to set the LAN-to-LAN profile for VPN dial in connection (from client to server) step by step.

1. Open **Wizards>>VPN Server Wizard**. The following page will appear.

VPN Server Wizard

Choose VPN Establishment Environment

VPN Server Mode Selection:	Remote Dial-in User (Teleworker) ▼
Please choose a LAN-to-LAN Profile:	[Index] [Status] [Name] ▼
Please choose a Dial-in User Accounts:	8 x ??? ▼
Allowed Dial-in Type:	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec <input checked="" type="checkbox"/> L2TP with IPsec Policy None ▼ <input checked="" type="checkbox"/> SSL Tunnel

Available settings are explained as follows:

Item	Description
VPN Server Mode Selection	Choose the direction for the VPN server. Site to Site VPN - To set a LAN-to-LAN profile automatically, please choose Site to Site VPN. Remote Dial-in User -You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in via VPN connection.
Please choose a LAN-to-LAN Profile	This item is available when you choose Site to Site VPN (LAN-to-LAN) as VPN server mode. There are 32 VPN profiles for users to set.
Please choose a Dial-in User Accounts	This item is available when you choose Remote Dial-in User (Teleworker) as VPN server mode. There are 32 VPN tunnels for users to set.
Allowed Dial-in Type	This item is available after you choose any one of dial-in user account profiles. Next, you have to select suitable dial-in type for the VPN server profile. There are several types provided here (similar to VPN Client Wizard).

	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec <input checked="" type="checkbox"/> L2TP with IPsec Policy <input checked="" type="checkbox"/> SSL Tunnel	<div style="border: 1px solid black; padding: 2px;"> None ▾ None Nice to Have Must </div>
<p>Different Dial-in Type will lead to different configuration page. In addition, adjustable items for each dial-in type will be changed according to the VPN Server Mode (Site to Site VPN and Remote Dial-in User) selected.</p>		

- After making the choices for the server profile, please click **Next**. You will see different configurations based on the selection you made. Here we take the examples of choosing **Site-to-Site VPN** as the **VPN Server Mode**.

When you check PPTP/SSL, you will see the following graphic:

VPN Server Wizard

VPN Authentication Setting

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

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

VPN Server Wizard

VPN Authentication Setting

Profile Name	???
PPTP / L2TP / L2TP over IPsec / SSL Tunnel Authentication	
Username	???
Password	
IPsec / L2TP over IPsec Authentication	
<input checked="" type="checkbox"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input type="checkbox"/> Digital Signature (X.509)	
Peer ID	None
Local ID	
<input type="radio"/> Alternative Subject Name First	
<input type="radio"/> Subject Name First	
Peer IP/VPN Client IP	
Peer ID	
Site to Site Information	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

When you check IPsec, you will see the following graphic:

VPN Server Wizard

VPN Authentication Setting

Profile Name	???
IPsec / L2TP over IPsec Authentication	
<input checked="" type="checkbox"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input type="checkbox"/> Digital Signature (X.509)	
Peer ID	None
Local ID	
<input type="radio"/> Alternative Subject Name First	
<input type="radio"/> Subject Name First	
Peer IP/VPN Client IP	
Peer ID	
Site to Site Information	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such profile. The length of the file is limited to 10 characters.
User Name	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 11 characters.

Password	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 11 characters.
Pre-Shared Key	For IPsec/L2TP IPsec authentication, you have to type a pre-shared key. The length of the name is limited to 64 characters.
Confirm Pre-Shared Key	Type the pre-shared key again for confirmation.
Digital Signature (X.509)	Check the box of Digital Signature to invoke this function. Peer ID - Choose the peer ID selection from the drop down list. Local ID - Choose Alternative Subject Name First or Subject Name First .
Peer IP/VPN Client IP	Type the WAN IP address or VPN client IP address for the remote client.
Peer ID	Type the ID name for the remote client. The length of the name is limited to 47 characters.

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

VPN Server Wizard

Please Confirm Your Settings

VPN Environment:	Remote Access VPN (Host-to-LAN)
Index:	8
Username:	???
Allowed Service:	IPsec
Peer IP/VPN Client IP:	192.168.1.58
Peer ID:	frank

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and proceed to the following action:

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

Available settings are explained as follows:

Item	Description
Go to the VPN Connection Management	Click this radio button to access VPN and Remote Access>>Connection Management for viewing VPN Connection status.
Do another VPN Server Wizard Setup	Click this radio button to set another profile of VPN Server through VPN Server Wizard.

View more detailed configuration	Click this radio button to access VPN and Remote Access>>LAN to LAN for viewing detailed configuration.
----------------------------------	--

IV-1-3 Remote Access Control

Enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should disable the VPN service of Vigor Router to allow VPN tunnel pass through, as well as the appropriate NAT settings, such as DMZ or open port.

Open **VPN and Remote Access>>Remote Access Control**.

VPN and Remote Access >> Remote Access Control Setup

Remote Access Control Setup

<input checked="" type="checkbox"/>	Enable PPTP VPN Service
<input checked="" type="checkbox"/>	Enable IPSec VPN Service
<input checked="" type="checkbox"/>	Enable L2TP VPN Service
<input checked="" type="checkbox"/>	Enable SSL VPN Service

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

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

IV-1-4 PPP General Setup

This submenu only applies to PPP-related VPN connections, such as PPTP, L2TP, L2TP over IPsec.

VPN and Remote Access >> PPP General Setup

PPP General Setup

<p>PPP/MP Protocol</p> <p>Dial-In PPP Authentication: <input type="text" value="PAP/CHAP/MS-CHAP/MS-CHAPv2"/> ▼</p> <p>Dial-In PPP Encryption(MPPE): <input type="text" value="Optional MPPE"/> ▼</p> <p>Mutual Authentication (PAP): <input type="radio"/> Yes <input checked="" type="radio"/> No</p> <p>Username: <input type="text"/></p> <p>Password: <input type="text"/></p> <p>IP Address Assignment for Dial-In Users (When DHCP Disable set)</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th></th> <th>Start IP Address</th> <th>IP Pool Counts</th> </tr> </thead> <tbody> <tr> <td>LAN 1</td> <td><input type="text" value="192.168.1.200"/></td> <td><input type="text" value="50"/></td> </tr> <tr> <td>LAN 2</td> <td><input type="text" value="192.168.2.200"/></td> <td><input type="text" value="50"/></td> </tr> <tr> <td>LAN 3</td> <td><input type="text" value="192.168.3.200"/></td> <td><input type="text" value="50"/></td> </tr> <tr> <td>LAN 4</td> <td><input type="text" value="192.168.4.200"/></td> <td><input type="text" value="50"/></td> </tr> </tbody> </table>		Start IP Address	IP Pool Counts	LAN 1	<input type="text" value="192.168.1.200"/>	<input type="text" value="50"/>	LAN 2	<input type="text" value="192.168.2.200"/>	<input type="text" value="50"/>	LAN 3	<input type="text" value="192.168.3.200"/>	<input type="text" value="50"/>	LAN 4	<input type="text" value="192.168.4.200"/>	<input type="text" value="50"/>	<p>PPP Authentication Methods</p> <p><input checked="" type="checkbox"/> Remote Dial-in User</p> <p><input checked="" type="checkbox"/> RADIUS</p> <p>Note:</p> <p>1. Default priority is Remote Dial-in User -> RADIUS.</p> <p>2. Vigor router also supports Frame-IP-Address from RADIUS server to assign IP address to VPN client.</p> <p>While using Radius Authentication:</p> <p>Assign IP from subnet: <input type="text" value="LAN1"/> ▼</p>
	Start IP Address	IP Pool Counts														
LAN 1	<input type="text" value="192.168.1.200"/>	<input type="text" value="50"/>														
LAN 2	<input type="text" value="192.168.2.200"/>	<input type="text" value="50"/>														
LAN 3	<input type="text" value="192.168.3.200"/>	<input type="text" value="50"/>														
LAN 4	<input type="text" value="192.168.4.200"/>	<input type="text" value="50"/>														

Available settings are explained as follows:

Item	Description
Dial-In PPP Authentication	<p>PAP Only - elect this option to force the router to authenticate dial-in users with the PAP protocol.</p> <p>PAP/CHAP/MS-CHAP/MS-CHAPv2 - Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication.</p>
Dial-In PPP Encryption (MPPE)	<p>Optional MPPE - This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit "no MPPE encrypted packets". Otherwise, the MPPE encryption scheme will be used to encrypt the data.</p> <ul style="list-style-type: none"> ● Require MPPE (40/128bits) - Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data. ● Maximum MPPE - This option indicates that the router will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.
Mutual Authentication (PAP)	The Mutual Authentication function is mainly used to communicate with other routers or clients who need bi-directional authentication in order to provide stronger security, for example, Cisco routers. So you should enable

	<p>this function when your peer router requires mutual authentication. You should further specify the User Name and Password of the mutual authentication peer.</p> <p>The length of the name/password is limited to 23/19 characters.</p>
IP Address Assignment for Dial-In Users	<p>Enter a start IP address for the dial-in PPP connection. You should choose an IP address from the local private network. For example, if the local private network is 192.168.1.0/255.255.255.0, you could choose 192.168.1.200 as the Start IP Address.</p> <p>You can configure up to four start IP addresses for LAN1 ~ LAN4.</p>
PPP Authentication Methods	<p>Select the method(s) to be used for authentication in PPP connection.</p> <p>PPP Authentication Methods</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Remote Dial-in User <input checked="" type="checkbox"/> RADIUS
While using Radius Authentication	<p>If PPP connection will be authenticated via RADIUS server, it is necessary to specify the LAN profile for the dial-in user to get IP from.</p>

IV-1-5 IPsec General Setup

In IPsec General Setup, there are two major parts of configuration.

There are two phases of IPsec.

- Phase 1: negotiation of IKE parameters including encryption, hash, Diffie-Hellman parameter values, and lifetime to protect the following IKE exchange, authentication of both peers using either a Pre-Shared Key or Digital Signature (x.509). The peer that starts the negotiation proposes all its policies to the remote peer and then remote peer tries to find a highest-priority match with its policies. Eventually to set up a secure tunnel for IKE Phase 2.
- Phase 2: negotiation IPsec security methods including Authentication Header (AH) or Encapsulating Security Payload (ESP) for the following IKE exchange and mutual examination of the secure tunnel establishment.

There are two encapsulation methods used in IPsec, **Transport** and **Tunnel**. The **Transport** mode will add the AH/ESP payload and use original IP header to encapsulate the data payload only. It can just apply to local packet, e.g., L2TP over IPsec. The **Tunnel** mode will not only add the AH/ESP payload but also use a new IP header (Tunneled IP header) to encapsulate the whole original IP packet.

Authentication Header (AH) provides data authentication and integrity for IP packets passed between VPN peers. This is achieved by a keyed one-way hash function to the packet to create a message digest. This digest will be put in the AH and transmitted along with packets. On the receiving side, the peer will perform the same one-way hash on the packet and compare the value with the one in the AH it receives.

Encapsulating Security Payload (ESP) is a security protocol that provides data confidentiality and protection with optional authentication and replay detection service.

VPN and Remote Access >> IPsec General Setup

VPN IKE/IPsec General Setup

Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method	
Certificate for Dial-in	None ▾
Pre-Shared Key	
Pre-Shared Key	<input type="text"/>
Confirm Pre-Shared Key	<input type="text"/>
IPsec Security Method	
<input checked="" type="checkbox"/> Medium (AH)	Data will be authentic, but will not be encrypted.
High (ESP)	<input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
Data will be encrypted and authentic.	

OK Cancel

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. Certificate for Dial-in -Choose one of the local certificates

	<p>from the drop down list.</p> <p>Pre-Shared Key- Specify a key for IKE authentication.</p> <p>Confirm Pre-Shared Key- Retype the characters to confirm the pre-shared key.</p> <p>Note: Any packets from the remote dial-in user which does not match the rule defined in VPN and Remote Access>>Remote Dial-In User will be applied with the method specified here.</p>
IPsec Security Method	<p>Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.</p> <p>High (ESP) - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.</p>

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

IV-1-6 IPsec Peer Identity

To use digital certificate for peer authentication in either LAN-to-LAN connection or Remote User Dial-In connection, here you may edit a table of peer certificate for selection. As shown below, the router provides 32 entries of digital certificates for peer dial-in users.

VPN and Remote Access >> IPsec Peer Identity

X509 Peer ID Accounts:

[Set to Factory Default](#)

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

Available settings are explained as follows:

Item	Description
Set to Factory Default	Click it to clear all indexes.
Index	Click the number below Index to access into the setting page of IPsec Peer Identity.

Name	Display the profile name of that index.
------	---

Click each index to edit one peer digital certificate. There are three security levels of digital signature authentication: Fill each necessary field to authenticate the remote peer. The following explanation will guide you to fill all the necessary fields.

VPN and Remote Access >> IPsec Peer Identity

Profile Index : 1

Profile Name	<input data-bbox="507 510 699 544" type="text" value="???"/>
<input type="checkbox"/> Enable this account	
<input checked="" type="radio"/> Accept Any Peer ID	
<input type="radio"/> Accept Subject Alternative Name	
Type	<input data-bbox="762 705 917 734" type="text" value="Domain Name"/>
Domain Name	<input data-bbox="762 741 1168 775" type="text"/>
<input type="radio"/> Accept Subject Name	
Country (C)	<input data-bbox="762 842 836 875" type="text"/>
State (ST)	<input data-bbox="762 882 1168 916" type="text"/>
Location (L)	<input data-bbox="762 922 1168 956" type="text"/>
Organization (O)	<input data-bbox="762 963 1168 996" type="text"/>
Organization Unit (OU)	<input data-bbox="762 1003 1168 1037" type="text"/>
Common Name (CN)	<input data-bbox="762 1043 1168 1077" type="text"/>
Email (E)	<input data-bbox="762 1084 1168 1117" type="text"/>

Available settings are explained as follows:

Item	Description
Profile Name	Type the name of the profile. The maximum length of the name you can set is 32 characters.
Enable this account	Check it to enable such account profile.
Accept Any Peer ID	Click to accept any peer regardless of its identity.
Accept Subject Alternative Name	Click to check one specific field of digital signature to accept the peer with matching value. The field can be IP Address , Domain , or E-mail . The box under the Type will appear according to the type you select and ask you to fill in corresponding setting.
Accept Subject Name	Click to check the specific fields of digital signature to accept the peer with matching value. The field includes Country (C) , State (ST) , Location (L) , Organization (O) , Organization Unit (OU) , Common Name (CN) , and Email (E) .

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

IV-1-7 Remote Dial-in User

You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in via VPN connection. You may set parameters including specified connection peer ID, connection type (VPN connection - including PPTP, IPsec Tunnel, and L2TP by itself or over IPsec) and corresponding security methods, etc.

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

VPN and Remote Access >> Remote Dial-in User



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

Index	User	Active	Status	Index	User	Active	Status
1.	???	<input type="checkbox"/>	---	17.	???	<input type="checkbox"/>	---
2.	???	<input type="checkbox"/>	---	18.	???	<input type="checkbox"/>	---
3.	???	<input type="checkbox"/>	---	19.	???	<input type="checkbox"/>	---
4.	???	<input type="checkbox"/>	---	20.	???	<input type="checkbox"/>	---
5.	???	<input type="checkbox"/>	---	21.	???	<input type="checkbox"/>	---
6.	???	<input type="checkbox"/>	---	22.	???	<input type="checkbox"/>	---
7.	???	<input type="checkbox"/>	---	23.	???	<input type="checkbox"/>	---
8.	???	<input type="checkbox"/>	---	24.	???	<input type="checkbox"/>	---
9.	???	<input type="checkbox"/>	---	25.	???	<input type="checkbox"/>	---
10.	???	<input type="checkbox"/>	---	26.	???	<input type="checkbox"/>	---
11.	???	<input type="checkbox"/>	---	27.	???	<input type="checkbox"/>	---
12.	???	<input type="checkbox"/>	---	28.	???	<input type="checkbox"/>	---
13.	???	<input type="checkbox"/>	---	29.	???	<input type="checkbox"/>	---
14.	???	<input type="checkbox"/>	---	30.	???	<input type="checkbox"/>	---
15.	???	<input type="checkbox"/>	---	31.	???	<input type="checkbox"/>	---
16.	???	<input type="checkbox"/>	---	32.	???	<input type="checkbox"/>	---

OK Cancel

Download Smart VPN Client:

[Smart VPN Client for Windows PC](#)

[Smart VPN Android/iOS App](#)

Available settings are explained as follows:

Item	Description
Set to Factory Default	Click to clear all indexes.
Index	Click the number below Index to access into the setting page of Remote Dial-in User.
User	Display the username for the specific dial-in user of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.
Active	Check the box to activate such profile.
Status	Display the access state of the specific dial-in user. The symbol V and X represent the specific dial-in user to be active and inactive, respectively.

Click each index to edit one remote user profile. Each Dial-In Type requires you to fill the different corresponding fields on the right. If the fields gray out, it means you may leave it untouched. The following explanation will guide you to fill all the necessary fields.

VPN and Remote Access >> Remote Dial-in User

Index No. 1

<p>User account and Authentication</p> <p><input type="checkbox"/> Enable this account</p> <p>Idle Timeout <input type="text" value="300"/> second(s)</p> <hr/> <p>Allowed Dial-In Type</p> <p><input checked="" type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> IPsec Tunnel</p> <p><input checked="" type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/></p> <p><input checked="" type="checkbox"/> SSL Tunnel</p> <p><input type="checkbox"/> Specify Remote Node</p> <p>Remote Client IP <input type="text"/></p> <p>or Peer ID <input type="text"/></p> <p>Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block</p> <p>Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)</p> <hr/> <p>Subnet</p> <p><input type="text" value="LAN 1"/></p> <p><input type="checkbox"/> Assign Static IP Address</p> <p><input type="text" value="0.0.0.0"/></p>	<p>Username <input style="background-color: #e0e0e0;" type="text" value="???"/></p> <p>Password(Max 19 char) <input style="background-color: #e0e0e0;" type="text"/></p> <p><input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP)</p> <p>PIN Code <input style="background-color: #e0e0e0;" type="text"/></p> <p>Secret <input style="background-color: #e0e0e0;" type="text"/></p> <hr/> <p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p>IKE Pre-Shared Key <input style="background-color: #e0e0e0;" type="text"/></p> <p><input type="checkbox"/> Digital Signature(X.509)</p> <p><input type="text" value="None"/></p> <hr/> <p>IPsec Security Method</p> <p><input checked="" type="checkbox"/> Medium(AH)</p> <p>High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p> <p>Local ID (optional) <input style="background-color: #e0e0e0;" type="text"/></p>
--	--

Available settings are explained as follows:

Item	Description
User account and Authentication	<p>Enable this account - Check the box to enable this function.</p> <p>Idle Timeout- If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.</p>
Allowed Dial-In Type	<p>PPTP - Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.</p> <p>IPsec Tunnel - Allow the remote dial-in user to make an IPsec VPN connection through Internet.</p> <p>L2TP with IPsec Policy - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below:</p> <ul style="list-style-type: none"> ● None - Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection. ● Nice to Have - Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. ● Must -Specify the IPsec policy to be definitely applied

	<p>on the L2TP connection.</p> <p>SSL Tunnel - Allow the remote dial-in user to make an SSL VPN connection through Internet.</p> <p>Specify Remote Node -You can specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode).</p> <p>Uncheck the checkbox means the connection type you select above will apply the authentication methods and security methods in the general settings.</p> <p>Netbios Naming Packet -</p> <ul style="list-style-type: none"> ● Pass - Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. ● Block - When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel. <p>Multicast via VPN - Some programs might send multicast packets via VPN connection.</p> <ul style="list-style-type: none"> ● Pass - Click this button to let multicast packets pass through the router. ● Block - This is default setting. Click this button to let multicast packets be blocked by the router. <p>User Name - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 23 characters.</p> <p>Password - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 19 characters.</p> <p>Enable Mobile One-Time Passwords (mOTP) - Check this box to make the authentication with mOTP function.</p> <p>PIN Code - Type the code for authentication (e.g, 1234).</p> <p>Secret - Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).</p>
Subnet	<p>Chose one of the subnet selections for such VPN profile.</p> <p>Assign Static IP Address - Please type a static IP address for the subnet you specified.</p>
IKE Authentication Method	<p>This group of fields is applicable for IPsec Tunnels and L2TP with IPsec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPsec tunnel either with or without specifying the IP address of the remote node.</p> <p>Pre-Shared Key - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key.</p> <p>Digital Signature (X.509) - Check the box of Digital Signature to invoke this function and Select one predefined Profiles set in the VPN and Remote Access >>IPsec Peer Identity.</p>
IPsec Security Method	<p>This group of fields is a must for IPsec Tunnels and L2TP with IPsec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method.</p> <p>Medium-Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it.</p>

	<p>High-Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.</p> <p>Local ID (Optional)- Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.</p>
--	---

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

IV-1-8 LAN to LAN

Here you can manage LAN-to-LAN connections by maintaining a table of connection profiles. You may set parameters including specified connection direction (dial-in or dial-out), connection peer ID, connection type (VPN connection - including PPTP, IPsec Tunnel, and L2TP by itself or over IPsec) and corresponding security methods, etc.

VPN and Remote Access >> LAN to LAN



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

Index	Name	Active	Status	Index	Name	Active	Status
1.	???	<input type="checkbox"/>	---	17.	???	<input type="checkbox"/>	---
2.	???	<input type="checkbox"/>	---	18.	???	<input type="checkbox"/>	---
3.	???	<input type="checkbox"/>	---	19.	???	<input type="checkbox"/>	---
4.	???	<input type="checkbox"/>	---	20.	???	<input type="checkbox"/>	---
5.	???	<input type="checkbox"/>	---	21.	???	<input type="checkbox"/>	---
6.	???	<input type="checkbox"/>	---	22.	???	<input type="checkbox"/>	---
7.	???	<input type="checkbox"/>	---	23.	???	<input type="checkbox"/>	---
8.	???	<input type="checkbox"/>	---	24.	???	<input type="checkbox"/>	---
9.	???	<input type="checkbox"/>	---	25.	???	<input type="checkbox"/>	---
10.	???	<input type="checkbox"/>	---	26.	???	<input type="checkbox"/>	---
11.	???	<input type="checkbox"/>	---	27.	???	<input type="checkbox"/>	---
12.	???	<input type="checkbox"/>	---	28.	???	<input type="checkbox"/>	---
13.	???	<input type="checkbox"/>	---	29.	???	<input type="checkbox"/>	---
14.	???	<input type="checkbox"/>	---	30.	???	<input type="checkbox"/>	---
15.	???	<input type="checkbox"/>	---	31.	???	<input type="checkbox"/>	---
16.	???	<input type="checkbox"/>	---	32.	???	<input type="checkbox"/>	---

Available settings are explained as follows:

Item	Description
Set to Factory Default	Click to clear all indexes.
Name	Indicate the name of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.
Active	V - means the profile has been enabled. X - means the profile has not been enabled.
Status	Online - means such LAN to LAN profile is in use. Offline - means such LAN to LAN profile isn't in use even if the profile has been enabled.

To edit each profile:

- Click each index to edit each profile and you will get the following page. Each LAN-to-LAN profile includes 4 subgroups. If the fields gray out, it means you may leave it untouched. The following explanations will guide you to fill all the necessary fields.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="???"/> <input type="checkbox"/> Enable this profile	Call Direction <input checked="" type="radio"/> Both <input type="radio"/> Dial-Out <input type="radio"/> Dial-in <input type="checkbox"/> Always on Idle Timeout <input type="text" value="300"/> second(s) <input type="checkbox"/> Enable PING to keep IPsec tunnel alive PING to the IP <input type="text"/>
Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	

2. Dial-Out Settings

Type of Server I am calling <input checked="" type="radio"/> PPTP <input type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy <input type="text" value="None"/> <input type="radio"/> SSL Tunnel	Username <input type="text" value="???"/> Password(Max 15 char) <input type="text"/> PPP Authentication <input type="text" value="PAP/CHAP/MS-CHAP/MS-CHAPv2"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <input type="text"/> Server Port (for SSL Tunnel): <input type="text" value="443"/>	IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key <input type="text" value="IKE Pre-Shared Key"/> <input type="radio"/> Digital Signature(X.509) Peer ID <input type="text" value="None"/> Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First Local Certificate <input type="text" value="None"/>
	IPsec Security Method <input type="radio"/> Medium(AH) <input checked="" type="radio"/> High(ESP) <input type="text" value="AES with Authentication"/> <input type="button" value="Advanced"/>
	Index(1-15) in Schedule Setup: <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>

Available settings are explained as follows:

Item	Description
Common Settings	<p>Profile Name - Specify a name for the profile of the LAN-to-LAN connection.</p> <p>Enable this profile - Check here to activate this profile.</p> <p>Netbios Naming Packet</p> <ul style="list-style-type: none"> Pass - click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. Block - When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel. <p>Multicast via VPN - Some programs might send multicast packets via VPN connection.</p> <ul style="list-style-type: none"> Pass - Click this button to let multicast packets pass through the router. Block - This is default setting. Click this button to let multicast packets be blocked by the router.

	<p>Call Direction - Specify the allowed call direction of this LAN-to-LAN profile.</p> <ul style="list-style-type: none"> ● Both:-initiator/responder ● Dial-Out- initiator only ● Dial-In- responder only. <p>Always On-Check to enable router always keep VPN connection.</p> <p>Idle Timeout: The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.</p> <p>Enable PING to keep IPsec tunnel alive - This function is to help the router to determine the status of IPsec VPN connection, especially useful in the case of abnormal VPN IPsec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address.</p> <p>This function is used to handle abnormal IPsec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial. Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer disconnects without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection).</p> <p>PING to the IP - Enter the IP address of the remote host that located at the other-end of the VPN tunnel.</p>
Dial-Out Settings	<p>Type of Server I am calling - PPTP - Build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server.</p> <p>IPsec Tunnel - Build an IPsec VPN connection to the server through Internet.</p> <p>L2TP with IPsec Policy - Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below:</p> <ul style="list-style-type: none"> ● None: Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection. ● Nice to Have: Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN connection becomes one pure L2TP connection. ● Must: Specify the IPsec policy to be definitely applied on the L2TP connection. <p>SSL Tunnel - Build an SSL VPN connection to the server through Internet.</p> <p>User Name - This field is applicable when you select, PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 49 characters.</p> <p>Password - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 15 characters.</p> <p>PPP Authentication - This field is applicable when you</p>

select, PPTP or L2TP with or without IPsec policy above. PAP/CHAP/MS-CHAP/MS-CHAPv2 is the most common selection due to compatibility.

VJ compression - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally set to **On** to improve bandwidth utilization.

IKE Authentication Method - This group of fields is applicable for IPsec Tunnels and L2TP with IPsec Policy.

- **Pre-Shared Key** - Input 1-63 characters as pre-shared key.
- **Digital Signature (X.509)** - Select one predefined Profiles set in the **VPN and Remote Access >>IPsec Peer Identity**.

Peer ID - Select one of the predefined Profiles set in **VPN and Remote Access >>IPsec Peer Identity**.

Local ID - Specify a local ID (**Alternative Subject Name First** or **Subject Name First**) to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.

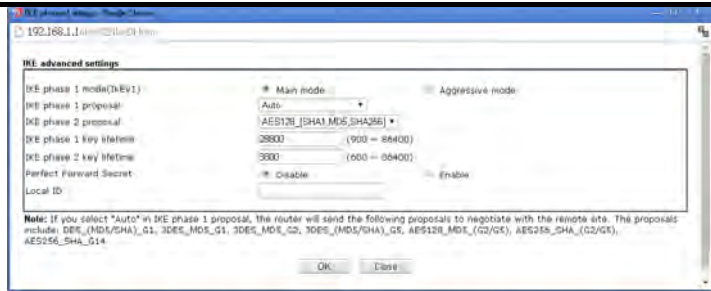
- **Local Certificate** - Select one of the profiles set in **Certificate Management>>Local Certificate**.

IPsec Security Method - This group of fields is a must for IPsec Tunnels and L2TP with IPsec Policy.

- **Medium AH (Authentication Header)** means data will be authenticated, but not be encrypted. By default, this option is active.
- **High (ESP-Encapsulating Security Payload)**- means payload (data) will be encrypted and authenticated. Select from below:
 - **DES without Authentication** -Use DES encryption algorithm and not apply any authentication scheme.
 - **DES with Authentication**-Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
 - **3DES without Authentication**-Use triple DES encryption algorithm and not apply any authentication scheme.
 - **3DES with Authentication**-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
 - **AES without Authentication**-Use AES encryption algorithm and not apply any authentication scheme.
 - **AES with Authentication**-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.

Advanced - Specify mode, proposal and key life of each IKE phase, Gateway, etc.

The window of advance setup is shown as below:



IKE phase 1 mode -Select from **Main mode** and **Aggressive mode**. The ultimate outcome is to exchange security proposals to create a protected secure channel. **Main mode** is more secure than **Aggressive mode** since more exchanges are done in a secure channel to set up the IPsec session. However, the **Aggressive mode** is faster. The default value in Vigor router is **Main mode**.

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

Local ID-In **Aggressive mode**, Local ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters.

Index(1-15) - Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications >> Schedule** setup. The default setting of this field is blank and the function will always work.

3. Dial-In Settings

<p>Allowed Dial-In Type</p> <p><input checked="" type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> IPsec Tunnel</p> <p><input checked="" type="checkbox"/> L2TP with IPsec Policy None</p> <p><input checked="" type="checkbox"/> SSL Tunnel</p> <p><input type="checkbox"/> Specify Remote VPN Gateway</p> <p>Peer VPN Server IP <input style="width: 100%;" type="text"/></p> <p>or Peer ID <input style="width: 100%;" type="text"/></p>	<p>Username <input data-bbox="1141 224 1348 257" style="width: 100%;" type="text" value="???"/></p> <p>Password(Max 11 char) <input data-bbox="1141 257 1348 291" style="width: 100%;" type="password"/></p> <p>VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off</p> <hr/> <p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p>IKE Pre-Shared Key <input data-bbox="1141 403 1348 436" style="width: 100%;" type="text"/></p> <p><input type="checkbox"/> Digital Signature(X.509)</p> <p>None</p> <p>Local ID</p> <p><input checked="" type="radio"/> Alternative Subject Name First</p> <p><input type="radio"/> Subject Name First</p> <hr/> <p>IPsec Security Method</p> <p><input checked="" type="checkbox"/> Medium(AH)</p> <p>High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p>
--	--

4. TCP/IP Network Settings

<p>My WAN IP <input style="width: 100%;" type="text" value="0.0.0.0"/></p> <p>Remote Gateway IP <input style="width: 100%;" type="text" value="0.0.0.0"/></p> <p>Remote Network IP <input style="width: 100%;" type="text" value="0.0.0.0"/></p> <p>Remote Network Mask <input style="width: 100%;" type="text" value="255.255.255.0"/></p> <p>Local Network IP <input style="width: 100%;" type="text" value="192.168.1.1"/></p> <p>Local Network Mask <input style="width: 100%;" type="text" value="255.255.255.0"/></p> <p style="text-align: center;"><input type="button" value="More"/></p>	<p>RIP Direction Disable</p> <p>From first subnet to remote network, you have to do</p> <p style="text-align: center;">Route</p> <p><input type="checkbox"/> IPsec VPN with the Same Subnets</p> <hr/> <p><input type="checkbox"/> Change default route to this VPN tunnel (Only active if one single WAN is up)</p>
--	--

Available settings are explained as follows:

Item	Description
<p>Dial-In Settings</p>	<p>Allowed Dial-In Type - Determine the dial-in connection with different types.</p> <ul style="list-style-type: none"> ● PPTP - Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below. ● IPsec Tunnel- Allow the remote dial-in user to trigger an IPsec VPN connection through Internet. ● L2TP with IPsec Policy - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below: <ul style="list-style-type: none"> ■ None - Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection. ■ Nice to Have - Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. ■ Must - Specify the IPsec policy to be definitely applied on the L2TP connection. ● SSL Tunnel- Allow the remote dial-in user to trigger an SSL VPN connection through Internet. <p>Specify Remote VPN Gateway - You can specify the IP address of the remote dial-in user or peer ID (should be the</p>

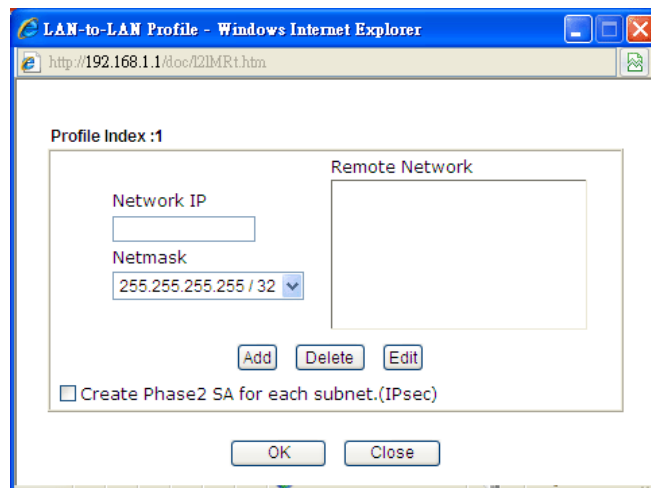
	<p>same with the ID setting in dial-in type) by checking the box. Also, you should further specify the corresponding security methods on the right side.</p> <p>If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings.</p> <p>Username - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 11 characters.</p> <p>Password - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 11 characters.</p> <p>VJ Compression - VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select PPTP or L2TP with or without IPsec policy above.</p> <p>IKE Authentication Method - This group of fields is applicable for IPsec Tunnels and L2TP with IPsec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPsec tunnel either with or without specify the IP address of the remote node.</p> <ul style="list-style-type: none"> ● Pre-Shared Key - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key. ● Digital Signature (X.509) - Check the box of Digital Signature to invoke this function and select one predefined Profiles set in the VPN and Remote Access >>IPsec Peer Identity. <ul style="list-style-type: none"> ■ Local ID - Specify which one will be inspected first. ■ Alternative Subject Name First - The alternative subject name (configured in Certificate Management>>Local Certificate) will be inspected first. ■ Subject Name First - The subject name (configured in Certificate Management>>Local Certificate) will be inspected first. <p>IPsec Security Method - This group of fields is a must for IPsec Tunnels and L2TP with IPsec Policy when you specify the remote node.</p> <ul style="list-style-type: none"> ● Medium- Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active. ● High- Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
TCP/IP Network Settings	<p>My WAN IP -This field is only applicable when you select PPTP or L2TP with or without IPsec policy above. The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.</p> <p>Remote Gateway IP - This field is only applicable when you select PPTP or L2TP with or without IPsec policy above. The</p>

default value is 0.0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.

Remote Network IP/ Remote Network Mask - Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPsec, this is the destination clients IDs of phase 2 quick mode.

Local Network IP / Local Network Mask - Display the local network IP and mask for TCP / IP configuration. You can modify the settings if required.

More - Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Masks through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.



RIP Direction - The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable.

From first subnet to remote network, you have to do - If the remote network only allows you to dial in with single IP, please choose **NAT**, otherwise choose **Route**.

Change default route to this VPN tunnel - Check this box to change the default route with this VPN tunnel.

IPSec VPN with the Same subnet

For both ends (e.g., different sections in a company) are within the same subnet, there is a function which allows you to build Virtual IP mapping between two ends. Thus, when VPN connection established, the router will change the IP address according to the settings configured here and block sessions which are not coming from the IP address defined in the Virtual IP Mapping list.

After checking the box of **IPSec VPN with the Same subnet**, the options under **TCP/IP Network Settings** will be changed as shown below:

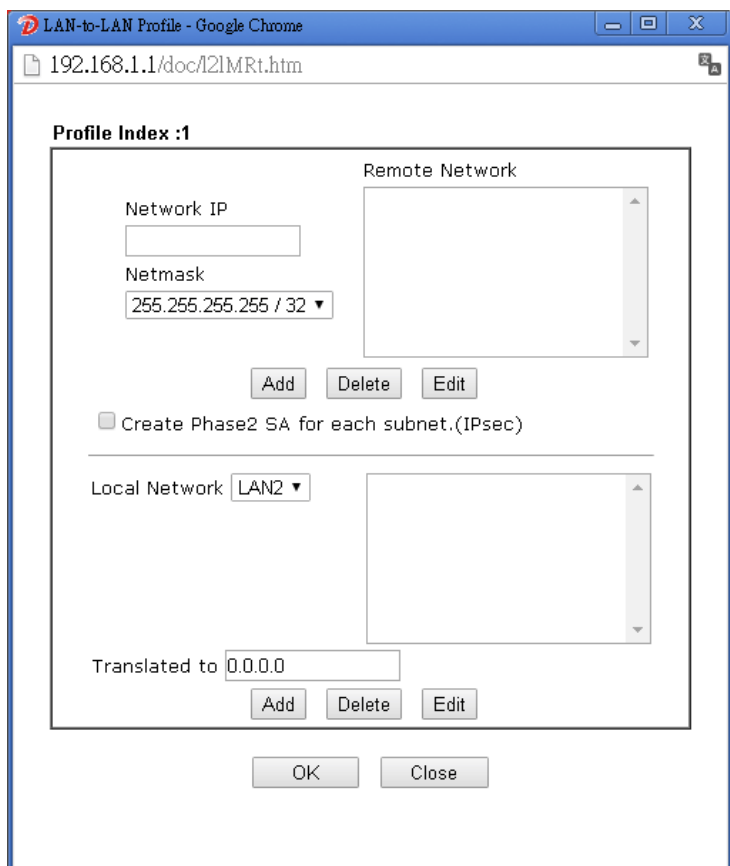
5. TCP/IP Network Settings

Remote Network IP 0.0.0.0	From Local Subnet to Remote network, you have to do
Remote Network Mask 255.255.255.0	<input type="button" value="Route"/>
<input checked="" type="checkbox"/> Translated Local Network	<input checked="" type="checkbox"/> IPsec VPN with the Same Subnets
LAN1 to	Translated Type
192.168.1.0	<input checked="" type="radio"/> Whole Subnet
<input type="button" value="Advanced"/>	<input type="radio"/> Specific IP Address
	<input type="button" value="Virtual IP Mapping"/>

Remote Network IP/ Remote Network Mask - Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPsec, this is the destination clients IDs of phase 2 quick mode.

Translated Local Network - This function is enabled in default. Use the drop down list to specify a LAN port as the transferred direction. Then specify an IP address. Click **Advanced** to configure detailed settings if required.

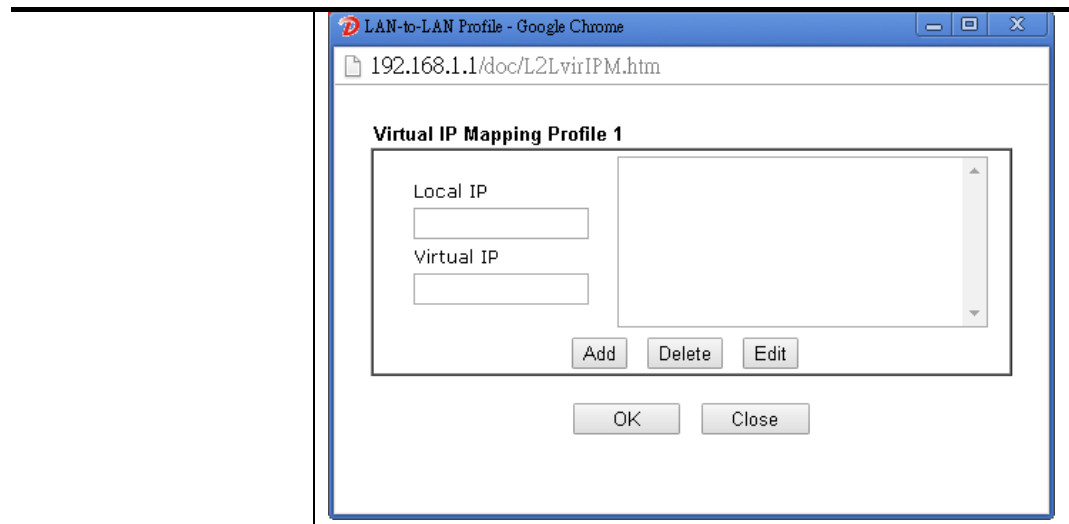
Advanced - Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.



Translated Type - There are two types for you to choose.

- Whole Subnet
- Specific IP Address

Virtual IP Mapping - A pop up dialog will appear for you to specify the local IP address and the mapping virtual IP address.



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

IV-1-9 Connection Management

You can find the summary table of all VPN connections. You may disconnect any VPN connection by clicking **Drop** button. You may also aggressively Dial-out by using Dial-out Tool and clicking **Dial** button.

VPN and Remote Access >> Connection Management

Dial-out Tool

Dial

VPN Connection Status

LAN-to-LAN VPN Status			Remote Dial-in User Status					
VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(bps)	Rx Pkts	Rx Rate(bps)	UpTime

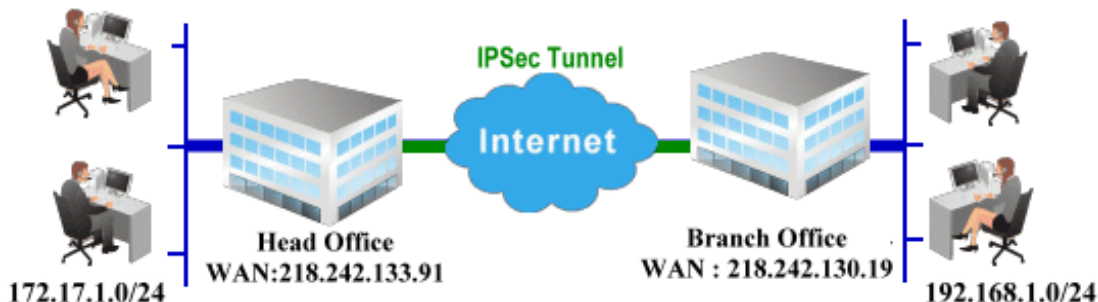
xxxxxxxx : Data is encrypted.
 xxxxxxxx : Data isn't encrypted.

Available settings are explained as follows:

Item	Description
Dial-out Tool	<p>General Mode - This field displays the profile configured in LAN-to-LAN (with Index number and VPN Server IP address). The VPN connection built by General Mode does not support VPN backup function.</p> <p>Dial - Click this button to execute dial out function.</p>

Application Notes

A-1 How to Build a LAN-to-LAN VPN Between Remote Office and Headquarter via IPsec Tunnel (Main Mode)



Configuration on Vigor Router for Head Office

1. Log into the web user interface of Vigor router.
2. Open **VPN and Remote Access >> LAN to LAN** to create a LAN-to-LAN profile. The following settings are for a permanent VPN connection.

VPN and Remote Access >> LAN to LAN

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

View: All Online Offline Trunk

Index	Name	Active	Status	Index	Name	Active	Status
1.	???	<input type="checkbox"/>	---	17.	???	<input type="checkbox"/>	---
2.	???	<input type="checkbox"/>	---	18.	???	<input type="checkbox"/>	---
3.	???	<input type="checkbox"/>	---	19.	???	<input type="checkbox"/>	---
4.	???	<input type="checkbox"/>	---	20.	???	<input type="checkbox"/>	---
5.	???	<input type="checkbox"/>	---	21.	???	<input type="checkbox"/>	---
6.	???	<input type="checkbox"/>	---	22.	???	<input type="checkbox"/>	---
7.	???	<input type="checkbox"/>	---	23.	???	<input type="checkbox"/>	---

3. Click any index number to open the configuration page. Type a name which is easy for identification for such profile (in this case, type *VPN Server*), and check the box of **Enable This Profile**. For Vigor router will be set as a **server**, the call direction shall be set as **Dial-in** and set 0 as **Idle Timeout**.

Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="VPN Server"/> <input checked="" type="checkbox"/> Enable this profile	Call Direction <input type="radio"/> Both <input type="radio"/> Dial-Out <input checked="" type="radio"/> Dial-in <input type="checkbox"/> Always on Idle Timeout <input type="text" value="0"/> second(s) <input type="checkbox"/> Enable PING to keep alive PING to the IP <input type="text"/>
VPN Dial-Out Through <input type="text" value="WAN1 First"/> Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input checked="" type="radio"/> Pass <input type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	

2. Dial-Out Settings

4. Now navigate to the next section, **Dial-In Settings** to check PPTP, IPsec Tunnel and L2TP boxes. Check the box of **Specify Remote...** and type the **Peer VPN Server IP** (e.g., 218.242.130.19 in this case). Press the **IKE Pre-Shared Key** button to set the PSK; and select **Medium (AH)** or **High (ESP)** as the security method.

3. Dial-In Settings

Allowed Dial-In Type <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input checked="" type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/>	Username <input type="text" value="???"/> Password <input type="text"/> VJ Compression <input type="radio"/> On <input checked="" type="radio"/> Off
<input checked="" type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text" value="218.242.130.19"/> or Peer ID <input type="text"/>	IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key <input type="button" value="IKE Pre-Shared Key"/> <input type="text"/> <input checked="" type="checkbox"/> Digital Signature(X.509) <input type="text" value="None"/> Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First
	IPsec Security Method <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES

4. Gre over IPsec Settings

5. Continue to navigate to the **TCP/IP Network Settings** for setting the LAN IP for remote side.

	High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
4. Gre over IPsec Settings <input type="checkbox"/> Enable IPsec Dial-Out function GRE over IPsec <input type="checkbox"/> Logical Traffic My GRE IP <input type="text"/> Peer GRE IP <input type="text"/>	
5. TCP/IP Network Settings	
My WAN IP <input type="text" value="0.0.0.0"/> Remote Gateway IP <input type="text" value="0.0.0.0"/> <input checked="" type="checkbox"/> Remote Network IP <input type="text" value="192.168.1.0"/> <input checked="" type="checkbox"/> Remote Network Mask <input type="text" value="255.255.255.0"/> Local Network IP <input type="text" value="192.168.1.9"/> Local Network Mask <input type="text" value="255.255.255.0"/> <input type="button" value="More"/>	RIP Direction <input type="text" value="Disable"/> From first subnet to remote network, you have to do <input type="text" value="Route"/> <input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)

- Click OK to save the settings.
- Open **VPN and Remote Access>>Connection Management** to check the dial-in connection status (from branch office).

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds : 5

VPN Connection Status
Current Page: 1 Page No.

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate (Bps)	Rx Pkts	Rx Rate (Bps)	UpTime
1 (VPN Server)	IPSec Tunnel DES-SHA1 Auth	218.242.130.19	192.168.1.0/24	353	3	291	3	0:13:58 <input type="button" value="Drop"/>

xxxxxxxx : Data is encrypted.
xxxxxxxx : Data isn't encrypted.

Configuration on Vigor Router for Branch Office

- Log into the web user interface of Vigor router.
- Open **VPN and Remote Access>>LAN to LAN** to create a LAN-to-LAN profile. The following settings are for a permanent VPN connection.

VPN and Remote Access >> LAN to LAN

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

View: All Online Offline Trunk

Index	Name	Active	Status	Index	Name	Active	Status
1.	???	<input type="checkbox"/>	---	17.	???	<input type="checkbox"/>	---
2.	???	<input type="checkbox"/>	---	18.	???	<input type="checkbox"/>	---
3.	???	<input type="checkbox"/>	---	19.	???	<input type="checkbox"/>	---
4.	???	<input type="checkbox"/>	---	20.	???	<input type="checkbox"/>	---
5.	???	<input type="checkbox"/>	---	21.	???	<input type="checkbox"/>	---
6.	???	<input type="checkbox"/>	---	22.	???	<input type="checkbox"/>	---
7.	???	<input type="checkbox"/>	---	23.	???	<input type="checkbox"/>	---

- Click any index number to open the configuration page. Type a name which is easy for identification for such profile (in this case, type *VPN Client*), and check the box of **Enable This Profile**. For such Vigor router will be set as a client, the call direction shall be set as **Dial-out**. Check the box of **Always on** for a permanent VPN connection.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name

Enable this profile

Call Direction Both Dial-Out Dial-in

Always on

Idle Timeout second(s)

Enable PING to keep alive

PING to the IP

VPN Dial-Out Through

Netbios Naming Packet Pass Block

Multicast via VPN Pass Block
(for some IGMP,IP-Camera,DHCP Relay..etc.)

2. Dial Out Settings

- Now navigate to the next section, **Dial-Out Settings** to select the **IPsec Tunnel** service and type the remote server IP/host name (e.g., 218.242.133.91, in this case). Press the **IKE Pre-Shared Key** button to set the PSK; and select **Medium (AH)** or **High (ESP)** as the security method.

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> PPTP <input checked="" type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy None		Username ??? Password PPP Authentication PAP/CHAP VJ Compression <input type="radio"/> On <input checked="" type="radio"/> Off
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) 218.242.133.91		IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key ●●●●●●●● <input type="radio"/> Digital Signature(X.509) Peer ID None Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First
		IPsec Security Method <input type="radio"/> Medium(AH) <input checked="" type="radio"/> High(ESP) 3DES with Authentication Advanced
Index(1-15) in Schedule Setup: , , , 		

- Continue to navigate to the **TCP/IP Network Settings** for setting the LAN IP for the remote side.

4. Gre over IPsec Settings <input type="checkbox"/> Enable IPsec Dial-Out function GRE over IPsec <input type="checkbox"/> Logical Traffic My GRE IP Peer GRE IP 	
5. TCP/IP Network Settings	
My WAN IP 0.0.0.0 Remote Gateway IP 0.0.0.0 Remote Network IP 172.17.1.0 Remote Network Mask 255.255.255.0 Local Network IP 192.168.1.9 Local Network Mask 255.255.255.0 More	RIP Direction Disable From first subnet to remote network, you have to do Route <input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)
OK Clear Cancel	

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

- Open **VPN and Remote Access >> Connection Management** to check the dial-in connection status (from head office).

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds : Refresh

Dial

VPN Connection Status

Current Page: 1 Page No. Go >>

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate (Bps)	Rx Pkts	Rx Rate (Bps)	UpTime	
1 (VPN Client)	IPSec Tunnel DES-SHA1 Auth	218.242.133.91	172.17.1.0/24	8	3	132	36	0:6:41	Drop

xxxxxxxx : Data is encrypted.
 xxxxxxxx : Data isn't encrypted.

IV-2 SSL VPN

An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser.

There are two benefits that SSL VPN provides:

- It is not necessary for users to preinstall VPN client software for executing SSL VPN connection.
- There are less restrictions for the data encrypted through SSL VPN in comparing with traditional VPN.

Web User Interface



IV-2-1 General Setup

This page determines the general configuration for SSL VPN Server and SSL Tunnel.

SSL VPN >> General Setup

SSL VPN General Setup

Bind to WAN	<input checked="" type="checkbox"/> WAN1	<input checked="" type="checkbox"/> WAN3
Port	<input type="text" value="443"/>	(Default: 443)
Server Certificate	<input type="text" value="self-signed"/> ▼	

Note:

- 1.The settings will act on all SSL applications.
- 2.Please go to **System Maintenance >> Management** to enable SSLv3.0 .
- 3.Please go to **System Maintenance >> Self-Signed Certificate** to generate a new "self-signed" certificate.

Available settings are explained as follows:

Item	Description
Bind to WAN	Choose and check WAN interface(s) for SSL VPN tunnel establishment.
Port	Such port is set for SSL VPN server. It will not affect the HTTPS Port configuration set in System Maintenance>>Management . In general, the default setting is 443.
Server Certificate	When the client does not set any certificate, default certificate will be used for HTTPS and SSL VPN server. Choose any one of the user-defined certificates from the drop down list if users set several certificates previously. Otherwise, choose Self-signed to use the router's built-in default certificate. The default certificate can be used in SSL VPN server and HTTPS Web Proxy.

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

IV-2-2 User Account

With SSL VPN, Vigor2133 series let teleworkers have convenient and simple remote access to central site VPN. The teleworkers do not need to install any VPN software manually. From regular web browser, you can establish VPN connection back to your main office even in a guest network or web cafe. The SSL technology is the same as the encryption that you use for secure web sites such as your online bank. The SSL VPN can be operated in either full tunnel mode or proxy mode. Now, Vigor2133 series allows up to 16 simultaneous incoming users.

For SSL VPN, identity authentication and power management are implemented through deploying user accounts. Therefore, the user account for SSL VPN must be set together with remote dial-in user web page. Such menu item will guide to access into VPN and Remote Access>>Remote Dial-in user.

SSL VPN >> Remote Dial-in User

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


Index	User	Active	Status	Index	User	Active	Status
1.	???	<input type="checkbox"/>	---	17.	???	<input type="checkbox"/>	---
2.	???	<input type="checkbox"/>	---	18.	???	<input type="checkbox"/>	---
3.	???	<input type="checkbox"/>	---	19.	???	<input type="checkbox"/>	---
4.	???	<input type="checkbox"/>	---	20.	???	<input type="checkbox"/>	---
5.	???	<input type="checkbox"/>	---	21.	???	<input type="checkbox"/>	---
6.	???	<input type="checkbox"/>	---	22.	???	<input type="checkbox"/>	---
7.	???	<input type="checkbox"/>	---	23.	???	<input type="checkbox"/>	---
8.	???	<input type="checkbox"/>	---	24.	???	<input type="checkbox"/>	---
9.	???	<input type="checkbox"/>	---	25.	???	<input type="checkbox"/>	---
10.	???	<input type="checkbox"/>	---	26.	???	<input type="checkbox"/>	---
11.	???	<input type="checkbox"/>	---	27.	???	<input type="checkbox"/>	---
12.	???	<input type="checkbox"/>	---	28.	???	<input type="checkbox"/>	---
13.	???	<input type="checkbox"/>	---	29.	???	<input type="checkbox"/>	---
14.	???	<input type="checkbox"/>	---	30.	???	<input type="checkbox"/>	---
15.	???	<input type="checkbox"/>	---	31.	???	<input type="checkbox"/>	---
16.	???	<input type="checkbox"/>	---	32.	???	<input type="checkbox"/>	---

Note:

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

Download Smart VPN Client:

 [Smart VPN Client for Windows PC](#)

 [Smart VPN Android/iOS App](#)

Click each index to edit one remote user profile.

SSL VPN >> Remote Dial-in User

Index No. 1

<p>User account and Authentication</p> <p><input type="checkbox"/> Enable this account</p> <p>Idle Timeout <input type="text" value="300"/> second(s)</p> <hr/> <p>Allowed Dial-In Type</p> <p><input checked="" type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> IPsec Tunnel</p> <p><input checked="" type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/></p> <p><input checked="" type="checkbox"/> SSL Tunnel</p> <p><input type="checkbox"/> Specify Remote Node</p> <p>Remote Client IP <input type="text"/></p> <p>or Peer ID <input type="text"/></p> <p>Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block</p> <p>Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block</p> <p><small>(for some IGMP,IP-Camera,DHCP Relay...etc.)</small></p> <hr/> <p>Subnet</p> <p><input type="text" value="LAN 1"/></p> <p><input type="checkbox"/> Assign Static IP Address</p> <p><input type="text" value="0.0.0.0"/></p>	<p>Username <input style="width: 100px;" type="text" value="???"/></p> <p>Password(Max 19 char) <input style="width: 100px;" type="text"/></p> <p><input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP)</p> <p>PIN Code <input style="width: 100px;" type="text"/></p> <p>Secret <input style="width: 100px;" type="text"/></p> <hr/> <p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p><input style="width: 100px;" type="text" value="IKE Pre-Shared Key"/></p> <p><input type="checkbox"/> Digital Signature(X.509)</p> <p><input type="text" value="None"/></p> <hr/> <p>IPsec Security Method</p> <p><input checked="" type="checkbox"/> Medium(AH)</p> <p>High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p> <p>Local ID (optional) <input style="width: 100px;" type="text"/></p>
---	--

Available settings are explained as follows:

Item	Description
<p>User account and Authentication</p>	<p>Enable this account - Check the box to enable this function.</p> <p>Idle Timeout- If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.</p> <p>User Name - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the name/password is limited to 23 characters.</p> <p>Password - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the name/password is limited to 19 characters.</p> <p>Enable Mobile One-Time Passwords (mOTP) - Check this box to make the authentication with mOTP function.</p> <p>PIN Code - Type the code for authentication (e.g, 1234).</p> <p>Secret - Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).</p>
<p>Allowed Dial-In Type</p>	<p>PPTP - Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.</p> <p>IPSec Tunnel - Allow the remote dial-in user to make an IPsec VPN connection through Internet.</p> <p>L2TP with IPsec Policy - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below:</p>

Item	Description
	<ul style="list-style-type: none"> ● None - Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. ● Nice to Have - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. ● Must -Specify the IPSec policy to be definitely applied on the L2TP connection. <p>SSL Tunnel - It allows the remote dial-in user to make an SSL VPN Tunnel connection through Internet, suitable for the application through network accessing (e.g., PPTP / L2TP / IPSec).</p> <p>If you check this box, the function of SSL Tunnel for this account will be activated immediately.</p> <p>Specify Remote Node - Check the checkbox to specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode). If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings.</p> <p>Netbios Naming Packet</p> <ul style="list-style-type: none"> ● Pass - Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. ● Block - When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel. <p>Multicast via VPN - Some programs might send multicast packets via VPN connection.</p> <ul style="list-style-type: none"> ● Pass - Click this button to let multicast packets pass through the router. ● Block - This is default setting. Click this button to let multicast packets be blocked by the router.
Subnet	<p>Chose one of the subnet selections for such VPN profile.</p> <p>Assign Static IP Address - Please type a static IP address for the subnet you specified.</p>
IKE Authentication Method	<p>This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node.</p> <p>Pre-Shared Key - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key.</p> <p>Digital Signature (X.509) - Check the box of Digital Signature to invoke this function and Select one predefined Profiles set in the VPN and Remote Access >>IPSec Peer Identity.</p>
IPSec Security Method	<p>This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method.</p> <p>Medium-Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is</p>

Item	Description
	<p>invoked. You can uncheck it to disable it.</p> <p>High-Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.</p> <p>Local ID - Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.</p>

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

IV-2-3 Online User Status

If you have finished the configuration of SSL Web Proxy (server), users can find out corresponding settings when they access into DrayTek SSL VPN portal interface.

DrayTek

Provide SSL VPN

The screenshot shows the DrayTek SSL VPN portal interface. At the top, there are navigation tabs for 'Home', 'SSL Web Proxy', and 'SSL Tunnel', along with a '[logout]' link. The main content area displays a 'Main Page:' with a message: 'You have successfully logged in! You are given the following privileges:'. Below this, there is a list of privileges: 'SSL Web Proxy' and 'SSL Tunnel'. On the left side, there is an 'INFO' box containing the user's name 'mike', IP address '(172.17.1.42)', and a welcome message. At the bottom of the INFO box, it says 'Timeout after 5 minutes.' and includes a '[Reset]' link. The footer of the page reads 'Copyright © 2006, DrayTek Corp. All Rights Reserved.'

Next, users can open SSL VPN>> Online Status to view logging status of SSL VPN.

SSL VPN >> Online User Status

Refresh Seconds :

Active User	Host IP	Time out(seconds)	Action
Kate	192.168.30.14	299	<input type="button" value="Drop"/>

Available settings are explained as follows:

Item	Description
Active User	Display current user who visits SSL VPN server.
Host IP	Display the IP address for the host.
Time out	Display the time remaining for logging out.
Action	You can click Drop to drop certain login user from the router's SSL Portal UI.

IV-3 Certificate Management

A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Here Vigor router support digital certificates conforming to standard X.509.

Any entity wants to utilize digital certificates should first request a certificate issued by a CA server. It should also retrieve certificates of other trusted CA servers so it can authenticate the peer with certificates issued by those trusted CA servers.

Here you can manage generate and manage the local digital certificates, and set trusted CA certificates. Remember to adjust the time of Vigor router before using the certificate so that you can get the correct valid period of certificate.

Below shows the menu items for Certificate Management.

Web User Interface

VPN and Remote Access
Certificate Management
Local Certificate
Trusted CA Certificate
Certificate Backup
SSL VPN

IV-3-1 Local Certificate

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify	
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>

Note:

1. Please setup the "System Maintenance >> **Time and Date**" correctly before signing the local certificate.
2. The Time Zone MUST be setup correctly!!

Available settings are explained as follows:

Item	Description
Generate	Click this button to open Generate Certificate Request window. Type in all the information that the window requests. Then click Generate again.
Import	Click this button to import a saved file as the certification information.
Refresh	Click this button to refresh the information listed below.
View	Click this button to view the detailed settings for certificate request.
Delete	Click this button to delete selected name with certification information.

GENERATE

Click this button to open **Generate Certificate Signing Request** window. Type in all the information that the window request such as certificate name (used for identifying different certificate), subject alternative name type and relational settings for subject name. Then click **GENERATE** again.

Generate Certificate Signing Request

Certificate Name	<input type="text"/>
Subject Alternative Name	
Type	IP Address ▼
IP	<input type="text"/>
Subject Name	
Country (C)	<input type="text"/>
State (ST)	<input type="text"/>
Location (L)	<input type="text"/>
Organization (O)	<input type="text"/>
Organization Unit (OU)	<input type="text"/>
Common Name (CN)	<input type="text"/>
Email (E)	<input type="text"/>
Key Type	RSA ▼
Key Size	1024 Bit ▼
Algorithm	SHA-256 ▼

Generate



Info

Please be noted that "Common Name" must be configured with router's WAN IP or domain name.

After clicking **GENERATE**, the generated information will be displayed on the window below:

X509 Local Certificate Configuration

Name	Subject	Status	Modify	
server	/C=TW/ST=Hsinchu/L=Hsinchu/O...	Requesting	View	Delete
---	---	---	View	Delete
---	---	---	View	Delete

[GENERATE](#) [IMPORT](#) [REFRESH](#)

IMPORT

Vigor router allows you to generate a certificate request and submit it the CA server, then import it as "Local Certificate". If you have already gotten a certificate from a third party, you may import it directly. The supported types are PKCS12 Certificate and Certificate with a private key.

Click this button to import a saved file as the certification information. There are three types of local certificate supported by Vigor router.

Import X509 Local Certificate

Upload Local Certificate
 Select a local certificate file.
 Certificate file:
 Click **Import** to upload the local certificate.

Upload PKCS12 Certificate
 Select a PKCS12 file.
 PKCS12 file:
 Password:
 Click **Import** to upload the PKCS12 file.

Upload Certificate and Private Key
 Select a certificate file and a matchable Private Key.
 Certificate file:
 Key file:
 Password:
 Click **Import** to upload the local certificate and private key.

Available settings are explained as follows:

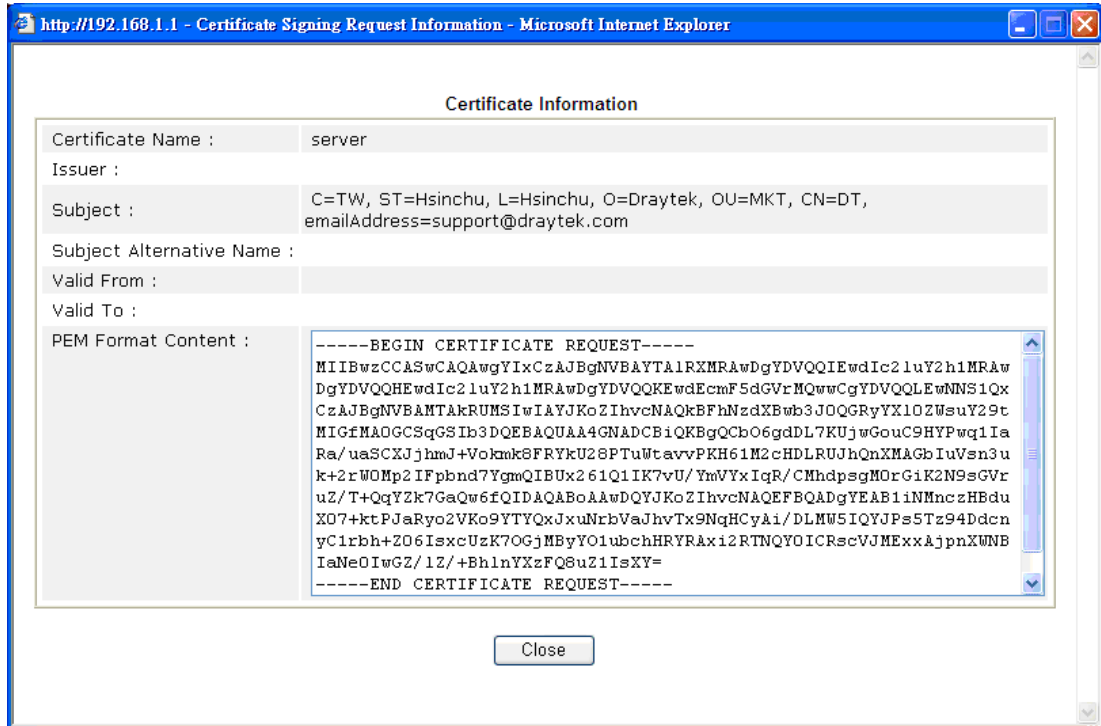
Item	Description																
Upload Local Certificate	<p>It allows users to import the certificate which is generated by Vigor router and signed by CA server.</p> <p>If you have done well in certificate generation, the Status of the certificate will be shown as "OK".</p> <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> <p style="color: red; font-size: small;">Import X509 Local Certificate</p> <p style="text-align: center;">Congratulation!</p> <p style="text-align: center; font-size: x-small;">Local Certificate has been imported successfully.</p> <p style="text-align: center; font-size: x-small;">Please click <input type="button" value="Back"/> to view the certificate.</p> </div> <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> <p style="color: red; font-size: small;">X509 Local Certificate Configuration</p> <table border="1" style="width: 100%; border-collapse: collapse; font-size: x-small;"> <thead> <tr> <th style="text-align: left;">Name</th> <th style="text-align: left;">Subject</th> <th style="text-align: left;">Status</th> <th style="text-align: left;">Modify</th> </tr> </thead> <tbody> <tr> <td>draytekdemo</td> <td>/O=Draytek/OU=Draytek Sales/...</td> <td>OK</td> <td><input type="button" value="View"/> <input type="button" value="Delete"/></td> </tr> <tr> <td>---</td> <td>---</td> <td>---</td> <td><input type="button" value="View"/> <input type="button" value="Delete"/></td> </tr> <tr> <td>---</td> <td>---</td> <td>---</td> <td><input type="button" value="View"/> <input type="button" value="Delete"/></td> </tr> </tbody> </table> <p style="text-align: center; font-size: x-small;"> <input type="button" value="GENERATE"/> <input type="button" value="IMPORT"/> <input type="button" value="REFRESH"/> </p> </div>	Name	Subject	Status	Modify	draytekdemo	/O=Draytek/OU=Draytek Sales/...	OK	<input type="button" value="View"/> <input type="button" value="Delete"/>	---	---	---	<input type="button" value="View"/> <input type="button" value="Delete"/>	---	---	---	<input type="button" value="View"/> <input type="button" value="Delete"/>
Name	Subject	Status	Modify														
draytekdemo	/O=Draytek/OU=Draytek Sales/...	OK	<input type="button" value="View"/> <input type="button" value="Delete"/>														
---	---	---	<input type="button" value="View"/> <input type="button" value="Delete"/>														
---	---	---	<input type="button" value="View"/> <input type="button" value="Delete"/>														
Upload PKCS12 Certificate	<p>It allows users to import the certificate whose extensions are usually .pfx or .p12. And these certificates usually need passwords.</p> <p>Note that PKCS12 is a standard for storing private keys and certificates securely. It is used in (among other things) Netscape and Microsoft Internet Explorer with their import and export options.</p>																
Upload Certificate and Private Key	<p>It is useful when users have separated certificates and private keys. And the password is needed if the private key is encrypted.</p>																

REFRESH

Click this button to refresh the information listed below.

View

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



Info

You have to copy the certificate request information from above window. Next, access your CA server and enter the page of certificate request, copy the information into it and submit a request. A new certificate will be issued to you by the CA server. You can save it.

Delete

Click this button to remove the selected certificate.

IV-3-2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate. In addition, you can build a RootCA certificate if required.

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

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



Info

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

Certificate Management >> Trusted CA Certificate

X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify
Root CA	---	---	<input type="button" value="Create"/>
Trusted CA-1	---	---	<input type="button" value="View"/> <input type="button" value="Delete"/>
Trusted CA-2	---	---	<input type="button" value="View"/> <input type="button" value="Delete"/>
Trusted CA-3	---	---	<input type="button" value="View"/> <input type="button" value="Delete"/>

Note:

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

Creating a Root CA

Click Create to open the following page. Type in all the information that the window request such as certificate name (used for identifying different certificate), subject alternative name type and relational settings for subject name. Then click Generate again.

Generate Root CA

Certificate Name	Root CA
Subject Alternative Name	
Type	IP Address ▼
IP	<input type="text"/>
Subject Name	
Country (C)	<input type="text"/>
State (ST)	<input type="text"/>
Location (L)	<input type="text"/>
Organization (O)	<input type="text"/>
Organization Unit (OU)	<input type="text"/>
Common Name (CN)	<input type="text"/>
Email (E)	<input type="text"/>
Key Type	RSA ▼
Key Size	1024 Bit ▼
Algorithm	SHA-256 ▼

Importing a Trusted CA

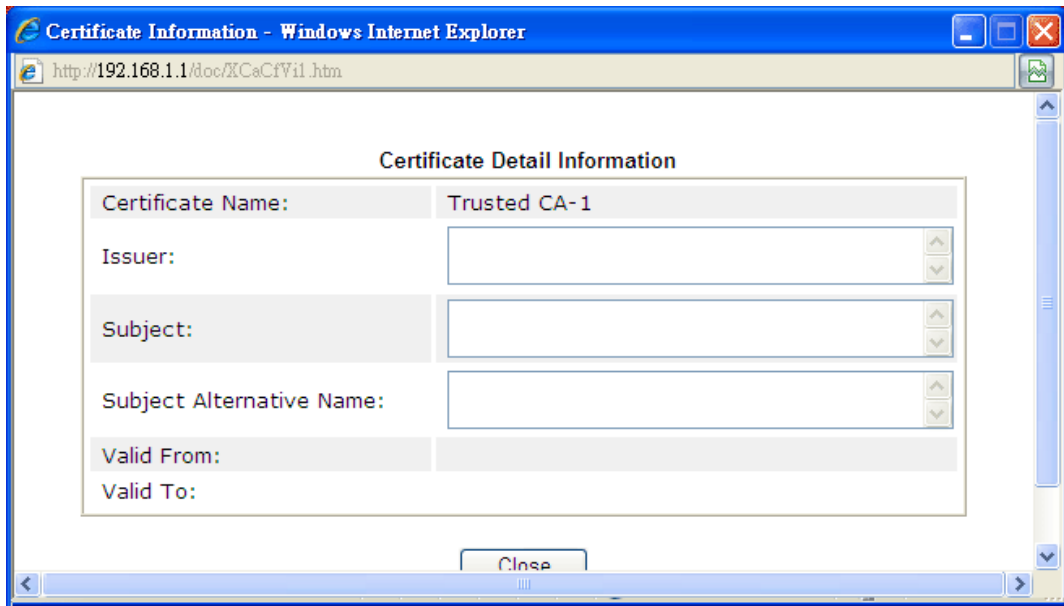
To import a pre-saved trusted CA certificate, please click **IMPORT** to open the following window. Use **Browse...** to find out the saved text file. Then click **Import**. The one you imported will be listed on the Trusted CA Certificate window.

Import X509 Trusted CA Certificate

Select a trusted CA certificate file.

Click [Import](#) to upload the certification.

For viewing each trusted CA certificate, click **View** to open the certificate detail information window. If you want to delete a CA certificate, choose the one and click **Delete** to remove all the certificate information.



IV-3-3 Certificate Backup

Local certificate and Trusted CA certificate for this router can be saved within one file. Please click **Backup** on the following screen to save them. If you want to set encryption password for these certificates, please type characters in both fields of **Encrypt password** and **Confirm password**.

Also, you can use **Restore** to retrieve these two settings to the router whenever you want.

Certificate Management >> Certificate Backup

Certificate Backup / Restoration

Backup

Encrypt password:

Confirm password:

Click to download certificates to your local PC as a file.

Restoration

Select a backup file to restore.

Decrypt password:

Click to upload the file.

Part V Security



Firewall



CSM

While the broadband users demand more bandwidth for multimedia, interactive applications, or distance learning, security has been always the most concerned. The firewall of the Vigor router helps to protect your local network against attack from unauthorized outsiders. It also restricts users in the local network from accessing the Internet.

CSM is an abbreviation of Central Security Management which is used to control IM/P2P usage, filter the web content and URL content to reach a goal of security management.

V-1 Firewall

While the broadband users demand more bandwidth for multimedia, interactive applications, or distance learning, security has been always the most concerned. The firewall of the Vigor router helps to protect your local network against attack from unauthorized outsiders. It also restricts users in the local network from accessing the Internet. Furthermore, it can filter out specific packets that trigger the router to build an unwanted outgoing connection.

Firewall Facilities

The users on the LAN are provided with secured protection by the following firewall facilities:

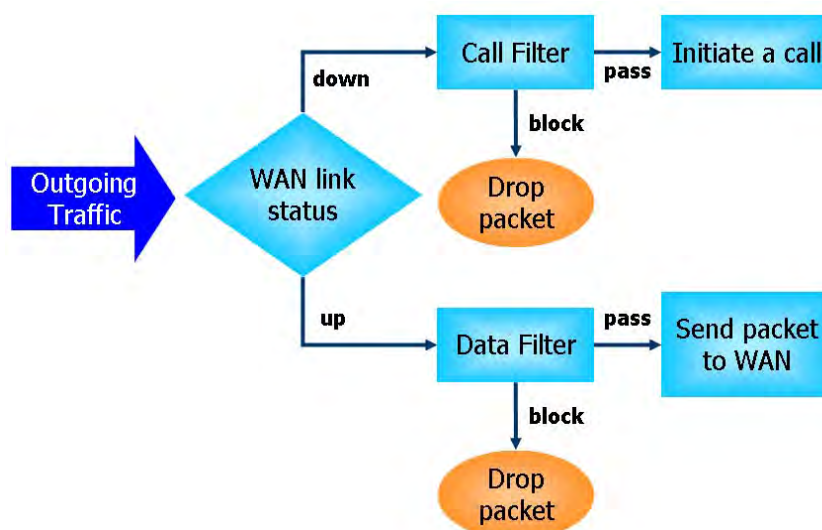
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

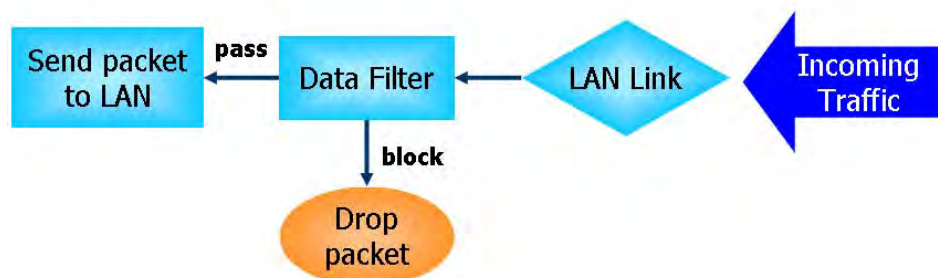
IP Filters

Depending on whether there is an existing Internet connection, or in other words "the WAN link status is up or down", the IP filter architecture categorizes traffic into two: **Call Filter** and **Data Filter**.

- **Call Filter** - When there is no existing Internet connection, **Call Filter** is applied to all traffic, all of which should be outgoing. It will check packets according to the filter rules. If legal, the packet will pass. Then the router shall "initiate a call" to build the Internet connection and send the packet to Internet.
- **Data Filter** - When there is an existing Internet connection, **Data Filter** is applied to incoming and outgoing traffic. It will check packets according to the filter rules. If legal, the packet will pass the router.

The following illustrations are flow charts explaining how router will treat incoming traffic and outgoing traffic respectively.





Stateful Packet Inspection (SPI)

Stateful inspection is a firewall architecture that works at the network layer. Unlike legacy static packet filtering, which examines a packet based on the information in its header, stateful inspection builds up a state machine to track each connection traversing all interfaces of the firewall and makes sure they are valid. The stateful firewall of Vigor router not only examines the header information also monitors the state of the connection.

Denial of Service (DoS) Defense

The DoS Defense functionality helps you to detect and mitigate the DoS attack. The attacks are usually categorized into two types, the flooding-type attacks and the vulnerability attacks. The flooding-type attacks will attempt to exhaust all your system's resource while the vulnerability attacks will try to paralyze the system by offending the vulnerabilities of the protocol or operation system.

The DoS Defense function enables the Vigor router to inspect every incoming packet based on the attack signature database. Any malicious packet that might duplicate itself to paralyze the host in the secure LAN will be strictly blocked and a Syslog message will be sent as warning, if you set up Syslog server.

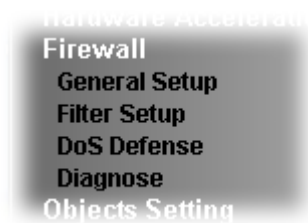
Also the Vigor router monitors the traffic. Any abnormal traffic flow violating the pre-defined parameter, such as the number of thresholds, is identified as an attack and the Vigor router will activate its defense mechanism to mitigate in a real-time manner.

The below shows the attack types that DoS/DDoS defense function can detect:

- | | |
|----------------------|--------------------------|
| 1. SYN flood attack | 9. SYN fragment |
| 2. UDP flood attack | 10. Fraggle attack |
| 3. ICMP flood attack | 11. TCP flag scan |
| 4. Port Scan attack | 12. Tear drop attack |
| 5. IP options | 13. Ping of Death attack |
| 6. Land attack | 14. ICMP fragment |
| 7. Smurf attack | 15. Unassigned Numbers |
| 8. Trace route | |

Web User Interface

Below shows the menu items for Firewall.



V-1-1 General Setup

General Setup allows you to adjust settings of IP Filter and common options. Here you can enable or disable the **Call Filter** or **Data Filter**. Under some circumstance, your filter set can be linked to work in a serial manner. So here you assign the **Start Filter Set** only. Also you can configure the **Log Flag** settings, **Apply IP filter to VPN incoming packets**, and **Accept incoming fragmented UDP packets**.

Click **Firewall** and click **General Setup** to open the general setup page.

General Setup Page

Such page allows you to enable / disable Call Filter and Data Filter, determine general rule for filtering the incoming and outgoing data.

Firewall >> General Setup

General Setup

General Setup	Default Rule	
Call Filter	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Start Filter Set: <input type="text" value="Set#1"/>
Data Filter	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Start Filter Set: <input type="text" value="Set#2"/>
<input checked="" type="checkbox"/> Always pass inbound fragmented large packets (required for certain games and streaming)		
<input checked="" type="checkbox"/> Enable Strict Security Firewall		
Block connections initiated from WAN: <input type="checkbox"/> IPv4 <input checked="" type="checkbox"/> IPv6		

Note:

Packets are filtered by firewall functions in the following order:
 1.Data Filter Sets and Rules 2.Block connections initiated from WAN 3.Default Rule

Backup Firewall: <input type="button" value="Backup"/>	Restore Firewall: <input type="button" value="選擇檔案"/> 未選擇任何檔案	<input type="button" value="Restore"/>
--	---	--

Note:

This will not backup the detail setting of Quality of Service and Schedule.

Available settings are explained as follows:

Item	Description
Call Filter	Check Enable to activate the Call Filter function. Assign a start filter set for the Call Filter.

Data Filter	Check Enable to activate the Data Filter function. Assign a start filter set for the Data Filter.
Always pass inbound fragmented large packets...	Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor router will reject these fragmented packets to prevent attack unless you enable " Always pass inbound fragmented large packets... ". By checking this box, you can play these kinds of on-line games. If security concern is in higher priority, you cannot enable " Always pass inbound fragmented large packets... ".
Enable Strict Security Firewall	For the sake of security, the router will execute strict security checking for data transmission. Such feature is enabled in default. All the packets, while transmitting through Vigor router, will be filtered by firewall. If the firewall system (e.g., content filter server) does not make any response (pass or block) for these packets, then the router's firewall will block the packets directly.
Block routing connections initiated from WAN	Usually, IPv6 network sessions/traffic from WAN to LAN will be accepted by IPv6 firewall in default. IPv6 - To prevent remote client accessing into the PCs on LAN, check the box to make the packets (routed from WAN to LAN) via IPv6 being blocked by such router. It is effective only for the packets routed but not for packets translated by NAT. IPv4 - To prevent remote client accessing into the PCs on LAN, check the box to make the incoming packets via IPv4 being blocked by such router. It is effective only for the packets routed but not for packets translated by NAT.
Backup Firewall	Click Backup to save the firewall configuration.
Restore Firewall	Click Select to choose a firewall configuration file. Then click Restore to apply the file.

Default Rule Page

Such page allows you to choose filtering profiles including QoS, Load-Balance policy, WCF, APP Enforcement, URL Content Filter, for data transmission via Vigor router.

Firewall >> General Setup

General Setup

General Setup Default Rule

Actions for default rule:

Application	Action/Profile	Syslog
Filter	Pass <input type="button" value="v"/>	<input type="checkbox"/>
Sessions Control	0 / 32000 <input type="text"/>	<input type="checkbox"/>
Quality of Service	None <input type="button" value="v"/>	<input type="checkbox"/>
APP Enforcement	None <input type="button" value="v"/>	<input type="checkbox"/>
URL Content Filter	None <input type="button" value="v"/>	<input type="checkbox"/>
Web Content Filter	None <input type="button" value="v"/>	<input type="checkbox"/>
DNS Filter	None <input type="button" value="v"/>	<input type="checkbox"/>

Advance Setting

Backup Firewall : Restore Firewall:

Note:

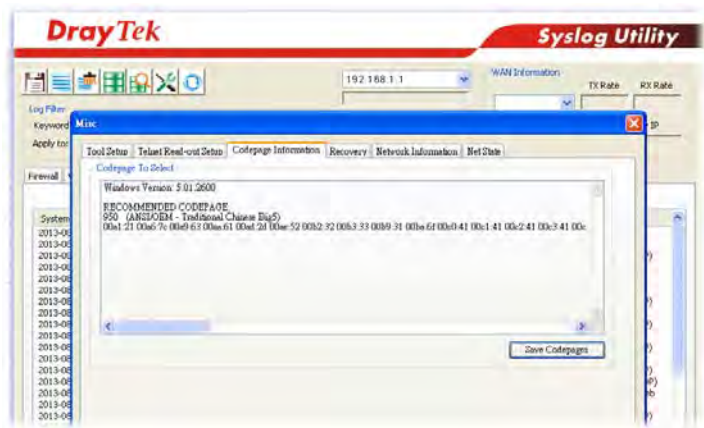
This will not backup the detail setting of Quality of Service and Schedule.

Available settings are explained as follows:

Item	Description
Filter	<p>Select Pass or Block for the packets that do not match with the filter rules.</p> <p>Filter <input type="button" value="Pass v"/></p> <div style="border: 1px solid black; padding: 2px; display: inline-block;"> Pass Block </div>
Sessions Control	<p>The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.</p>
Quality of Service	<p>Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later.</p> <div style="border: 1px solid black; padding: 2px; display: inline-block;"> None <input type="button" value="v"/> None Class 1 Class 2 Class 3 Default </div>

APP Enforcement	<p>Select an APP Enforcement profile for global IM/P2P application blocking. If there is no profile for you to select, please choose [Create New] from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the APP Enforcement profile selected here. For detailed information, refer to the section of APP Enforcement profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p>
URL Content Filter	<p>Select one of the URL Content Filter profile settings (created in CSM>> URL Content Filter) for applying with this router. Please set at least one profile for choosing in CSM>> URL Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for URL Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p>
Web Content Filter	<p>Select one of the Web Content Filter profile settings (created in CSM>> Web Content Filter) for applying with this router. Please set at least one profile for anti-virus in CSM>> Web Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for Web Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p>
DNS Filter	<p>Select one of the DNS Filter profile settings (created in CSM>>DNS Filter) for applying with this router. Please set at least one profile in CSM>> Web Content Filter web page first. Or click the DNS Filter link in this page to create a new profile.</p>
Advance Setting	<p>Click Edit to open the following window. However, it is strongly recommended to use the default settings here.</p> <div data-bbox="710 1397 1385 1693" style="border: 1px solid #ccc; padding: 10px;"> <p>Firewall >> General Setup</p> <hr/> <p>Advance Setting</p> <p>Codepage: <input type="text" value="ANSI(1252)-Latin I"/> ▼</p> <p>Window size: <input type="text" value="65535"/></p> <p>Session timeout: <input type="text" value="1440"/> Minute</p> <p style="text-align: center;"> <input type="button" value="OK"/> <input type="button" value="Close"/> </p> </div> <p>Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtain correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage.</p> <p>If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the</p>

dialog box.



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

Session timeout - Setting timeout for sessions can make the best utilization of network resources.

Backup Firewall	Click Backup to save the firewall configuration.
Restore Firewall	Click Select to choose a firewall configuration file. Then click Restore to apply the file.

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

V-1-2 Filter Setup

Click Firewall and click Filter Setup to open the setup page.

Firewall >> Filter Setup

Filter Setup				Set to Factory Default
Set	Comments	Set	Comments	
1.	Default Call Filter	7.		
2.	Default Data Filter	8.		
3.		9.		
4.		10.		
5.		11.		
6.		12.		

To edit or add a filter, click on the set number to edit the individual set. The following page will be shown. Each filter set contains up to 7 rules. Click on the rule number button to edit each rule. Check Active to enable the rule.

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1
 Comments :

Rule	Active	Comments	Direction	Src IP	Dst IP	Service Type	Action	CSM	Move Up	Move Down
1	<input checked="" type="checkbox"/>	Block NetBios	LAN/DMZ/RT/VPN -> WAN	Any	Any	TCP/UDP, Port: from 137~139 to any	Block Immediately			Down
2	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
3	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
4	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
5	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
6	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
7	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	

Filter Set [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) Next Filter Set

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

Available settings are explained as follows:

Item	Description
Filter Rule	Click a button numbered (1 ~ 7) to edit the filter rule. Click the button will open Edit Filter Rule web page. For the detailed information, refer to the following page.
Active	Enable or disable the filter rule.
Comment	Enter filter set comments/description. Maximum length is 23-character long.
Direction	Display the direction of packet.
Src IP / Dst IP	Display the IP address of source /destination.
Service Type	Display the type and port number of the packet.

Action	Display the packets to be passed /blocked.
CSM	Display the content security managed
Move Up/Down	Use Up or Down link to move the order of the filter rules.
Next Filter Set	Set the link to the next filter set to be executed after the current filter run. Do not make a loop with many filter sets.
Wizard Mode	Allow to configure frequently used settings for filter rule via several setting pages.
Advance Mode	Allow to configure detailed settings of filter rule.

To use Wizard Mode, simple do the following steps:

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

Firewall >> Edit Filter Set >> Edit Filter Rule Wizard

Filter Set 1 Rule 1

Firewall Rule applies to packets that meet the following criteria

Comments:

Direction:

Source IP:

Start IP Address:

End IP Address:

Subnet Mask:

Destination IP:

Start IP Address:

End IP Address:

Subnet Mask:

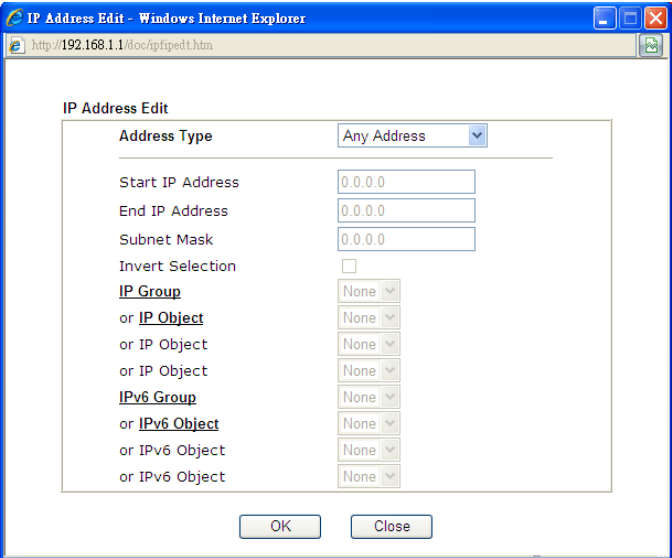
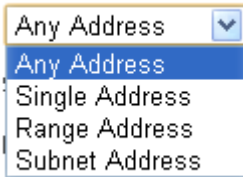
Protocol:

Source Port:

Destination Port:

Available settings are explained as follows:

Item	Description
Comments	Enter filter set comments/description. Maximum length is 14- character long.
Direction	Set the direction of packet flow. It is for Data Filter only. For the Call Filter , this setting is not available since Call Filter is only applied to outgoing traffic. Note: RT means routing domain for 2nd subnet or other LAN.

<p>Source/Destination IP</p>	<p>Click Edit to access into the following dialog to choose the source/destination IP or IP ranges.</p>  <p>To set the IP address manually, please choose Any Address/Single Address/Range Address/Subnet Address as the Address Type and type them in this dialog.</p> 
<p>Protocol</p>	<p>Specify the protocol(s) which this filter rule will apply to.</p>
<p>Source Port / Destination Port</p>	<p>(=) - when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type.</p> <p>(!=) - when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.</p> <p>(>) - the port number greater than this value is available.</p> <p>(<) - the port number less than this value is available for this profile.</p>

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

Filter Set 1 Rule 1

Based on the settings in the previous pages, we guess you want to have: **Pass**
 The current setting is :

Pass Immediately

APP Enforcement:

URL Content Filter:

Web Content Filter:

DNS Filter:

Block Immediately

Available settings are explained as follows:

Item	Description
Pass Immediately	<p>Packets matching the rule will be passed immediately.</p> <p>APP Enforcement - Select an APP Enforcement profile for global IM/P2P application blocking. If there is no profile for you to select, please choose [Create New] from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the APP Enforcement profile selected here. For detailed information, refer to the section of APP Enforcement profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p> <p>URL Content Filter - Select one of the URL Content Filter profile settings (created in CSM>> URL Content Filter) for applying with this router. Please set at least one profile for choosing in CSM>> URL Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for URL Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p> <p>Web Content Filter - Select one of the Web Content Filter profile settings (created in CSM>> Web Content Filter) for applying with this router. Please set at least one profile for anti-virus in CSM>> Web Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for Web Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p> <p>DNS Filter - Select one of the DNS Filter profile settings (created in CSM>>DNS Filter) for applying with this router. Please set at least one profile in CSM>> Web Content Filter web page first. Or click the DNS Filter link from the drop down list in this page to create a new profile.</p>
Block Immediately	<p>Packets matching the rule will be dropped immediately.</p>

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

Firewall >> Edit Filter Set >> Edit Filter Rule Wizard

Filter Set 1 Rule 1 Configuration Summary

Comments :	Block NetBios
Direction	
LAN/RT/VPN -> WAN	
Criteria	
Source IP	Any
Destination IP	Any
Protocol	TCP/UDP, Port: from 137 ~ 139 to any
More options	
Pass Immediately	
APP Enforcement :	None
URL Content Filter :	None
Web Content Filter :	1 - Default
DNS Filter :	None

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

To use **Advance Mode**, do the following steps:

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

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 1

Check to enable the Filter Rule

Comments: Block NetBios

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

Clear sessions when schedule ON: Enable

Direction: LAN/RT/VPN -> WAN

Source IP: Any [Edit]

Destination IP: Any [Edit]

Service Type: TCP/UDP, Port: from 137~139 to any [Edit]

Fragments: Don't Care

Application	Action/Profile	Syslog
Filter	Block Immediately	<input type="checkbox"/>
Branch to Other Filter Set	None	
Sessions Control	0 / 32000	<input type="checkbox"/>
MAC Bind IP	Non-Strict	<input type="checkbox"/>
Quality of Service	None	<input type="checkbox"/>
APP Enforcement	None	<input type="checkbox"/>
URL Content Filter	None	<input type="checkbox"/>
Web Content Filter	None	<input type="checkbox"/>
DNS Filter	None	<input type="checkbox"/>

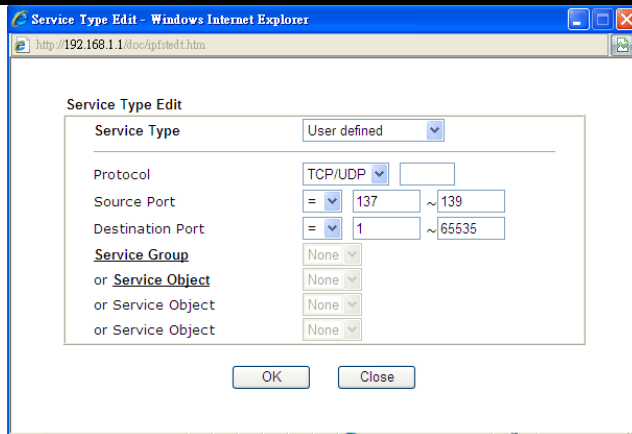
Advance Setting [Edit]

OK Clear Cancel

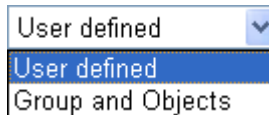
Available settings are explained as follows:

Item	Description
Check to enable the Filter Rule	Check this box to enable the filter rule.
Comments	Enter filter set comments/description. Maximum length is 14- character long.
Index(1-15)	Set PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in Applications >> Schedule setup. The default setting of this field is blank and the function will always work.
Clear sessions when schedule ON	Check this box to clear the sessions when the above schedule profiles are applied.
Direction	Set the direction of packet flow. It is for Data Filter only. For the Call Filter , this setting is not available since Call Filter is only applied to outgoing traffic.

	<div data-bbox="699 203 1098 349" style="border: 1px solid black; padding: 2px;"> LAN/RT/VPN -> WAN LAN/RT/VPN -> WAN WAN -> LAN/RT/VPN LAN/RT/VPN -> LAN/RT/VPN </div> <p>Note: RT means routing domain for 2nd subnet or other LAN.</p>
<p>Source/Destination IP</p>	<p>Click Edit to access into the following dialog to choose the source/destination IP or IP ranges.</p> <div data-bbox="699 506 1374 1059" style="border: 1px solid black; padding: 5px;"> </div> <p>To set the IP address manually, please choose Any Address/Single Address/Range Address/Subnet Address as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose Group and Objects as the Address Type.</p> <div data-bbox="699 1261 970 1469" style="border: 1px solid black; padding: 2px;"> Group and Objects Any Address Single Address Range Address Subnet Address Group and Objects </div> <p>From the IP Group drop down list, choose the one that you want to apply. Or use the IP Object drop down list to choose the object that you want.</p>
<p>Service Type</p>	<p>Click Edit to access into the following dialog to choose a suitable service type.</p>



To set the service type manually, please choose **User defined** as the Service Type and type them in this dialog. In addition, if you want to use the service type from defined groups or objects, please choose **Group and Objects** as the Service Type.



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

Source/Destination Port -

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

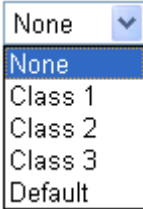
(!=) - when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.

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

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

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

<p>Fragments</p>	<p>Specify the action for fragmented packets. And it is used for Data Filter only.</p> <p>Don't care -No action will be taken towards fragmented packets.</p> <p>Unfragmented -Apply the rule to unfragmented packets.</p> <p>Fragmented - Apply the rule to fragmented packets.</p> <p>Too Short - Apply the rule only to packets that are too short to contain a complete header.</p>
<p>Filter</p>	<p>Specifies the action to be taken when packets match the rule.</p> <p>Block Immediately - Packets matching the rule will be dropped immediately.</p> <p>Pass Immediately - Packets matching the rule will be passed immediately.</p> <p>Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped.</p>

	Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through.
Branch to other Filter Set	If the packet matches the filter rule, the next filter rule will branch to the specified filter set. Select next filter rule to branch from the drop-down menu. Be aware that the router will apply the specified filter rule for ever and will not return to previous filter rule any more.
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.
MAC Bind IP	Strict - Make the MAC address and IP address settings configured in IP Object for Source IP and Destination IP are bound for applying such filter rule. No-Strict - no limitation.
Quality of Service	Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later. 
APP Enforcement	Select an APP Enforcement profile for global IM/P2P application blocking. If there is no profile for you to select, please choose [Create New] from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the APP Enforcement profile selected here. For detailed information, refer to the section of APP Enforcement profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.
URL Content Filter	Select one of the URL Content Filter profile settings (created in CSM>> URL Content Filter) for applying with this router. Please set at least one profile for choosing in CSM>> URL Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for URL Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.
Web Content Filter	Select one of the Web Content Filter profile settings (created in CSM>> Web Content Filter) for applying with this router. Please set at least one profile for anti-virus in CSM>> Web Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for Web Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.
DNS Filter	Select one of the DNS Filter profile settings (created in CSM>>DNS Filter) for applying with this router. Please set at least one profile in CSM>> Web Content Filter web page

first. Or click the DNS Filter link from the drop down list in this page to create a new profile.

Advance Setting

Click **Edit** to open the following window. However, it is **strongly recommended** to use the default settings here.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 1

Advance Setting

Codepage	ANSI(1252)-Latin I
Window size:	65535
Session timeout:	1440 Minute
DrayTek Banner:	<input checked="" type="checkbox"/>

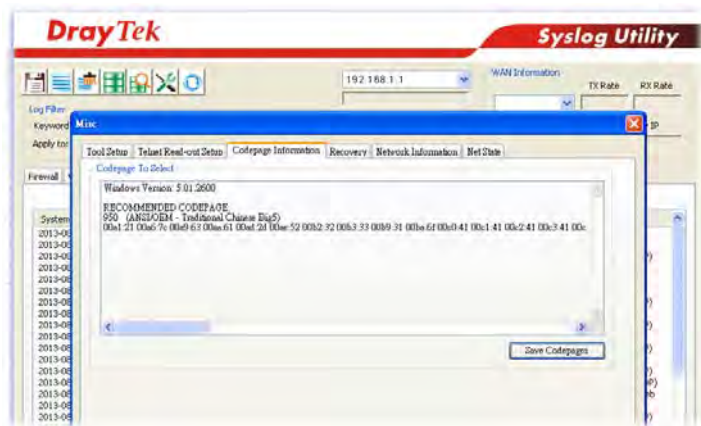
Strict Security Checking

APP Enforcement

OK Close

Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage.

If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.



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

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

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

The requested Web page has been blocked by Web Content Filter.

Please contact your system administrator for further information.

[Powered by Draytek]

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

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

V-1-3 DoS Defense

As a sub-functionality of IP Filter/Firewall, there are 15 types of detect/ defense function in the DoS Defense setup. The DoS Defense functionality is disabled for default.

Click **Firewall** and click **DoS Defense** to open the setup page.

Firewall >> DoS defense Setup

DoS defense Setup

Enable DoS Defense

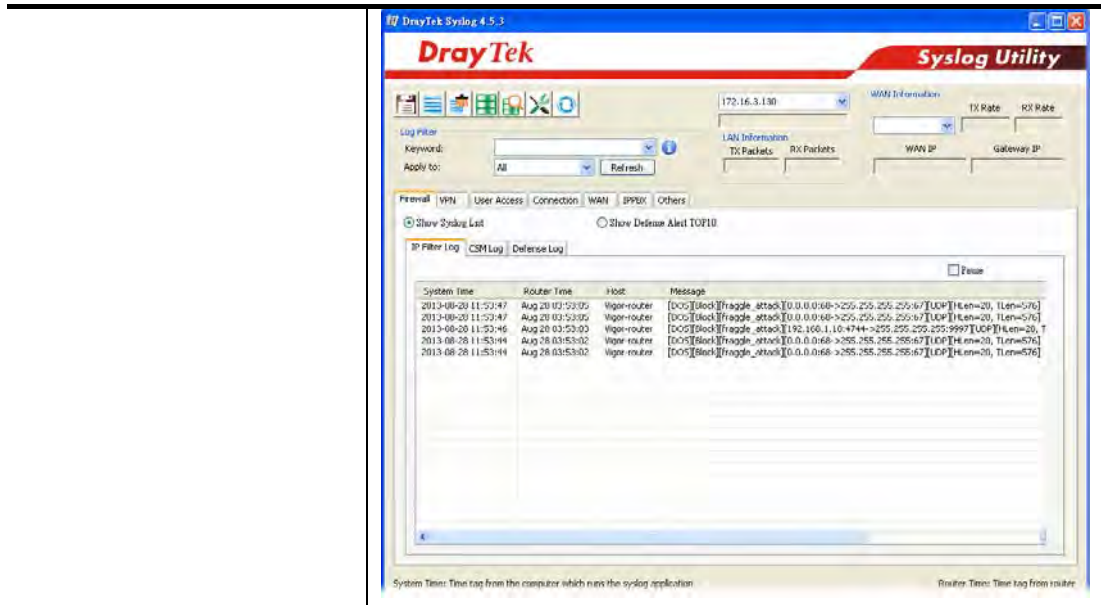
<input type="checkbox"/> Enable SYN flood defense	Threshold	<input type="text" value="2000"/>	packets / sec
	Timeout	<input type="text" value="10"/>	sec
<input type="checkbox"/> Enable UDP flood defense	Threshold	<input type="text" value="2000"/>	packets / sec
	Timeout	<input type="text" value="10"/>	sec
<input type="checkbox"/> Enable ICMP flood defense	Threshold	<input type="text" value="250"/>	packets / sec
	Timeout	<input type="text" value="10"/>	sec
<input type="checkbox"/> Enable Port Scan detection	Threshold	<input type="text" value="2000"/>	packets / sec
<input type="checkbox"/> Block IP options	<input type="checkbox"/> Block TCP flag scan		
<input type="checkbox"/> Block Land	<input type="checkbox"/> Block Tear Drop		
<input type="checkbox"/> Block Smurf	<input type="checkbox"/> Block Ping of Death		
<input type="checkbox"/> Block trace route	<input type="checkbox"/> Block ICMP fragment		
<input type="checkbox"/> Block SYN fragment	<input type="checkbox"/> Block Unassigned Numbers		
<input type="checkbox"/> Block Fraggle Attack			

Available settings are explained as follows:

Item	Description
Enable Dos Defense	Check the box to activate the DoS Defense Functionality.
Select All	Click this button to select all the items listed below.
Enable SYN flood defense	<p>Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent TCP SYN packets for a period defined in Timeout. The goal for this is prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor router.</p> <p>By default, the threshold and timeout values are set to 2000 packets per second and 10 seconds, respectively. That means, when 2000 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.</p>
Enable UDP flood defense	<p>Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent UDP packets for a period defined in Timeout.</p> <p>The default setting for threshold and timeout are 2000</p>

	<p>packets per second and 10 seconds, respectively. That means, when 2000 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.</p>
Enable ICMP flood defense	<p>Check the box to activate the ICMP flood defense function. Similar to the UDP flood defense function, once if the Threshold of ICMP packets from Internet has exceeded the defined value, the router will discard the ICMP echo requests coming from the Internet.</p> <p>The default setting for threshold and timeout are 250 packets per second and 10 seconds, respectively. That means, when 250 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.</p>
Enable Port Scan detection	<p>Port Scan attacks the Vigor router by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the port-scanning Threshold rate, the Vigor router will send out a warning.</p> <p>By default, the Vigor router sets the threshold as 2000 packets per second. That means, when 2000 packets per second received, they will be regarded as "attack event".</p>
Block IP options	<p>Check the box to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messages...etc. An eavesdropper outside might learn the details of your private networks.</p>
Block Land	<p>Check the box to enforce the Vigor router to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.</p>
Block Smurf	<p>Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.</p>
Block trace route	<p>Check the box to enforce the Vigor router not to forward any trace route packets.</p>
Block SYN fragment	<p>Check the box to activate the Block SYN fragment function. The Vigor router will drop any packets having SYN flag and more fragment bit set.</p>
Block Fraggle Attack	<p>Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked.</p> <p>Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.</p>

Block TCP flag scan	Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include <i>no flag scan</i> , <i>FIN without ACK scan</i> , <i>SYN FINscan</i> , <i>Xmas scan</i> and <i>full Xmas scan</i> .		
Block Tear Drop	Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.		
Block Ping of Death	Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.		
Block ICMP Fragment	Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.		
Block Unassigned Numbers	Check the box to activate the Block Unknown Protocol function. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and reject this kind of packets.		
Warning Messages	<p>We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client.</p> <p>All the warning messages related to DoS Defense will be sent to user and user can review it through Syslog daemon. Look for the keyword DoS in the message, followed by a name to indicate what kind of attacks is detected.</p> <p>System Maintenance >> SysLog / Mail Alert Setup</p> <hr/> <p>SysLog / Mail Alert Setup</p> <table border="1"> <tr> <td data-bbox="708 1384 1066 1720"> <p>SysLog Access Setup</p> <p><input checked="" type="checkbox"/> Enable</p> <p>Syslog Save to:</p> <p><input checked="" type="checkbox"/> Syslog Server</p> <p><input type="checkbox"/> USB Disk</p> <p>Router Name <input type="text" value="DrayTek"/></p> <p>Server IP/Hostname <input type="text"/></p> <p>Destination Port <input type="text" value="514"/></p> <p>Mail Syslog <input type="checkbox"/> Enable</p> <p>Enable syslog message:</p> <p><input checked="" type="checkbox"/> Firewall Log</p> <p><input checked="" type="checkbox"/> VPN Log</p> <p><input checked="" type="checkbox"/> User Access Log</p> <p><input checked="" type="checkbox"/> Call Log</p> <p><input checked="" type="checkbox"/> WAN Log</p> <p><input checked="" type="checkbox"/> Router/DSL information</p> <p><input checked="" type="checkbox"/> WLAN Log</p> </td> <td data-bbox="1070 1384 1394 1720"> <p>Mail Alert Setup</p> <p><input type="checkbox"/> Enable <input type="button" value="Send a test e-mail"/></p> <p>SMTP Server <input type="text"/></p> <p>SMTP Port <input type="text" value="25"/></p> <p>Mail To <input type="text"/></p> <p>Return-Path <input type="text"/></p> <p><input type="checkbox"/> Use SSL</p> <p><input type="checkbox"/> Authentication</p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>Enable E-Mail Alert:</p> <p><input checked="" type="checkbox"/> DoS Attack</p> <p><input checked="" type="checkbox"/> APPE</p> <p><input checked="" type="checkbox"/> VPN LOG</p> <p><input type="checkbox"/> APPE Signature</p> <p><input type="checkbox"/> Debug Log</p> </td> </tr> </table> <p>Note:</p> <ol style="list-style-type: none"> 1. Mail Syslog cannot be activated unless USB Disk is ticked for "Syslog Save to". 2. Mail Syslog feature sends a Syslog file when its size reaches 1M Bytes. 3. We only support secured SMTP connection on port 465. <p><input type="button" value="OK"/> <input type="button" value="Clear"/></p>	<p>SysLog Access Setup</p> <p><input checked="" type="checkbox"/> Enable</p> <p>Syslog Save to:</p> <p><input checked="" type="checkbox"/> Syslog Server</p> <p><input type="checkbox"/> USB Disk</p> <p>Router Name <input type="text" value="DrayTek"/></p> <p>Server IP/Hostname <input type="text"/></p> <p>Destination Port <input type="text" value="514"/></p> <p>Mail Syslog <input type="checkbox"/> Enable</p> <p>Enable syslog message:</p> <p><input checked="" type="checkbox"/> Firewall Log</p> <p><input checked="" type="checkbox"/> VPN Log</p> <p><input checked="" type="checkbox"/> User Access Log</p> <p><input checked="" type="checkbox"/> Call Log</p> <p><input checked="" type="checkbox"/> WAN Log</p> <p><input checked="" type="checkbox"/> Router/DSL information</p> <p><input checked="" type="checkbox"/> WLAN Log</p>	<p>Mail Alert Setup</p> <p><input type="checkbox"/> Enable <input type="button" value="Send a test e-mail"/></p> <p>SMTP Server <input type="text"/></p> <p>SMTP Port <input type="text" value="25"/></p> <p>Mail To <input type="text"/></p> <p>Return-Path <input type="text"/></p> <p><input type="checkbox"/> Use SSL</p> <p><input type="checkbox"/> Authentication</p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>Enable E-Mail Alert:</p> <p><input checked="" type="checkbox"/> DoS Attack</p> <p><input checked="" type="checkbox"/> APPE</p> <p><input checked="" type="checkbox"/> VPN LOG</p> <p><input type="checkbox"/> APPE Signature</p> <p><input type="checkbox"/> Debug Log</p>
<p>SysLog Access Setup</p> <p><input checked="" type="checkbox"/> Enable</p> <p>Syslog Save to:</p> <p><input checked="" type="checkbox"/> Syslog Server</p> <p><input type="checkbox"/> USB Disk</p> <p>Router Name <input type="text" value="DrayTek"/></p> <p>Server IP/Hostname <input type="text"/></p> <p>Destination Port <input type="text" value="514"/></p> <p>Mail Syslog <input type="checkbox"/> Enable</p> <p>Enable syslog message:</p> <p><input checked="" type="checkbox"/> Firewall Log</p> <p><input checked="" type="checkbox"/> VPN Log</p> <p><input checked="" type="checkbox"/> User Access Log</p> <p><input checked="" type="checkbox"/> Call Log</p> <p><input checked="" type="checkbox"/> WAN Log</p> <p><input checked="" type="checkbox"/> Router/DSL information</p> <p><input checked="" type="checkbox"/> WLAN Log</p>	<p>Mail Alert Setup</p> <p><input type="checkbox"/> Enable <input type="button" value="Send a test e-mail"/></p> <p>SMTP Server <input type="text"/></p> <p>SMTP Port <input type="text" value="25"/></p> <p>Mail To <input type="text"/></p> <p>Return-Path <input type="text"/></p> <p><input type="checkbox"/> Use SSL</p> <p><input type="checkbox"/> Authentication</p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>Enable E-Mail Alert:</p> <p><input checked="" type="checkbox"/> DoS Attack</p> <p><input checked="" type="checkbox"/> APPE</p> <p><input checked="" type="checkbox"/> VPN LOG</p> <p><input type="checkbox"/> APPE Signature</p> <p><input type="checkbox"/> Debug Log</p>		



V-1-4 Diagnose

The purpose of this function is to test when the router receiving incoming packet, which firewall rule will be applied to that packet. The test result, including firewall rule profile, IP address translation in packet transmission, state of the firewall functions and etc., also will be shown on this page.



Info

The result obtained by using Diagnose is offered for RD debug. It will be different according to actual state such as network connection, LAN/WAN settings and so on.

Firewall >> Diagnose

Mode

ICMP UDP TCP IPv4

Direction

From LAN

Test View



Packet & Payload

Packet	Enable	Direction	Protocol
1	<input checked="" type="checkbox"/>	A->B	UDP:Customize
2	<input checked="" type="checkbox"/>	B->A	UDP:Customize

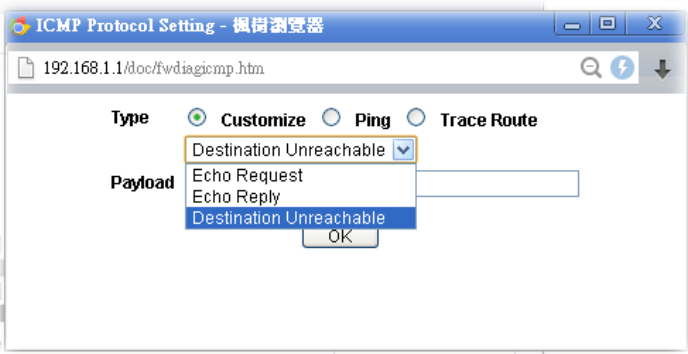
Note:

This is firewall live test which need setup WAN and plug cable in.

Analyze

Available settings are explained as follows:

Item	Description
Mode	To have a firewall rule test, specify the service type (ICMP, UDP, TCP) of the packet and type of the IP address (IPv4/IPv6).
Direction	Set the way (from WAN or from LAN) that Vigor router receives the first packet for test. Different way means the firewall will process the connection initiated from LAN or from WAN.
Test View	This is a dynamic display page. According to the direction specified, test view will display the figure to guide you typing IP address, port number, and MAC address. Later, after clicking the Analyze button, the information for the firewall rule profile and address translation will be shown on this page.
Src IP	Type the IPv4/IPv6 address of the packet's source.
Src Port	Type the port number of the packet's source.
Src MAC	Type the MAC address of the packet's source.

Dst IP	Type the IPv4/IPv6 address of the packet's destination.
Dst Port	Type the port number of the packet's destination.
Packet & Payload	<p>In firewall diagnose, two packets belong to one connection. In general, two packets are enough for Vigor router to perform this test.</p> <p>Enable - Check the box to send out the test packet.</p> <p>Direction - The first packet of the firewall test will follow the direction specified above. However, the direction for the second packet might be different. Simply choose the direction (from Computer A to B or from the B to A) for the second packet.</p> <p>Protocol - It displays the mode selected above and the sate. If required, click the mode link to configure advanced setting. The common service type (Customize, Ping, Trace Route / Customize, DNS, Trace Route / Customize, Http(GET) related to that mode (ICMP / UDP / TCP) will be shown on the following dialog box.</p>  <ul style="list-style-type: none"> ● Type - Choose Customize, Ping, Trace Route / Customize, DNS, Trace Route / Customize, Http (GET). ● Payload - It is available when Customzie is selected. Simply type 16 HEX characters which represent certain packet (e.g., DNS packet) if you want to set the data transfered with protocol (ICMP/UDP/TCP) which is different to Type setting.
Analyze	Execute the test and analyze the result.

The following figure shows the test result after clicking **Analyze**. Processing state for the functions (MAC Filter, QoS, User management, etc.) related to the firewall will be displayed by green or red LED.

Firewall >> Diagnose

Mode
 ICMP UDP TCP IPv4 ▾

Direction
 From LAN ▾

Test View

A

192.168.1.111:22222
->7.7.7.7:51348

LAN

Firewall

WAN1

<<REPLY

7.7.7.7:51348
172.16.2.234:62094<-

B

Status	Packet	Set	Rule	UCF/WCF
Pass	2	default	default	n/a

Packet & Payload

Packet	Enable	Direction	Protocol			
1	<input checked="" type="checkbox"/>	A->B ▾	UDP:Customize			
Acceleration						
2	<input checked="" type="checkbox"/>	B->A ▾	UDP:Customize			
Acceleration						
<input checked="" type="checkbox"/> SESS CTL	<input checked="" type="checkbox"/> MAC FILTER	<input checked="" type="checkbox"/> PCAP	<input checked="" type="checkbox"/> USER MGT	<input checked="" type="checkbox"/> APPE	<input checked="" type="checkbox"/> UCF	<input checked="" type="checkbox"/> WCF
<input checked="" type="checkbox"/> DNSF	<input checked="" type="checkbox"/> SESS LMT	<input checked="" type="checkbox"/> BW LMT	<input checked="" type="checkbox"/> QOS	<input checked="" type="checkbox"/> APP_QOS	<input checked="" type="checkbox"/> HW ACC	

APP: The APP need to check. ● : The APP is completed.
 APP: The APP doesn't need to check. ● : The APP is processing.

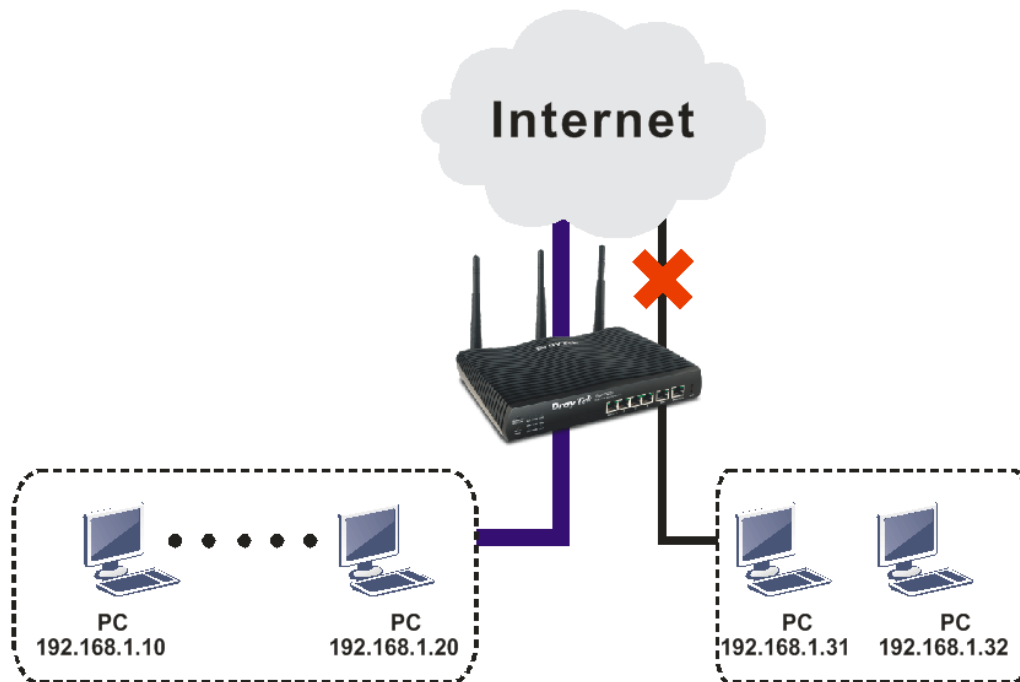
Note:
 PCAP is "ip pcap" in telnet command.

<<Back Reset

Application Notes

A-1 How to Configure Certain Computers Accessing to Internet

We can specify certain computers (e.g., 192.168.1.10 ~ 192.168.1.20) accessing to Internet through Vigor router. Others (e.g., 192.168.1.31 and 192.168.1.32) outside the range can get the source from LAN only.



The way we can use is to set two rules under Firewall. For Rule 1 of Set 2 under Firewall>>Filter Setup is used as the default setting, we have to create a new rule starting from Filter Rule 2 of Set 2.

1. Access into the web user interface of Vigor router.
2. Open Firewall>>Filter Setup. Click the Set 2 link, choose Advance Mode and choose the Filter Rule 2 button.

Firewall >> Filter Setup

Filter Setup		Set to Factory Default	
Set	Comments	Set	Comments
1.	Default Call Filter	7.	
2.	Default Data Filter	8.	
3.		9.	
4.		10.	
5.		11.	
6.		12.	



3. Check the box of Check to enable the Filter Rule. Type the comments (e.g., `block_all`). Choose **Block If No Further Match** for the Filter setting. Then, click **OK**.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 2

Check to enable the Filter Rule

Comments:

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

Clear sessions when schedule ON: Enable

Direction:

Source IP:

Destination IP:

Service Type:

Fragments:

Application

Filter:

Branch to Other Filter Set:

Sessions Control:

Syslog:



Info

In default, the router will check the packets starting with Set 2, Filter Rule 2 to Filter Rule 7. If Block If No Further Match for is selected for Filter, the firewall of the router would check the packets with the rules starting from Rule 3 to Rule 7. The packets not matching with the rules will be processed according to Rule 2.

4. Next, set another rule. Just open **Firewall>>Filter Setup**. Click the **Set 2** link and choose the **Filter Rule 3** button.
5. Check the box of **Check to enable the Filter Rule**. Type the comments (e.g., `open_ip`). Click the **Edit** button for **Source IP**.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 3

Check to enable the Filter Rule

Comments:

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

Clear sessions when schedule ON: Enable

Direction:

Source IP:

Destination IP:

Service Type:

Fragments:

Application

Filter:

Branch to Other Filter Set:

Syslog:

- A dialog box will be popped up. Choose **Range Address** as **Address Type** by using the drop down list. Type 192.168.1.10 in the field of **Start IP**, and type 192.168.1.20 in the field of **End IP**. Then, click **OK** to save the settings. The computers within the range can access into the Internet.

IP Address Edit

Address Type	Range Address
Start IP Address	192.168.1.10
End IP Address	192.168.1.20
Subnet Mask	0.0.0.0
Invert Selection	<input type="checkbox"/>
IP Group	None
or IP Object	None
or IP Object	None
or IP Object	None
IPv6 Group	None
or IPv6 Object	None
or IPv6 Object	None
or IPv6 Object	None

OK Close

- Now, check the content of **Source IP** is correct or not. The action for **Filter** shall be set with **Pass Immediately**. Then, click **OK** to save the settings.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 3

Check to enable the Filter Rule

Comments: open_ip

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

Clear sessions when schedule ON: Enable

Direction: LAN/RT/VPN -> WAN

Source IP: 192.168.1.10~192.168.1.20 Edit

Destination IP: Any Edit

Service Type: Any Edit

Fragments: Don't Care

Application

Filter: Action/Profile Pass Immediately Syslog

Branch to Other Filter Set: None

8. Both filter rules have been created. Click **OK**.

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 2

Comments :

Filter Rule	Active	Comments	Move Up	Move Down
<input type="button" value="1"/>	<input checked="" type="checkbox"/>	xNetBios -> DNS		<u>Down</u>
<input type="button" value="2"/>	<input checked="" type="checkbox"/>	block_all	<u>UP</u>	<u>Down</u>
<input type="button" value="3"/>	<input checked="" type="checkbox"/>	open_ip	<u>UP</u>	<u>Down</u>
<input type="button" value="4"/>	<input type="checkbox"/>		<u>UP</u>	<u>Down</u>
<input type="button" value="5"/>	<input type="checkbox"/>		<u>UP</u>	<u>Down</u>
<input type="button" value="6"/>	<input type="checkbox"/>		<u>UP</u>	<u>Down</u>
<input type="button" value="7"/>	<input type="checkbox"/>		<u>UP</u>	

Next Filter Set

Now, all the settings are configured well. Only the computers with the IP addresses within 192.168.1.10 ~ 192.168.1.20 can access to Internet.

V-2 Central Security Management (CSM)

CSM is an abbreviation of **Central Security Management** which is used to control IM/P2P usage, filter the web content and URL content to reach a goal of security management.

APP Enforcement Filter

As the popularity of all kinds of instant messenger application arises, communication cannot become much easier. Nevertheless, while some industry may leverage this as a great tool to connect with their customers, some industry may take reserved attitude in order to reduce employee misuse during office hour or prevent unknown security leak. It is similar situation for corporation towards peer-to-peer applications since file-sharing can be convenient but insecure at the same time. To address these needs, we provide CSM functionality.

URL Content Filter

To provide an appropriate cyberspace to users, Vigor router equips with **URL Content Filter** not only to limit illegal traffic from/to the inappropriate web sites but also prohibit other web feature where malicious code may conceal.

Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines to teenagers. At office, **URL Content Filter** can also provide a job-related only environment hence to increase the employee work efficiency. How can URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.

On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from websites, you may risk bringing threat to your system. For example, an ActiveX control object is usually used for providing interactive web feature. If malicious code hides inside, it may occupy user's system.

Web Content Filter

We all know that the content on the Internet just like other types of media may be inappropriate sometimes. As a responsible parent or employer, you should protect those in your trust against the hazards. With Web filtering service of the Vigor router, you can protect your business from common primary threats, such as productivity, legal liability, network and security threats. For parents, you can protect your children from viewing adult websites or chat rooms.

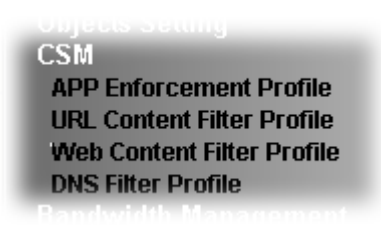
Once you have activated your Web Filtering service in Vigor router and chosen the categories of website you wish to restrict, each URL address requested (e.g. www.bbc.co.uk) will be checked against our server database. This database is updated as frequent as daily by a global team of Internet researchers. The server will look up the URL and return a category to your router. Your Vigor router will then decide whether to allow access to this site according to the categories you have selected. Please note that this action will not introduce any delay in your Web surfing because each of multiple load balanced database servers can handle millions of requests for categorization.



Info

The priority of URL Content Filter is higher than Web Content Filter.

Web User Interface



V-2-1 APP Enforcement Profile

You can define policy profiles for IM (Instant Messenger)/P2P (Peer to Peer)/Protocol/Misc application. This page allows you to set 32 profiles for different requirements. The APP Enforcement Profile will be applied in Default Rule of Firewall>>General Setup for filtering.

CSM >> APP Enforcement Profile

APP Enforcement Profile Table:

[Set to Factory Default](#)

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

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Profile	Display the number of the profile which allows you to click to set different policy.
Name	Display the name of the APP Enforcement Profile.

Click the number under Index column for settings in detail.

There are four tabs IM, P2P, Protocol and Others displayed on this page. Each tab will bring out different items with supported versions that you can choose to disallow people using.

Below shows the items which are categorized under IM.

CSM >> APP Enforcement Profile

Profile Index : 1 Profile Name:

IM	P2P	Protocol	OTHERS
<input type="button" value="Select All"/>	<input type="button" value="Clear All"/>		

IM			
Enable	APP Name	Version	Note
<input type="checkbox"/> <input type="button" value="Adv"/>	AIM	5.9	
<input type="checkbox"/>	AIM	8	Only block Login. If users have already logged in, AIM services can not be blocked.
<input type="checkbox"/>	AliWW	2008	
<input type="checkbox"/>	Ares	2.0.9	
<input type="checkbox"/>	BaiduHi	37378	
<input type="checkbox"/>	Facebook	97.0.0.18.69	To block Facebook for PC and mobile phone(97.0.0.18.69).
<input type="checkbox"/>	Fetion	2010	

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
Select All	Click it to choose all of the items in this page.
Clear All	Uncheck all the selected boxes.
Enable	Check the box to select the APP to be blocked by Vigor router.
Adv	A button under Enable check box allows you to open a pop up window to specify activity for that APP.

The profiles configured here can be applied in the Firewall>>General Setup and Firewall>>Filter Setup pages as the standard for the host(s) to follow.

Below shows the items which are categorized under Protocol.

CSM >> APP Enforcement Profile

Profile Index : 1 Profile Name:

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

The items categorized under P2P -----

CSM >> APP Enforcement Profile

Profile Index : 1 Profile Name:

IM	P2P	Protocol	OTHERS
Select All	Clear All		
BitTorrent			
Enable	APP Name	Version	Note
<input type="checkbox"/>	BitTorrent		The encrypted connection can not be 100% blocked. To block BitComet (1.30), BitSpirit (3.2.1), BitTorrent (4.4.1) and UltraTorrent (2.0).
FastTrack			
Enable	APP Name	Version	Note
<input type="checkbox"/>	FASTTRACK		To block BareShare (6.2.0.45), iMesh (9.1), KazaA (1.0.0.3) and Shareaza (4.1.0).
Gnutella			
Enable	APP Name	Version	Note
<input type="checkbox"/>	GNUTELLA		To block BareShare (5.1.0.26), Foxy (1.9.9), LimeWireWin (4.18.3) and Shareaza (2.3.0.0).
OpenFT			
Enable	APP Name	Version	Note
<input type="checkbox"/>	OpenFT		When blocking the connection, it will show "Connected" at first while the connection is not established successfully. After few seconds it will change back to "Connecting" status. KCeasy (0.19) also supports Ares

The items categorized under OTHERS-----

CSM >> APP Enforcement Profile

Profile Index : 1 Profile Name:

IM	P2P	Protocol	OTHERS
<input type="button" value="Select All"/>	<input type="button" value="Clear All"/>		

TUNNEL			
Enable	APP Name	Version	Note
<input type="checkbox"/>	DNSCrypt	0.0.6	Only blocks DNSCrypt login.
<input type="checkbox"/>	DynaPass	1.5	
<input type="checkbox"/>	FreeGate	7.58	
<input type="checkbox"/>	HTTP Proxy		
<input type="checkbox"/>	HTTP Tunnel	4.4.4000	
<input type="checkbox"/>	Hamachi	1.0.2.5	
<input type="checkbox"/>	Hotspot Shield	6.5.2	Block Hotspot Shield from establishing VPN connections. Please note that the APP Enforcement needs to be enabled prior than the VPN connections, or the blocking may not be successful.
<input type="checkbox"/>	MS Teredo		
<input type="checkbox"/>	PGPNet	7.0.3	
<input type="checkbox"/>	Ping Tunnel	0.61	
<input type="checkbox"/>	RealTunnel	1.0.1	
<input type="checkbox"/>	Skyfire	1.5	

V-2-2 URL Content Filter Profile

To provide an appropriate cyberspace to users, Vigor router equips with **URL Content Filter** not only to limit illegal traffic from/to the inappropriate web sites but also prohibit other web feature where malicious code may conceal.

Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines to teenagers. At office, **URL Content Filter** can also provide a job-related only environment hence to increase the employee work efficiency. How can URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.

On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from websites, you may risk bringing threat to your system. For example, an ActiveX control object is usually used for providing interactive web feature. If malicious code hides inside, it may occupy user's system.

For example, if you add key words such as "sex", Vigor router will limit web access to web sites or web pages such as "www.sex.com", "www.backdoor.net/images/sex/p_386.html". Or you may simply specify the full or partial URL such as "www.sex.com" or "sex.com".

Also the Vigor router will discard any request that tries to retrieve the malicious code.

Click CSM and click URL Content Filter Profile to open the profile setting page.

CSM >> URL Content Filter Profile



URL Content Filter Profile Table:

[Set to Factory Default](#)

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

Administration Message (Max 255 characters)

[Preview](#)

[Default Message](#)

```
<body><center><br><p>The requested Web page has been blocked by URL Content Filter.
<p>Please contact your system administrator for further information.</center></body>
```

OK

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Profile	Display the number of the profile which allows you to click to set different policy.
Name	Display the name of the URL Content Filter Profile.
Administration Message	You can type the message manually for your necessity. Default Message - You can type the message manually for your necessity or click this button to get the default message which will be displayed on the field of Administration Message .

You can set eight profiles as URL content filter. Simply click the index number under Profile to open the following web page.

CSM >> URL Content Filter Profile

Profile Index: 1

Profile Name:

Priority: **Log:**

1.URL Access Control

Enable URL Access Control Prevent web access from IP address

Action: Group/Object Selections:

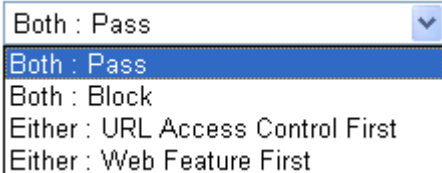
Exception List

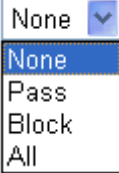
2.Web Feature

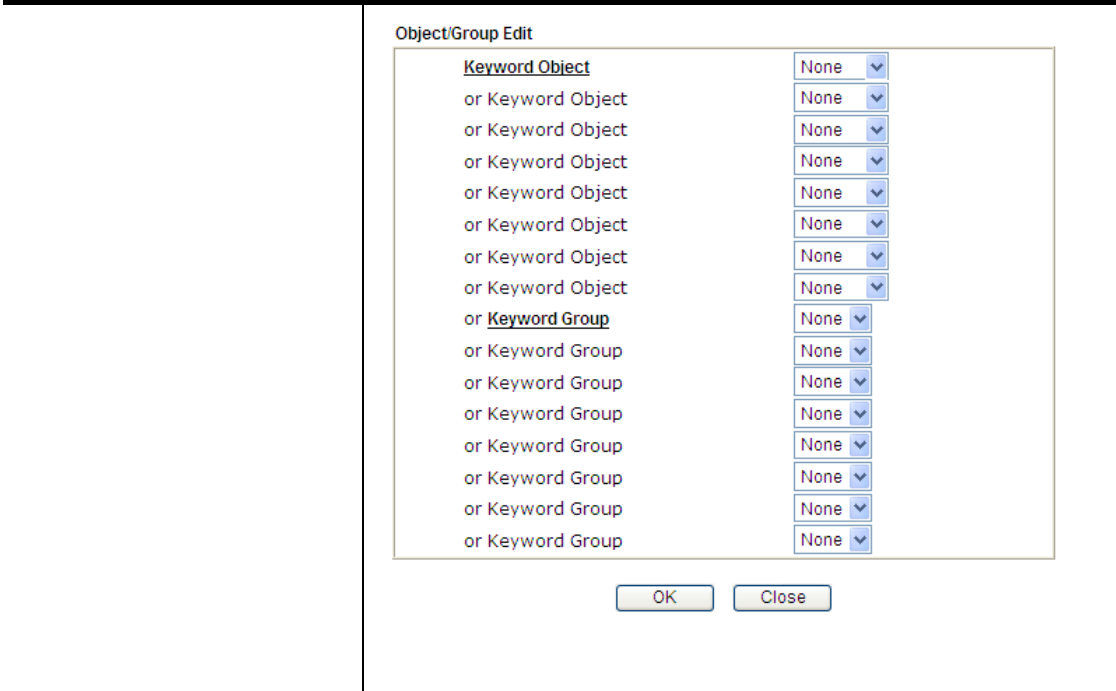
Enable Web Feature Restriction

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

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
Priority	<p>It determines the action that this router will apply.</p> <p>Both: Pass - The router will let all the packages that match with the conditions specified in URL Access Control and Web Feature below passing through. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.</p> <p>Both:Block -The router will block all the packages that match with the conditions specified in URL Access Control and Web Feature below. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.</p> <p>Either: URL Access Control First - When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for URL first, then Web feature second.</p> <p>Either: Web Feature First -When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for web feature first, then URL second.</p> 

Log	<p>None - There is no log file will be recorded for this profile. Pass - Only the log about Pass will be recorded in Syslog. Block - Only the log about Block will be recorded in Syslog. All - All the actions (Pass and Block) will be recorded in Syslog.</p> 
URL Access Control	<p>Enable URL Access Control - Check the box to activate URL Access Control. Note that the priority for URL Access Control is higher than Restrict Web Feature. If the web content match the setting set in URL Access Control, the router will execute the action specified in this field and ignore the action specified under Restrict Web Feature.</p> <p>Prevent web access from IP address - Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control. You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.</p> <p>Action - This setting is available only when Either : URL Access Control First or Either : Web Feature First is selected.</p> <ul style="list-style-type: none"> ● <i>Pass</i> - Allow accessing into the corresponding webpage with the keywords listed on the box below. ● <i>Block</i> - Restrict accessing into the corresponding webpage with the keywords listed on the box below. If the web pages do not match with the keyword set here, it will be processed with reverse action. <p>Exception List - Specify the object profile(s) as the exception list which will be processed in an opposite manner to the action selected above.</p> <p>Group/Object Selections - The Vigor router provides several frames for users to define keywords and each frame supports multiple keywords. The keyword could be a noun, a partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or semicolon. In addition, the maximal length of each frame is 32-character long. After specifying keywords, the Vigor router will decline the connection request to the website whose URL string matched to any user-defined keyword. It should be noticed that the more simplified the blocking keyword list is, the more efficiently the Vigor router performs.</p>



Web Feature

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

Action - This setting is available only when **Either: URL Access Control First** or **Either: Web Feature First** is selected.

Pass - Allow accessing into the corresponding webpage with the keywords listed on the box below.

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

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

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

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

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

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

V-2-3 Web Content Filter Profile

There are three ways to activate WCF on vigor router, using **Service Activation Wizard**, by means of **CSM>>Web Content Filter Profile** or via **System Maintenance>>Activation**.

Service Activation Wizard allows you to use trial version of WCF directly without accessing into the server (**MyVigor**) located on <http://myvigor.draytek.com>.

However, if you use the **Web Content Filter Profile** page to activate WCF feature, it is necessary for you to access into the server (**MyVigor**) located on <http://myvigor.draytek.com>. Therefore, you need to register an account on <http://myvigor.draytek.com> for using corresponding service. Please refer to section of creating MyVigor account.

WCF adopts the mechanism developed and offered by certain service provider (e.g., DrayTek). No matter activating WCF feature or getting a new license for web content filter, you have to click **Activate** to satisfy your request. Be aware that service provider matching with Vigor router currently offers a period of time for trial version for users to experiment. If you want to purchase a formal edition, simply contact with the channel partner or your dealer.

Click **CSM** and click **Web Content Filter Profile** to open the profile setting page. The default setting for Setup Query Server /Setup Test Server is **auto-selected**. You can choose another server for your necessity by clicking **Find more** to open <http://myvigor.draytek.com> for searching another qualified and suitable one.



Info 1

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

Info 2

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



Web-Filter License

[Activate](#)

[Status: **Not Activated**]

Setup Query Server	auto-selected	Find more
Setup Test Server	auto-selected	Find more

Web Content Filter Profile Table:

[Set to Factory Default](#)

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

Cache :

Administration Message (Max 255 characters)

[Preview](#)

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

Legend:

%SIP% - Source IP , %DIP% - Destination IP , %URL% - URL
 %CL% - Category , %RNAME% - Router Name

Available settings are explained as follows:

Item	Description
Activate	Click it to access into MyVigor for activating WCF service.
Setup Query Server	It is recommended for you to use the default setting, auto-selected. You need to specify a server for categorize searching when you type URL in browser based on the web content filter profile.
Setup Test Server	It is recommended for you to use the default setting, auto-selected.
Find more	Click it to open http://myvigor.draytek.com for searching another qualified and suitable server.
Test a site to verify whether it is categorized	Click this link to do the verification.
Set to Factory Default	Click this link to retrieve the factory settings.
Administration Message	You can type the message manually for your necessity or click Default Message button to get the default text displayed on the field of Administration Message . Preview - A dialog will appear to display the message typed in the Administration Message.
Cache	None - the router will check the URL that the user wants to access via WCF precisely, however, the processing rate is normal. Such item can provide the most accurate URL matching. L1 - the router will check the URL that the user wants to access via WCF. If the URL has been accessed previously, it

	<p>will be stored in the router to be accessed quickly if required. Such item can provide accurate URL matching with faster rate.</p> <p>L2 - the router will check the URL that the user wants to access via WCF. If the data has been accessed previously, the IP addresses of source and destination IDs will be memorized for a short time (about 1 second) in the router. When the user tries to access the same destination ID, the router will check it by comparing the record stored. If it matches, the page will be retrieved quickly. Such item can provide URL matching with the fastest rate.</p> <p>L1+L2 Cache - the router will check the URL with fast processing rate combining the feature of L1 and L2.</p>
--	--

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

CSM >> Web Content Filter Profile

Profile Index: 1

Profile Name:

Log:

Black/White List

Enable

Action:

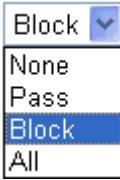
URL keywords:

Action:

<p>Groups</p> <p>Child Protection</p> <p><input type="button" value="Select All"/></p> <p><input type="button" value="Clear All"/></p> <p>Leisure</p> <p><input type="button" value="Select All"/></p> <p><input type="button" value="Clear All"/></p> <p>Business</p> <p><input type="button" value="Select All"/></p>	<p>Categories</p> <p><input checked="" type="checkbox"/> Alcohol & Tobacco</p> <p><input checked="" type="checkbox"/> Hate & Intolerance</p> <p><input checked="" type="checkbox"/> Porn & Sexually</p> <p><input checked="" type="checkbox"/> School Cheating</p> <p><input checked="" type="checkbox"/> Child Abuse Images</p> <p><input type="checkbox"/> Entertainment</p> <p><input type="checkbox"/> Travel</p>	<p><input checked="" type="checkbox"/> Criminal Activity</p> <p><input checked="" type="checkbox"/> Illegal Drug</p> <p><input checked="" type="checkbox"/> Violence</p> <p><input checked="" type="checkbox"/> Sex Education</p> <p><input type="checkbox"/> Games</p> <p><input type="checkbox"/> Leisure & Recreation</p>	<p><input checked="" type="checkbox"/> Gambling</p> <p><input checked="" type="checkbox"/> Nudity</p> <p><input checked="" type="checkbox"/> Weapons</p> <p><input checked="" type="checkbox"/> Tasteless</p> <p><input type="checkbox"/> Sports</p> <p><input type="checkbox"/> Fashion & Beauty</p>
--	--	--	---

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
Black/White List	<p>Enable - Activate white/black list function for such profile.</p> <p>URL keywords - Click Edit to choose the group or object profile as the content of white/black list.</p> <p>Pass - allow accessing into the corresponding webpage with the characters listed on Group/Object Selections. If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below.</p>

	<p>Block - restrict accessing into the corresponding webpage with the characters listed on Group/Object Selections. If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below.</p>
Action	<p>Pass - allow accessing into the corresponding webpage with the categories listed on the box below.</p> <p>Block - restrict accessing into the corresponding webpage with the categories listed on the box below.</p> <p>If the web pages do not match with the specified feature set here, it will be processed with reverse action.</p>
Log	<p>None - There is no log file will be recorded for this profile.</p> <p>Pass - Only the log about Pass will be recorded in Syslog.</p> <p>Block - Only the log about Block will be recorded in Syslog.</p> <p>All - All the actions (Pass and Block) will be recorded in Syslog.</p> 

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

V-2-4 DNS Filter Profile

The DNS Filter monitors DNS queries on UDP port 53 and will pass the DNS query information to the WCF to help with categorizing HTTPS URL's.

DNS can be specified in LAN>>General Setup by using the server (e.g., 168.95.1.1) on router or external DNS server (e.g., 8.8.8.8). If the router server is used, **DNS Filter General Setting** will be applied to DNS query from clients on LAN. However, if the external DNS server is used, **DNS Filter Profile** will be applied to DNS query coming from clients on LAN.



Info

For DNS filter must use the WCF service profile to filter the packets, therefore WCF license must be activated first. Otherwise, DNS filter does not have any effect on packets.

CSM >> DNS Filter

DNS Filter Profile Table

[Set to Factory Default](#)

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

DNS Filter Local Setting

DNS Filter	<input type="checkbox"/> Enable	
Syslog	None ▾	
WCF	None ▾	
UCE	None ▾	
Black/White List	<input type="checkbox"/> Enable	Blacklist ▾
	Address Type	Any Address ▾
	Start IP Address	0.0.0.0
	End IP Address	0.0.0.0
	Subnet Mask	0.0.0.0
	IP Group	None ▾
	or IP Group	None ▾
	or IP Object	None ▾
	or IP Object	None ▾

Administration Message (Max 255 characters)	Default Message
<pre><body><center>

<p>The requested Web page
 from %SIP%
to %URL%
that is categorized with %CL%
has been blocked by %RNAME% DNS Filter. <p>Please contact your system administrator for further information.</center></body></pre>	
Legend:	
%SIP% - Source IP , %URL% - URL	
%CL% - Category , %RNAME% - Router Name	

OK Cancel

Available settings are explained as follows:

Item	Description
DNS Filter Profile Table	It displays a list of different DNS filter profiles (with

	<p>specified WCF and UCF).</p> <p>Click the profile link to open the following page. Then, type the name of the profile and specify WCF/UCF based on your requirement.</p> <p>CSM >> DNS Filter</p> <hr/> <p>Index No. 1</p> <table border="1" data-bbox="703 405 1390 506"> <tr> <td>Profile Name</td> <td><input type="text"/></td> </tr> <tr> <td>Syslog</td> <td>None ▼</td> </tr> <tr> <td>WCF</td> <td>None ▼</td> </tr> <tr> <td>UCF</td> <td>None ▼</td> </tr> </table> <p style="text-align: center;"> <input type="button" value="OK"/> <input type="button" value="Clear"/> <input type="button" value="Cancel"/> </p>	Profile Name	<input type="text"/>	Syslog	None ▼	WCF	None ▼	UCF	None ▼
Profile Name	<input type="text"/>								
Syslog	None ▼								
WCF	None ▼								
UCF	None ▼								
<p>DNS Filter Local Setting</p>	<p>DNS Filter Local Setting will be applied to DNS query from clients on LAN when router's DNS server is used.</p> <p>DNS Filter - Check Enable to enable such feature.</p> <p>Syslog - The filtering result can be recorded according to the setting selected for Syslog.</p> <ul style="list-style-type: none"> ● None - There is no log file will be recorded for this profile. ● Pass - Only the log about Pass will be recorded in Syslog. ● Block - Only the log about Block will be recorded in Syslog. ● All - All the actions (Pass and Block) will be recorded in Syslog. <p>WCF- Set the filtering conditions.</p> <p>UCF - Set the filtering conditions.</p> <p>Black/White List - Specify IP address, subnet mask, IP object, or IP group as a black list or white list for DNS packets passing through or blocked by Vigor router.</p>								
<p>Administration Message</p>	<p>Specify IP address, subnet mask, IP object, or IP group as a black list or white list for DNS packets passing through or blocked by Vigor router.</p> <p>Type the words or sentences which will be displayed when a web page is blocked by Vigor router. You can type the message manually for your necessity or click Default Message button to get the default text displayed on the field of Administration Message.</p>								

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

Application Notes

A-1 How to Create an Account for MyVigor

The website of MyVigor (a server located on <http://myvigor.draytek.com>) provides several useful services (such as Anti-Spam, Web Content Filter, Anti-Intrusion, and etc.) to filtering the web pages for the sake of protecting your system.

To access into MyVigor for getting more information, please create an account for MyVigor.

Create an Account via Vigor Router

1. Click CSM>> Web Content Filter Profile. The following page will appear.

CSM >> Web Content Filter Profile ?

Web-Filter License **Activate**
[Status:Not Activated]

Setup Query Server	auto-selected	Find more
Setup Test Server	auto-selected	Find more

Web Content Filter Profile Table: [Set to Factory Default](#)

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

Administration Message (Max 255) [Preview!](#) [Cache :](#)

Or

Click System Maintenance>>Activation to open the following page.

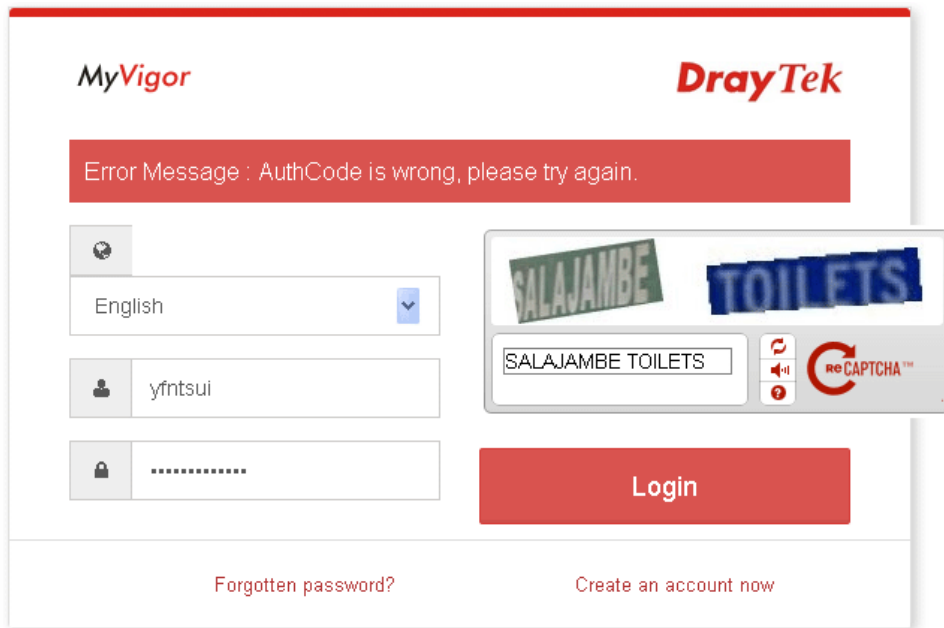
System Maintenance >> Activation Activate via interface : auto-selected ▼

Web-Filter License **Activate**
[Status:Not Activated]

Authentication Message

Note: If you want to use email alert or syslog, please configure the [SysLog/Mail Alert Setup](#) page.

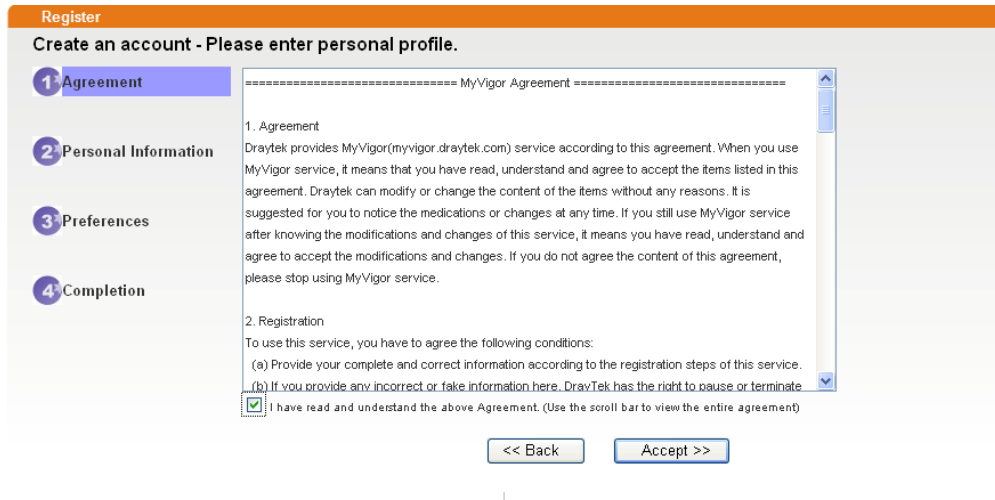
2. Click the **Activate** link. A login page for MyVigor web site will pop up automatically.



The screenshot shows the MyVigor login page. At the top left is the 'MyVigor' logo and at the top right is the 'DrayTek' logo. A red banner displays the error message: 'Error Message : AuthCode is wrong, please try again.' Below this, there is a language selection dropdown set to 'English', a username field containing 'yfntsui', and a password field with masked characters. To the right of the login fields is a reCAPTCHA widget with the text 'SALAJAMBE TOILETS'. A large red 'Login' button is positioned to the right of the password field. At the bottom of the form, there are two links: 'Forgotten password?' and 'Create an account now'.

Customer Service : (886) 3 597 2727 or email to : support@draytek.com

3. Click the link of **Create an account now**.
4. Check to confirm that you accept the Agreement and click **Accept**.



The screenshot shows the 'Register' page with the heading 'Create an account - Please enter personal profile.' A sidebar on the left lists four steps: 1 Agreement (highlighted), 2 Personal Information, 3 Preferences, and 4 Completion. The main content area displays the 'MyVigor Agreement' text, which includes sections for '1. Agreement' and '2. Registration'. The '2. Registration' section lists conditions (a) and (b). Below the agreement text is a checkbox labeled 'I have read and understand the above Agreement. (Use the scroll bar to view the entire agreement)' which is checked. At the bottom of the page are two buttons: '<< Back' and 'Accept >>'.

5. Type your personal information in this page and then click **Continue**.

Register

Create an account - Please enter personal profile. (Fields marked by (*) are required)

1 Agreement

2 Personal Information

3 Preferences

4 Completion

Account Information

UserName:*
(3 - 20 characters)

Password:*
(4 - 20 characters : Do not set the same as the username.)

Confirm Password:*

Personal Information

First Name:*

Last Name:*

Company Name:

Email Address:*
Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.

Tel: -

Country:*

Career:*

6. Choose proper selection for your computer and click **Continue**.

Register

Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 Completion

How did you find out about this website?

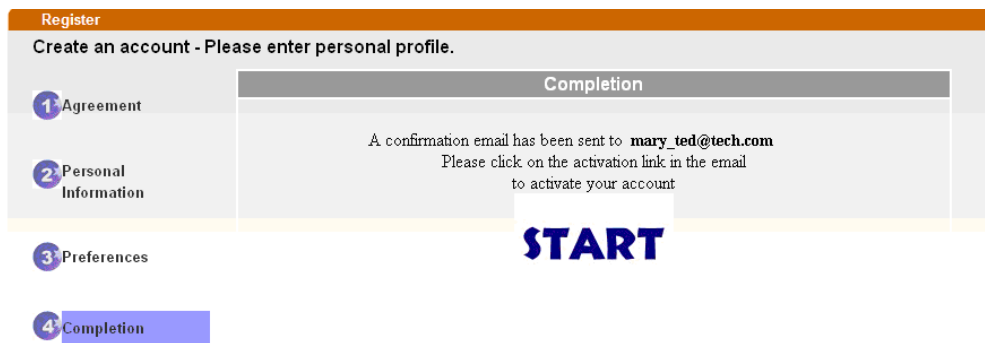
What kind of anti-virus do you use?

I would like to subscribe to the MyVigor e-letter.

I would like to receive DrayTek product news.

Please select the mail server for receiving the verification mail.

- Now you have created an account successfully. Click START.



- Check to see the confirmation *email* with the title of New Account Confirmation Letter from myvigor.draytek.com.

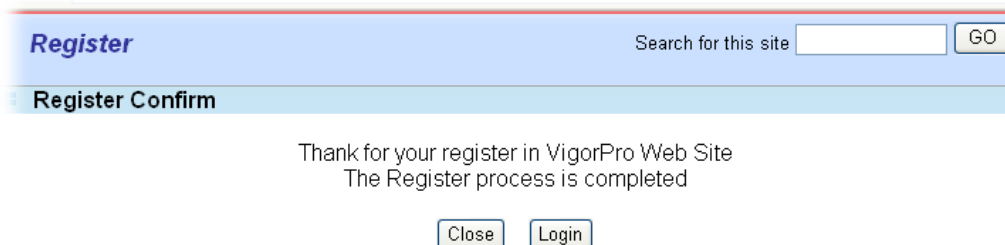
***** This is an automated message from myvigor.draytek.com.*****

Thank you (**Mary**) for creating an account.

Please click on the activation link below to activate your account

Link : [Activate my Account](#)

- Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.



- When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**.

The screenshot shows the MyVigor login interface. At the top left is the MyVigor logo and at the top right is the DrayTek logo. A red error message box states: "Error Message : AuthCode is wrong, please try again." Below this, there is a language dropdown menu set to "English". The username field contains "yfntsui" and the password field is masked with dots. To the right of the login fields is a CAPTCHA image showing the text "SALAJAMBE TOILETS" and a ReCAPTCHA logo. A large red "Login" button is positioned below the CAPTCHA. At the bottom of the form, there are two links: "Forgotten password?" and "Create an account now".

Customer Service : (886) 3 597 2727 or email to : support@draytek.com

- Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

Create an Account via MyVigor Web Site

- Access into <http://myvigor.draytek.com>. Find the line of **Not registered yet?**. Then, click the link **Click here!** to access into next page.

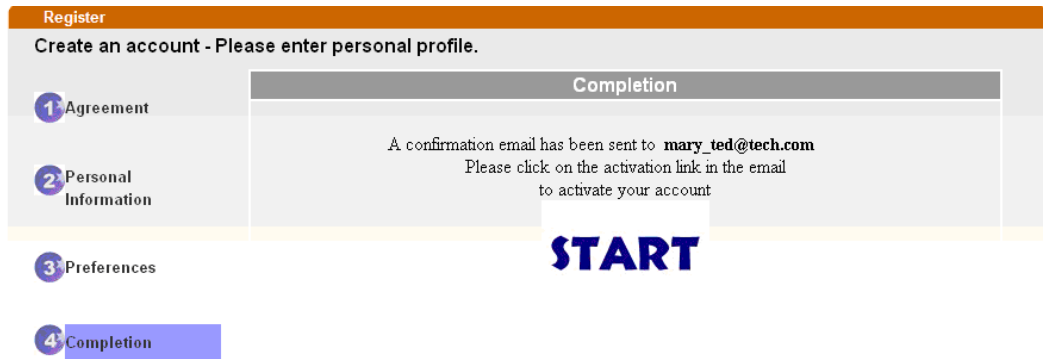
The screenshot shows the MyVigor website home page. The header includes the DrayTek logo on the left and the MyVigor logo on the right. Below the header is a navigation menu with links for Home, About Us, Product, My Information, and VigorPro. The main content area is titled "MyVigor for you" and contains information about the website's purpose and supported services. On the right side, there is a "Customer Survey" button and a "Login" form. The login form includes fields for Username, Password, and AuthCode, along with a CAPTCHA image showing "QbkqVd". Below the CAPTCHA is a "Login" button and a "Forget password?" link. At the bottom of the login form, there is a link for "Not registered yet ? Click here!".

2. Check to confirm that you accept the Agreement and click **Accept**.

3. Type your personal information in this page and then click **Continue**.

4. Choose proper selection for your computer and click **Continue**.

5. Now you have created an account successfully. Click **START**.



6. Check to see the confirmation *email* with the title of New Account Confirmation Letter from myvigor.draytek.com.

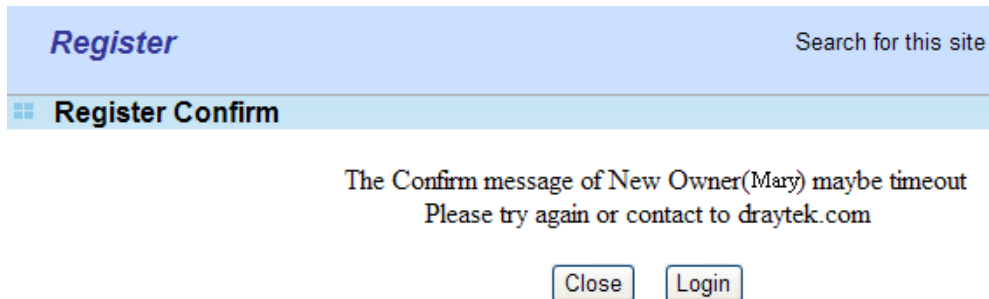
***** This is an automated message from myvigor.draytek.com.*****

Thank you (**Mary**) for creating an account.

Please click on the activation link below to activate your account

Link : [Activate my Account](#)

7. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.



8. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**. Then type the code in the box of Auth Code according to the value displayed on the right side of it.

The screenshot shows the MyVigor login interface. At the top left is the 'MyVigor' logo and at the top right is the 'DrayTek' logo. A red error message banner reads: 'Error Message : AuthCode is wrong, please try again.' Below this, there are three input fields: a language dropdown menu set to 'English', a username field containing 'yfntsui', and a password field with masked characters. To the right of these fields is a CAPTCHA challenge box displaying the text 'SALAJAMBE TOILETS' in a distorted font. Below the CAPTCHA is a 'reCAPTCHA' logo and a 'Login' button. At the bottom of the form, there are two links: 'Forgotten password?' and 'Create an account now'.

Customer Service : (886) 3 597 2727 or email to : support@draytek.com

Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

A-2 How to Block Facebook Service Accessed by the Users via Web Content Filter / URL Content Filter

There are two ways to block the facebook service, Web Content Filter and URL Content Filter.

Web Content Filter,

Benefits: Easily and quickly implement the category/website that you want to block.

Note: License is required.

URL Content Filter,

Benefits: Free, flexible for customize webpage.

Note: Manual setting (e.g., one keyword for one website.)

I. Via Web Content Filter

1. Make sure the Web Content Filter (powered by Commtouch) license is valid.

CSM >> Web Content Filter Profile

Web-Filter License

[Activate](#)

[Status: **Commtouch**] [Start Date: **2012-12-31** Expire Date: **2013-01-08**]

Setup Query Server	auto-selected	Find more
Setup Test Server	auto-selected	Find more

Web Content Filter Profile Table:

[Set to Factory Default](#)

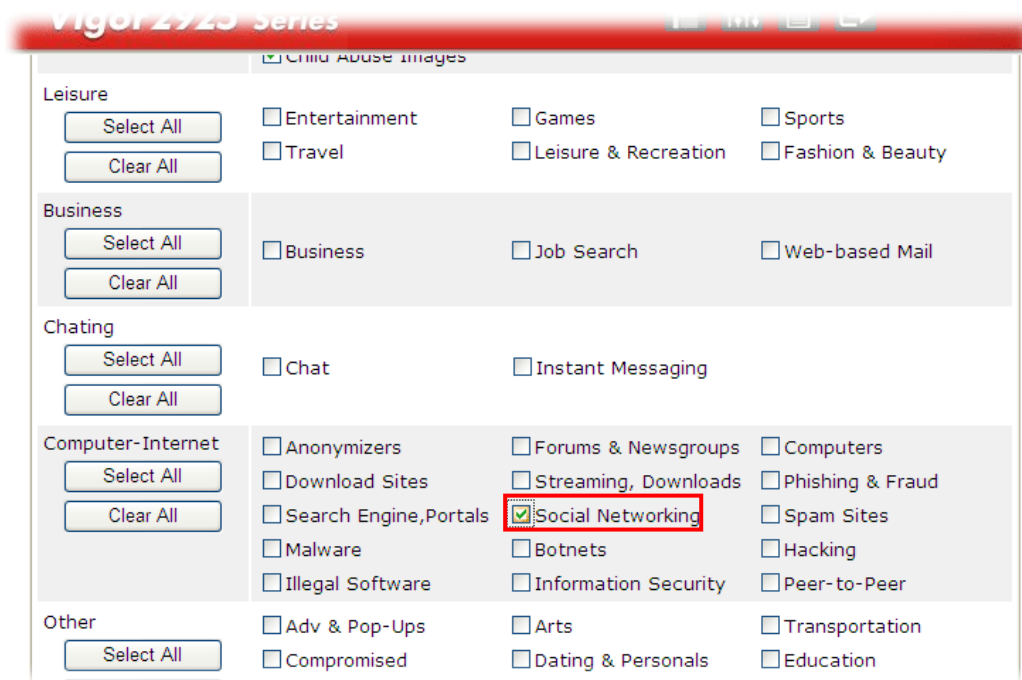
Profile	Name	Profile	Name
1.	Default	5.	
2.		6.	
3.		7.	
4.		8.	

Administration Message (Max 255 characters)

Cache : [L1 + L2 Cache](#)

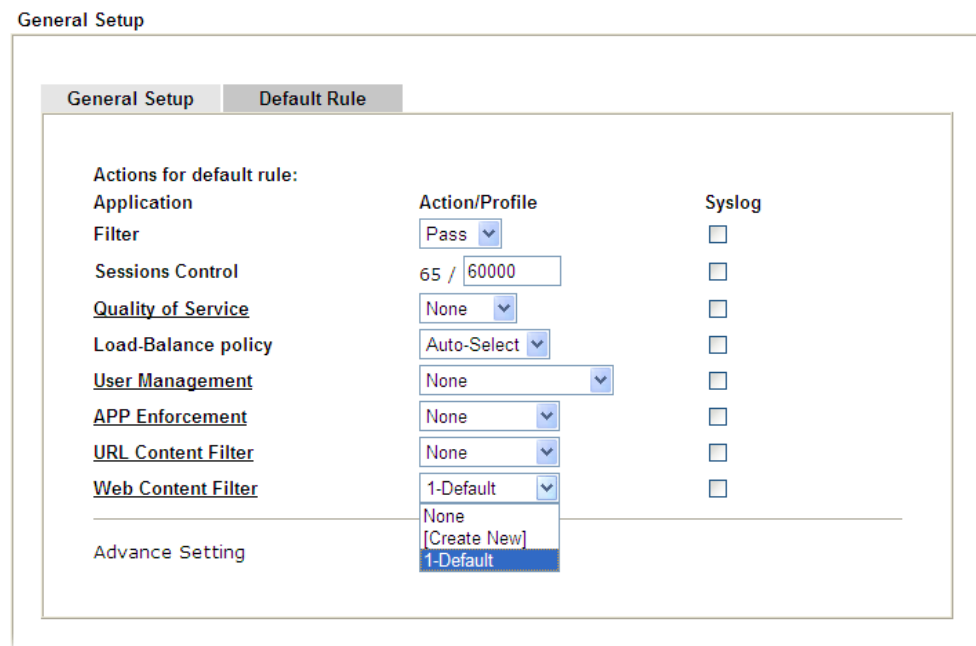
```
<body><center><br><br><br><p>The requested Web page <br> from %SIP% <br>to %URL%
<br>that is categorized with %CL% <br>has been blocked by %RNAME% Web Content
Filter.<p>Please contact your system administrator for further
information.</center></body>
```

- 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”

- Open Object Settings>>Keyword Object. Click an index number to open the setting page.
- In the field of Contents, please type *facebook*. Configure the settings as the following figure.

Objects Setting >> Keyword Object Setup

Profile Index : 1

Name	<input type="text" value="Facebook"/>
Contents	<input type="text" value="facebook"/>

Limit of Contents: Max 3 Words and 63 Characters.
 Each word should be separated by a single space.

You can replace a character with %HEX.
 Example:
 Contents: backdoo%72 virus keep%20out

Result:

- backdoor
- virus
- keep out

- Open CSM>>URL Content Filter Profile. Click an index number to open the setting page.
- Configure the settings as the following figure.

Profile Index: 1

Profile Name:

Priority: Log:

1.URL Access Control

Enable URL Access Control Prevent web access from IP address

Action: Group/Object Selections:

2.Web Feature

Enable Restrict Web Feature

Action: Cookie Proxy Upload File Extension Profile:

5. When you finished the above steps, click OK. Then, open Firewall>>General Setup.
6. Click the Default Rule tab. Choose the profile just configured from the drop down list in the field of URL Content Filter. Now, users cannot open any web page with the word "facebook" inside.

General Setup

General Setup **Default Rule**

Actions for default rule:

Application	Action/Profile	Syslog
Filter	<input type="text" value="Pass"/>	<input type="checkbox"/>
Sessions Control	<input type="text" value="0 / 60000"/>	<input type="checkbox"/>
Quality of Service	<input type="text" value="None"/>	<input type="checkbox"/>
Load-Balance policy	<input type="text" value="Auto-Select"/>	<input type="checkbox"/>
User Management	<input type="text" value="None"/>	<input type="checkbox"/>
APP Enforcement	<input type="text" value="None"/>	<input type="checkbox"/>
URL Content Filter	<input type="text" value="1-Facebook"/>	<input type="checkbox"/>
Web Content Filter	<input type="text" value="None"/>	<input type="checkbox"/>

Advance Setting

B. Disallow users to play games on Facebook

1. Open Object Settings>>Keyword Object. Click an index number to open the setting page.
2. In the field of Contents, please type *apps.facebook*. Configure the settings as the following figure.

Objects Setting >> Keyword Object Setup

Profile Index : 2

Name	facebook-apps
Contents	apps facebook

Limit of Contents: Max 3 Words and 63 Characters.
Each word should be separated by a single space.

You can replace a character with %HEX.
Example:
Contents: backdoo%72 virus keep%20out

Result:
1. backdoor
2. virus
3. keep out

OK Clear Cancel

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: 2

Profile Name:	face.apps		
Priority:	Either : URL Access Control First	Log:	None
1.URL Access Control			
<input checked="" type="checkbox"/> Enable URL Access Control		<input type="checkbox"/> Prevent web access from IP address	
Action:		Group/Object Selections	
Block		facebook..	
2.Web Feature			
<input type="checkbox"/> Enable Restrict Web Feature			
Action:			
Pass		<input type="checkbox"/> Cookie	<input type="checkbox"/> Proxy
		<input type="checkbox"/> Upload	File Extension Profile: None

OK Clear Cancel

5. When you finished the above steps, please open Firewall>>General Setup.
6. Click the **Default Rule** tab. Choose the profile just configured from the drop down list in the field of URL Content Filter. Now, users cannot open any web page with the word "facebook" inside.

General Setup

General Setup	Default Rule	
Actions for default rule:		
Application	Action/Profile	Syslog
Filter	Pass	<input type="checkbox"/>
Sessions Control	0 / 60000	<input type="checkbox"/>
Quality of Service	None	<input type="checkbox"/>
Load-Balance policy	Auto-Select	<input type="checkbox"/>
User Management	None	<input type="checkbox"/>
APP Enforcement	None	<input type="checkbox"/>
URL Content Filter	2-face.apps	<input type="checkbox"/>
Web Content Filter	None	<input type="checkbox"/>
Advance Setting	<input type="button" value="Edit"/>	

This page is left blank.

Part VI 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).



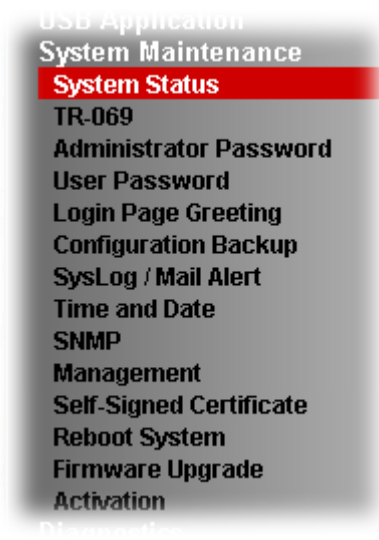
User
Management

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.

VI-1 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: System Status, TR-069, Administrator Password, User Password, Login Page Greeting, Configuration Backup, Syslog /Mail Alert, Time and Date, Management, Reboot System, Firmware Upgrade and Activation.

Below shows the menu items for System Maintenance.



Web User Interface

VI-1-1 System Status

The System Status provides basic network settings of Vigor router. It includes LAN and WAN interface information. Also, you could get the current running firmware version or firmware related information from this presentation.

System Status

Model Name : Vigor2133Vac
Firmware Version : 3.8.8
Build Date/Time : Feb 27 2018 17:29:02

LAN					
	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-1D-AA-66-DF-F0	192.168.1.1	255.255.255.0	ON	8.8.8.8
LAN2	00-1D-AA-66-DF-F0	192.168.2.1	255.255.255.0	ON	8.8.8.8
LAN3	00-1D-AA-66-DF-F0	192.168.3.1	255.255.255.0	ON	8.8.8.8
LAN4	00-1D-AA-66-DF-F0	192.168.4.1	255.255.255.0	ON	8.8.8.8
IP Routed Subnet	00-1D-AA-66-DF-F0	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-66-DF-F0	Europe	4.0.1.0rev2.P1	DrayTek

Wireless LAN(5GHz)			
MAC Address	Frequency Domain	Firmware Version	SSID
00-1D-AA-66-DF-F2	Europe	10.2-00082-4	DrayTek_5G

WAN				
Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1 Disconnected	00-1D-AA-66-DF-F1	DHCP Client	---	---
WAN3 Disconnected	00-1D-AA-66-DF-F3	---	---	---

IPv6		
Address	Scope	Internet Access Mode
LAN FE80::21D:AFF:FE66:DFF0/64	Link	---

VoIP			
Port	Profile	Reg.	In/Out
Phone1		No	0/0
Phone2		No	0/0

User Mode is OFF now.

Available settings are explained as follows:

Item	Description
Model Name	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
Build Date/Time	Display the date and time of the current firmware build.
LAN	MAC Address - Display the MAC address of the LAN Interface. IP Address - Display the IP address of the LAN interface. Subnet Mask - Display the subnet mask address of the LAN interface. DHCP Server - Display the current status of DHCP server of the LAN

	<p>interface.</p> <p>DNS</p> <ul style="list-style-type: none"> - Display the assigned IP address of the primary DNS.
WAN	<p>Link Status</p> <ul style="list-style-type: none"> - Display current connection status. <p>MAC Address</p> <ul style="list-style-type: none"> - Display the MAC address of the WAN Interface. <p>Connection</p> <ul style="list-style-type: none"> - Display the connection type. <p>IP Address</p> <ul style="list-style-type: none"> - Display the IP address of the WAN interface. <p>Default Gateway</p> <ul style="list-style-type: none"> - Display the assigned IP address of the default gateway.
IPv6	<p>Address - Display the IPv6 address for LAN.</p> <p>Scope - Display the scope of IPv6 address. For example, IPv6 Link Local could only be used for direct IPv6 link. It can't be used for IPv6 internet.</p> <p>Internet Access Mode - Display the connection mode chosen for accessing into Internet.</p>

VI-1-2 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through an Auto Configuration Server, e.g., VigorACS.

System Maintenance >> TR-069 Setting

ACS and CPE Settings	Export Parameters									
Tr069 <input checked="" type="radio"/> Disable <input type="radio"/> Enable ACS Server On <input type="text" value="Internet"/>										
ACS Server URL <input type="text"/> <input type="button" value="Wizard"/> <input type="checkbox"/> Acquire URL from DHCP option 43 Username <input type="text"/> Password <input type="text"/> <input type="button" value="Test With Inform"/> Event Code <input type="text" value="PERIODIC"/>										
Last Inform Response Time :(NA) ●										
CPE Client <input checked="" type="radio"/> Http <input type="radio"/> Https URL <input type="text"/> Port <input type="text" value="8069"/> Username <input type="text" value="vigor"/> Password <input type="text" value="*****"/>										
Periodic Inform Settings <input checked="" type="radio"/> Disable <input type="radio"/> Enable Interval Time <input type="text" value="900"/> second(s)										
STUN Settings <input checked="" type="radio"/> Disable <input type="radio"/> Enable Server Address <input type="text"/> Server Port <input type="text" value="3478"/> Minimum Keep Alive Period <input type="text" value="60"/> second(s) Maximum Keep Alive Period <input type="text" value="-1"/> second(s)										
Apply Settings to APs <input checked="" type="radio"/> Disable <input type="radio"/> Enable AP Password <input type="text"/> <input type="checkbox"/> Apply Specific STUN Settings to APs										
Bandwidth Utilisation Notification Settings <input checked="" type="radio"/> Disable <input type="radio"/> Enable Time Period <input type="text" value="15 mins"/>										
<p>Note: Please turn off Hardware Acceleration in the router to receive Alerts Notifications, and accuracy of Bandwidth data.</p> <table border="1"> <thead> <tr> <th>WAN</th> <th>Threshold Level</th> <th>Line Speed</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> WAN1</td> <td>Medium <input type="text" value="0"/> % High <input type="text" value="0"/> %</td> <td>of TX: <input type="text" value="0"/> Mbps RX: <input type="text" value="0"/> Mbps</td> </tr> <tr> <td><input type="checkbox"/> WAN3</td> <td>Medium <input type="text" value="0"/> % High <input type="text" value="0"/> %</td> <td>of TX: <input type="text" value="0"/> Mbps RX: <input type="text" value="0"/> Mbps</td> </tr> </tbody> </table>		WAN	Threshold Level	Line Speed	<input type="checkbox"/> WAN1	Medium <input type="text" value="0"/> % High <input type="text" value="0"/> %	of TX: <input type="text" value="0"/> Mbps RX: <input type="text" value="0"/> Mbps	<input type="checkbox"/> WAN3	Medium <input type="text" value="0"/> % High <input type="text" value="0"/> %	of TX: <input type="text" value="0"/> Mbps RX: <input type="text" value="0"/> Mbps
WAN	Threshold Level	Line Speed								
<input type="checkbox"/> WAN1	Medium <input type="text" value="0"/> % High <input type="text" value="0"/> %	of TX: <input type="text" value="0"/> Mbps RX: <input type="text" value="0"/> Mbps								
<input type="checkbox"/> WAN3	Medium <input type="text" value="0"/> % High <input type="text" value="0"/> %	of TX: <input type="text" value="0"/> Mbps RX: <input type="text" value="0"/> Mbps								
<p>Note: If "Apply Specific STUN Settings to APs" is enabled, router STUN Settings would be discarded.</p>										
<input type="button" value="OK"/> <input type="button" value="Clear"/>										

Available settings are explained as follows:

Item	Description
Tr069	Click Enable to activate the settings on this page.
ACS Server On	Choose the interface for the router connecting to ACS server.
ACS Server	URL/Username/Password - Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information.

	<p>Wizard - Click it to enter the IP address of VigorACS server, port number and the handler.</p> <p>Test With Inform - Click it to send a message based on the event code selection to test if such CPE is able to communicate with VigorACS SI server.</p> <p>Event Code - Use the drop down menu to specify an event to perform the test.</p> <p>Last Inform Response Time - Display the time that VigorACS server made a response while receiving Inform message from CPE last time.</p>
CPE Client	<p>Such information is useful for Auto Configuration Server.</p> <p>Enable/Disable - Allow/Deny the CPE Client to connect with Auto Configuration Server.</p> <p>Port - Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE.</p> <p>Username and Password - Type the username and password that VigorACS can use to access into such CPE.</p>
Periodic Inform Settings	<p>The default setting is Enable. Please set interval time or schedule time for the router to send notification to CPE. Or click Disable to close the mechanism of notification.</p>
STUN Settings	<p>The default is Disable. If you click Enable, please type the relational settings listed below:</p> <p>Server Address - Type the IP address of the STUN server.</p> <p>Server Port - Type the port number of the STUN server.</p> <p>Minimum Keep Alive Period - If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds".</p> <p>Maximum Keep Alive Period - If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.</p>
Apply Settings to APs	<p>This feature is able to apply TR-069 settings (including STUN and ACS server settings) to all of APs managed by Vigor2133 at the same time.</p> <p>Disable - Related settings will not be applied to VigorAP.</p> <p>Enable - Above STUN settings will be applied to VigorAP after clicking OK. If such feature is enabled, you have to type the password for accessing VigorAP.</p> <ul style="list-style-type: none"> ● AP Password - Type the password of the VigorAP that you want to apply Vigor2133's TR-069 settings. <p>Apply Specific STUN Settings to APs - After clicking the Enable radio button for Apply Settings to APs, if you want to apply specific STUN settings (not the STUN Settings configured for Vigor2133) to VigorAPs to meet specific requirements, simply check this box. Then, type the server IP address, server port, minimum keep alive period and maximum keep alive period respectively.</p>
Bandwidth Utilisation Notification Settings	<p>To administrator, this feature is useful to monitor the bandwidth utilization of CPE(s). When the bandwidth used is over the threshold level (percentage defined in medium and high fields), a notification will be sent to VigorACS. After a</p>

long time observation, the administrator can determine if it is necessary to increase the bandwidth setting for that CPE or not.

Enable - Click it to enable such feature.

Time Period - Choose the time interval (15 mins, 30 mins, 1hour, 3 hours, or 6 hours) for CPE to send a notification of bandwidth utilization to VigorACS.

WAN - Choose the WAN interface for applying the bandwidth utilization notification mechanism.

Threshold Level - Set the percentage of bandwidth in transmission and receiving data as threshold values for CPE to detect bandwidth utilization.

Line Speed - Set the transmission rate and receiving rate for specified WAN interface.

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

VI-1-3 Administrator Password

This page allows you to set new password.

System Maintenance >> Administrator Password Setup

Administrator Password

Old Password:

New Password: (Max. 83 characters allowed)

Confirm Password: (Max. 83 characters allowed)

Password Strength: Weak Medium Strong

Strong password requirements:

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

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

Administrator Local User

Local User

Local User List

Index	User Name

Specific User

User Name:

Password: Confirm Password:

Enable 'Admin' Login From Wan

Available settings are explained as follows:

Item	Description
Administrator Password	<p>Old Password - Type in the old password. The factory default setting for password is "admin".</p> <p>New Password - Type in new password in this field. The length of the password is limited to 23 characters.</p> <p>Confirm Password - Type in the new password again.</p> <p>Password Strength - Display the security strength of the password specified above.</p>
Administrator Local User	<p>The administrator can login web user interface of Vigor router to modify all of the settings to fit the requirements. This feature allows other user in LAN who can access into the web user interface with the same privilege of the administrator.</p> <p>Local User - Check the box to enable the local user configuration.</p> <p>Local User List - It displays the username of the local user.</p> <p>User Name - Give a user name for the local user.</p> <p>Password - Type the password for the local user.</p> <p>Confirm Password - Type the password again for</p>

confirmation.

Add - After typing the user name and password above, simply click it to create a new local user. The new one will be shown on the Local User List immediately.

Edit - If the username listed on the box above is not satisfied, simply click the username and modify it on the field of User Name. Later, click **Edit** to update the information.

Delete - If the local user listed on the box above is not satisfied, simply click the username and click **Delete** to remove it.

Enable Admin Login From Wan - The default setting is enabled. It can ensure any user accessing into web user interface of Vigor router through **Internet** by username/password of "admin/admin".

When you click **OK**, the login window will appear. Please use the new password to access into the web user interface again.

VI-1-4 User Password

This page allows you to set new password for user operation.

System Maintenance >> User Password

Enable User Mode for simple web configuration

User Password

[Set to Factory Default](#)

Password	<input type="password"/>	
Confirm Password	<input type="password"/>	(Max. 23 characters allowed)
Password Strength:	Weak Medium Strong	
Strong password requirements:		
1. Have at least one upper-case letter and one lower-case letter.		
2. Including non-alphanumeric characters is a plus.		

Note:

1. Password can contain a-z A-Z 0-9 , ; : . " < > * + = | ? @ # ^ ! ()
2. Password can't be all asterisks(*). For example, '*' or '****' is illegal, but '123*' or '*45' is OK.

OK

Available settings are explained as follows:

Item	Description
Enable User Mode for simple web configuration	After checking this box, you can access into the web user interface with the password typed here for simple web configuration. The settings on simple web user interface will be different with full web user interface accessed by using the administrator password.
Password	Type in new password in this field. The length of the password is limited to 31 characters.
Confirm Password	Type in the new password again.
Password Strength	Display the security strength of the password specified above.
Set to Factory Default	Click to return to the factory default setting.

When you click OK, the login window will appear. Please use the new password to access into the web user interface again. Below shows an example for accessing into User Operation with User Password.

1. Open System Maintenance>>User Password.
2. Check the box of **Enable User Mode for simple web configuration** to enable user mode operation. Type a new password in the field of New Password and click OK.

System Maintenance >> User Password

Enable User Mode for simple web configuration

User Password

[Set to Factory Default](#)

Password	<input type="password"/>	(Max. 23 characters allowed)
Confirm Password	<input type="password"/>	(Max. 23 characters allowed)
Password Strength:	Weak Medium Strong	
Strong password requirements:		
1. Have at least one upper-case letter and one lower-case letter.		
2. Including non-alphanumeric characters is a plus.		

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 **Vigor2133 Series**

Login

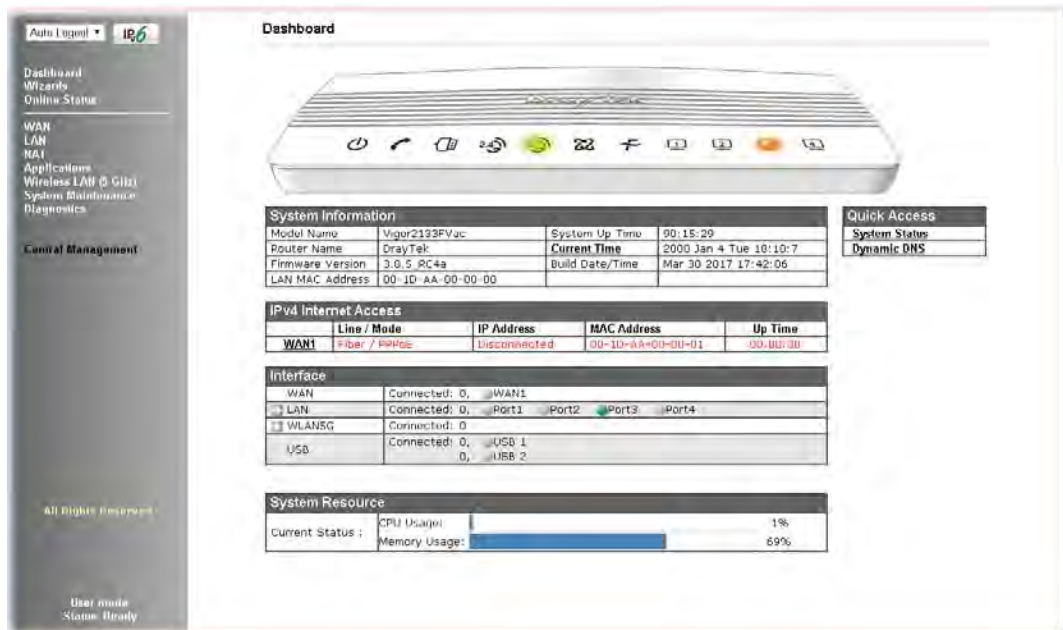
Username

Password

Login

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

6. The main screen with User Mode will be shown as follows.



Settings to be configured in User Mode will be less than settings in Admin Mode. Only basic configuration settings will be available in User Mode.



Info

Setting in User Mode can be configured as same as in Admin Mode.

VI-1-5 Login Page Greeting

When you want to access into the web user interface of Vigor router, the system will ask you to offer username and password first. At that moment, the background of the web page is blank and no heading will be displayed on the Login window. This page allows you to specify login URL and the heading on the Login window if you have such requirement.

System Maintenance >> Login Page Greeting

Login Page Greeting

Enable

Login Page Title (31 char max.)

Welcome Message and Bulletin (Max 511 characters) [Preview](#) | [Set to Factory Default](#) |

```
<h1><b><font color=red>Welcome Message</font></b></h1><p>This welcome message is displayed in the Login page of the router. Replace this text with your own message. </p><ol><li>The welcome message can be written in HTML so lists such as this one can be created </li><li>Other markup tags such as p, font or img can be used</li></ol>
```

Examples of Welcome Message and Bulletin:
<h1>Welcome Message</h1>
<p>Message</p>

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable the login customization function.
Login Page Title	Type a brief description (e.g., Welcome to DrayTek) which will be shown on the heading of the login dialog.
Welcome Message and Bulletin	Type words or sentences here. It will be displayed for bulletin message. In addition, it can be displayed on the login dialog at the bottom. Note that do not type URL redirect link here.
Preview	Click it to display the preview of the login window based on the settings on this web page.
Set to Factory Default	Click to return to the factory default setting.

Below shows an example of login customization with the information typed in Login Description and Bulletin.

Login

Just for Access Internet

Username
Password

Login

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

Welcome Message

This welcome message is displayed in the Login page of the router. Replace this text with your own message.

1. The welcome message can be written in HTML so lists such as this one can be created
2. Other markup tags such as p, font or img can be used

VI-1-6 Configuration Backup

Such function can be used to apply the router settings configured by Vigor2132 to Vigor2133.

Backup the Configuration

Follow the steps below to backup your configuration.

1. Go to **System Maintenance >> Configuration Backup**. The following page will be popped-up, as shown below.


System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restore

Restore settings from a configuration file.

選擇檔案 未選擇任何檔案

USB Storage 

Restore configuration except the login password.

Note:
This will work only if the selected configuration file was created from this device.


Backup

Back up the current settings into a configuration file.

Protect with password

Auto Backup to USB storage

Enable

Backup folder 

Periodicity backup
Cycle duration: days and hours

Backup after change configuration

Note:

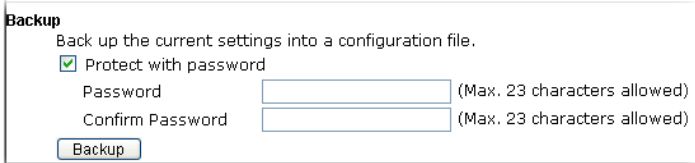
1. When loading a configuration file from a model in the Supported Model List please note that features and functionality can vary between models so please manually verify the settings after the restoration.
2. Auto backup to USB: if settings do not change, configuration doesn't backup.
3. Auto backup to USB: if configuration backup multiple times in one hour, the old file will be overwritten with the same filename.

Supported Model List

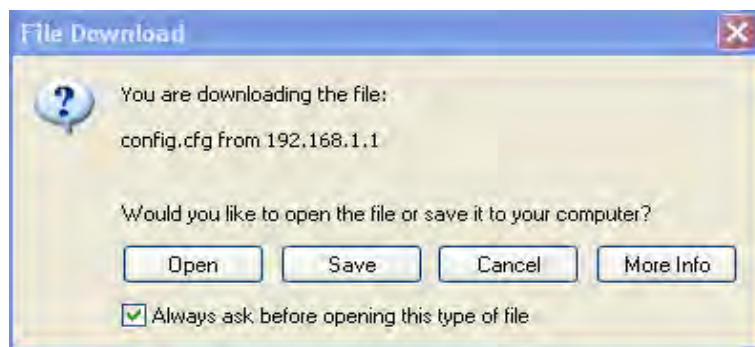
Model	Firmware Version
Vigor2132	3.7.9, or later

Available settings are explained as follows:

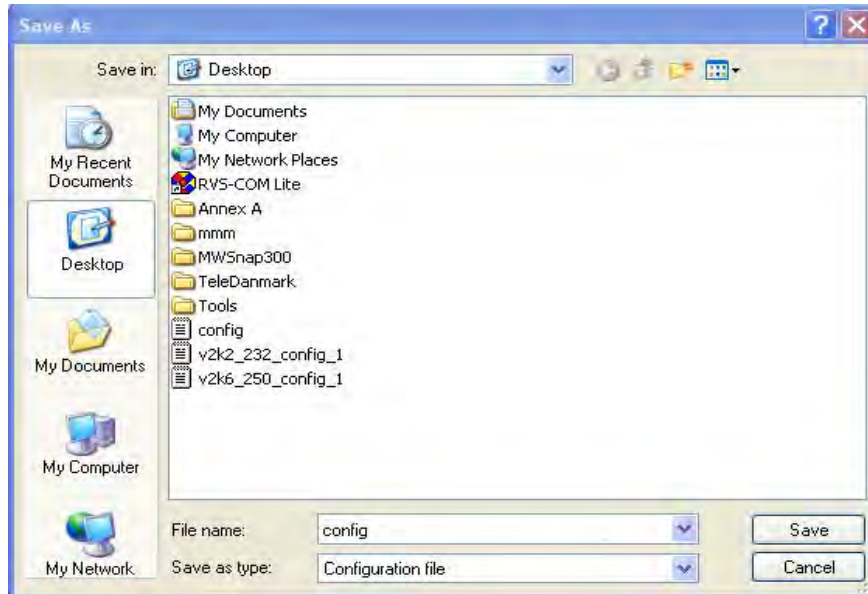
Item	Description
Restore	<p>Choose File - Click it to specify a file to be restored.</p> <p>Restore configuration except the login password - If the password settings shall not be restored and applied to Vigor2133, simply check this box to get rid of password settings.</p> <p>Click Restore to restore the configuration. If the file is encrypted, the system will ask you to type the password to decrypt the configuration file.</p>

<p>Backup</p>	<p>Click it to perform the configuration backup of this router.</p> <p>Protect with password- For the sake of security, the configuration file for the router can be encrypted.</p>  <p><small>Note: When loading a configuration file from a model in the Supported Model List please:</small></p> <ul style="list-style-type: none"> ● Password - Type several characters as the password for encrypting the configuration file. ● Confirm Password - Type the password again for confirmation.
<p>Auto Backup to USB storage</p>	<p>The configuration can be stored to a USB connecting to Vigor router as a backup.</p> <p>Backup folder - Set the path for downloading.</p> <p>Periodicity backup - Set the circle duration for backup.</p> <p>Backup after change configuration - Backup will be executed whenever the configuration is changed.</p>
<p>Support Model List</p>	<p>Web configuration file from <i>other</i> Vigor router can be applied to Vigor2133 series. At present, only the configuration file of Vigor2132 is accepted for Vigor2133.</p> <p>This field displays model name(s) and firmware which web configuration file saved can be used by such router.</p>

2. Click **Backup** button to get into the following dialog. Click **Save** button to open another dialog for saving configuration as a file.



3. In **Save As** dialog, the default filename is **config.cfg**. You could give it another name by yourself.



4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

The above example is using **Windows** platform for demonstrating examples. The **Mac** or **Linux** platform will appear different windows, but the backup function is still available.



Info

Backup for Certification must be done independently. The Configuration Backup does not include information of Certificate.

Restore Configuration

1. Go to **System Maintenance >> Configuration Backup**. The following windows will be popped-up, as shown below.

System Maintenance >> Configuration Backup

Configuration Backup / Restoration

<p>Restore</p> <p>Restore settings from a configuration file.</p> <p><input checked="" type="radio"/> 選擇檔案 未選擇任何檔案</p> <p><input type="radio"/> USB Storage <input type="text"/></p> <p><input type="checkbox"/> Restore configuration except the login password.</p> <p>Note: This will work only if the selected configuration file was created from this device.</p> <p><input type="button" value="Restore"/></p>
<p>Backup</p> <p>Back up the current settings into a configuration file.</p> <p><input type="checkbox"/> Protect with password</p> <p><input type="button" value="Backup"/></p>
<p>Auto Backup to USB storage</p> <p><input type="checkbox"/> Enable</p> <p>Backup folder <input type="text"/></p> <p><input checked="" type="radio"/> Periodicity backup Cycle duration: <input type="text"/> days and <input type="text"/> hours</p> <p><input type="radio"/> Backup after change configuration</p> <p><input type="button" value="OK"/></p>

2. Click **Choose File** button to choose the correct configuration file for uploading to the router.
3. Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

VI-1-7 Syslog/Mail Alert

SysLog function is provided for users to monitor router.

System Maintenance >> SysLog / Mail Alert Setup

SysLog / Mail Alert Setup

<p>SysLog Access Setup</p> <p><input checked="" type="checkbox"/> Enable</p> <p>Syslog Save to:</p> <p><input checked="" type="checkbox"/> Syslog Server</p> <p><input type="checkbox"/> USB Disk</p> <p>Router Name <input type="text" value="DrayTek"/></p> <p>Server IP/Hostname <input type="text"/></p> <p>Destination Port <input type="text" value="514"/></p> <p>Mail Syslog <input type="checkbox"/> Enable</p> <p>Enable syslog message:</p> <p><input checked="" type="checkbox"/> Firewall Log</p> <p><input checked="" type="checkbox"/> VPN Log</p> <p><input checked="" type="checkbox"/> User Access Log</p> <p><input checked="" type="checkbox"/> Call Log</p> <p><input checked="" type="checkbox"/> WAN Log</p> <p><input checked="" type="checkbox"/> Router/DSL information</p> <p><input checked="" type="checkbox"/> WLAN Log</p>	<p>Mail Alert Setup</p> <p><input checked="" type="checkbox"/> Enable <input type="button" value="Send a test e-mail"/></p> <p>SMTP Server <input type="text"/></p> <p>SMTP Port <input type="text" value="25"/></p> <p>Mail To <input type="text"/></p> <p>Return-Path <input type="text"/></p> <p><input type="checkbox"/> Use SSL</p> <p><input type="checkbox"/> Authentication</p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>Enable E-Mail Alert:</p> <p><input checked="" type="checkbox"/> DoS Attack</p> <p><input checked="" type="checkbox"/> APPE</p> <p><input checked="" type="checkbox"/> VPN LOG</p> <p><input type="checkbox"/> APPE Signature</p> <p><input type="checkbox"/> Debug Log</p>
---	--

Note:

1. Mail Syslog cannot be activated unless USB Disk is ticked for "Syslog Save to".
2. Mail Syslog feature sends a Syslog file when its size reaches 1M Bytes.
3. We only support secured SMTP connection on port 465.

Available settings are explained as follows:

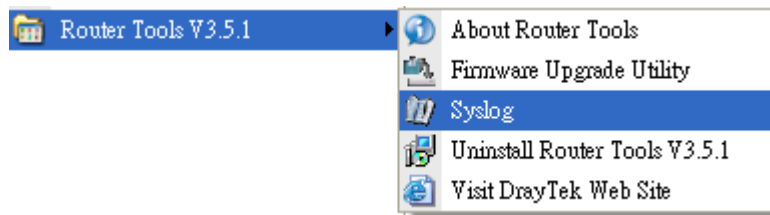
Item	Description
SysLog Access Setup	<p>Enable - Check Enable to activate function of syslog.</p> <p>Syslog Save to - Check Syslog Server to save the log to Syslog server.</p> <p>Check USB Disk to save the log to the attached USB storage disk.</p>
Router Name	<p>Display the name for such router configured in System Maintenance>>Management.</p> <p>If there is no name here, simply lick the link to access into System Maintenance>>Management to set the router name.</p> <p>Server IP /Hostname -The IP address of the Syslog server.</p> <p>Destination Port - Assign a port for the Syslog protocol.</p> <p>Mail Syslog - Check the box to recode the mail event on Syslog.</p> <p>Enable syslog message - Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to Syslog.</p>
Mail Alert Setup	<p>Check Enable to activate function of mail alert.</p> <p>Send a test e-mail - Make a simple test for the e-mail address specified in this page. Please assign the mail address first and click this button to execute a test for verify the mail</p>

	<p>address is available or not.</p> <p>SMTP Server/SMTP Port - The IP address/Port number of the SMTP server.</p> <p>Mail To - Assign a mail address for sending mails out.</p> <p>Return-Path - Assign a path for receiving the mail from outside.</p> <p>Use SSL - Check this box to use port 465 for SMTP server for some e-mail server uses https as the transmission method.</p> <p>Authentication - Check this box to activate this function while using e-mail application.</p> <p>User Name - Type the user name for authentication.</p> <p>Password - Type the password for authentication.</p> <p>Enable E-mail Alert - Check the box to send alert message to the e-mail box while the router detecting the item(s) you specify here.</p>
--	--

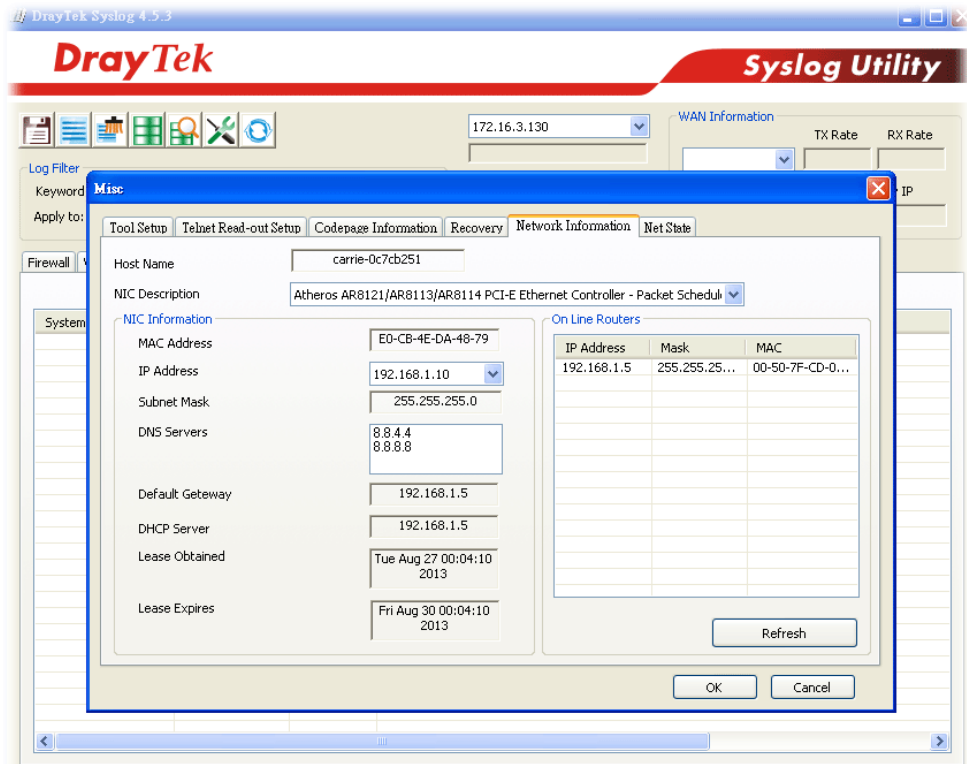
Click **OK** to save these settings.

For viewing the Syslog, please do the following:

1. Just set your monitor PC's IP address in the field of Server IP Address
2. Install the Router Tools in the **Utility** within provided CD. After installation, click on the **Router Tools>>Syslog** from program menu.



- From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.



System Time: Time taken from the computer which runs the custom application.

Router Time: Time taken from router.

VI-1-8 Time and Date

It allows you to specify where the time of the router should be inquired from.

System Maintenance >> Time and Date

Time Information

Current System Time: 2000 Jan 4 Tue 18 : 22 : 53 Inquire Time

Time Setup

Use Browser Time
 Use Internet Time

Time Server:

Priority:

Time Zone:

Enable Daylight Saving: Advanced

Automatically Update Interval:

Send NTP Request Through:

Available settings are explained as follows:

Item	Description
Current System Time	Click Inquire Time to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.
Time Server	Type the web site of the time server.
Priority	Choose Auto or IPv6 First as the priority.
Time Zone	Select the time zone where the router is located.
Enable Daylight Saving	Check the box to enable the daylight saving. Such feature is available for certain area. Advanced - Click it to open a pop up dialog.
Automatically Update Interval	Select a time interval for updating from the NTP server.
Send NTP Request	Specify a WAN interface to send NTP request for time

Daylight Saving Advanced

Default
 Start: No Daylight Saving
 End: No Daylight Saving

Date Range
 Start: Year Month Day 00 : 00
 End: Year Month Day 00 : 00

Yearly
 Start: Yearly On 00 : 00
 End: Yearly On 00 : 00

Through	synchronization.
---------	------------------

Click OK to save these settings.

VI-1-9 SNMP

This page allows you to configure settings for SNMP and SNMPV3 services.

The SNMPv3 is more secure than SNMP through the encryption method (support AES and DES) and authentication method (support MD5 and SHA) for the management needs.

System Maintenance >> SNMP

SNMP Setup

Enable SNMP Agent

Get Community:

Set Community:

Manager Host IP(IPv4)

Index	IP	Subnet Mask
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>

Manager Host IP(IPv6)

Index	IPv6 Address	Prefix Length
1	<input type="text"/>	<input type="text" value="/0"/>
2	<input type="text"/>	<input type="text" value="/0"/>
3	<input type="text"/>	<input type="text" value="/0"/>

Trap Community:

Notification Host IP(IPv4)

Index	IP
1	<input type="text"/>
2	<input type="text"/>

Notification Host IP(IPv6)

Index	IPv6 Address
1	<input type="text"/>
2	<input type="text"/>

Trap Timeout:

Enable SNMPV3 Agent

USM User:

Auth Algorithm:

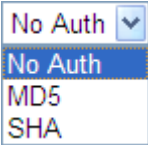
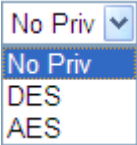
Auth Password:

Privacy Algorithm:

Privacy Password:

Available settings are explained as follows:

Item	Description
Enable SNMP Agent	Check it to enable this function.
Get Community	Set the name for getting community by typing a proper character. The default setting is public . The maximum length of the text is limited to 23 characters.
Set Community	Set community by typing a proper name. The default setting is private . The maximum length of the text is limited to 23 characters.
Manager Host IP (IPv4)	Set one host as the manager to execute SNMP function. Please type in IPv4 address to specify certain host.

Manager Host IP (IPv6)	Set one host as the manager to execute SNMP function. Please type in IPv6 address to specify certain host.
Trap Community	Set trap community by typing a proper name. The default setting is public . The maximum length of the text is limited to 23 characters.
Notification Host IP (IPv4)	Set the IPv4 address of the host that will receive the trap community.
Notification Host IP (IPv6)	Set the IPv6 address of the host that will receive the trap community.
Trap Timeout	The default setting is 10 seconds.
Enable SNMPV3 Agent	Check it to enable this function.
USM User	USM means user-based security mode. Type a username which will be used for authentication. The maximum length of the text is limited to 23 characters.
Auth Algorithm	Choose one of the encryption methods listed below as the authentication algorithm. 
Auth Password	Type a password for authentication. The maximum length of the text is limited to 23 characters.
Privacy Algorithm	Choose one of the methods listed below as the privacy algorithm. 
Privacy Password	Type a password for privacy. The maximum length of the text is limited to 23 characters.

Click OK to save these settings.

VI-1-10 Management

This page allows you to manage the settings for Internet/LAN Access Control, Access List from Internet, Management Port Setup, TLS/SSL Encryption Setup, CVM Access Control and Device Management.

The management pages for IPv4 and IPv6 protocols are different.

For IPv4


System Maintenance >> Management




IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup																																	
Router Name <input type="text" value="DrayTek"/>																																			
<input type="checkbox"/> Default:Disable Auto-Logout <input type="checkbox"/> Enable Validation Code in Internet/LAN Access <p>Note: IE8 and below version does NOT support DrayOS CAPTCHA auth code.</p> <p>Internet Access Control</p> <input type="checkbox"/> Allow management from the Internet Domain name allowed <input type="text"/> <input type="checkbox"/> FTP Server <input type="checkbox"/> HTTP Server <input type="checkbox"/> Enforce HTTPS Access <input checked="" type="checkbox"/> HTTPS Server <input type="checkbox"/> Telnet Server <input type="checkbox"/> TR069 Server <input type="checkbox"/> SSH Server <input type="checkbox"/> SNMP Server <input checked="" type="checkbox"/> Disable PING from the Internet	<p>Management Port Setup</p> <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports Telnet Port <input type="text" value="23"/> (Default: 23) HTTP Port <input type="text" value="80"/> (Default: 80) HTTPS Port <input type="text" value="443"/> (Default: 443) FTP Port <input type="text" value="21"/> (Default: 21) TR069 Port <input type="text" value="8069"/> (Default: 8069) SSH Port <input type="text" value="22"/> (Default: 22)																																		
	<p>TLS/SSL Encryption Setup</p> <input checked="" type="checkbox"/> Enable TLS 1.2 <input checked="" type="checkbox"/> Enable TLS 1.1 <input checked="" type="checkbox"/> Enable TLS 1.0 <input type="checkbox"/> Enable SSL 3.0																																		
	<p>AP Management</p> <input checked="" type="checkbox"/> Enable AP Management																																		
<p>Access List from the Internet</p> <table border="1"> <thead> <tr> <th>List</th> <th>index in IP Object</th> <th>IP / Mask</th> </tr> </thead> <tbody> <tr><td>1</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>2</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>3</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>4</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>5</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>6</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>7</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>8</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>9</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>10</td><td><input type="text"/></td><td><input type="text"/></td></tr> </tbody> </table>	List	index in IP Object	IP / Mask	1	<input type="text"/>	<input type="text"/>	2	<input type="text"/>	<input type="text"/>	3	<input type="text"/>	<input type="text"/>	4	<input type="text"/>	<input type="text"/>	5	<input type="text"/>	<input type="text"/>	6	<input type="text"/>	<input type="text"/>	7	<input type="text"/>	<input type="text"/>	8	<input type="text"/>	<input type="text"/>	9	<input type="text"/>	<input type="text"/>	10	<input type="text"/>	<input type="text"/>	<p>Device Management</p> <input type="checkbox"/> Respond to external device	
List	index in IP Object	IP / Mask																																	
1	<input type="text"/>	<input type="text"/>																																	
2	<input type="text"/>	<input type="text"/>																																	
3	<input type="text"/>	<input type="text"/>																																	
4	<input type="text"/>	<input type="text"/>																																	
5	<input type="text"/>	<input type="text"/>																																	
6	<input type="text"/>	<input type="text"/>																																	
7	<input type="text"/>	<input type="text"/>																																	
8	<input type="text"/>	<input type="text"/>																																	
9	<input type="text"/>	<input type="text"/>																																	
10	<input type="text"/>	<input type="text"/>																																	

OK

Available settings are explained as follows:

Item	Description
Router Name	Type in the router name provided by ISP.
Default: Disable Auto-Logout	If it is enabled, the function of auto-logout for web user interface will be disabled.  The web user interface will be open until you click the Logout icon manually.

	
Internet Access Control	<p>Allow management from the Internet - Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.</p> <p>Disable PING from the Internet - Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.</p>
Access List from the Internet	<p>You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.</p> <p>List index in IP Object- Type the index number of the IP object profile. Related IP with Subnet Mask will appear automatically.</p>
Management Port Setup	<p>User Define Ports - Check to specify user-defined port numbers for the Telnet, HTTP, HTTPS, FTP, TR-069 and SSH servers.</p> <p>Default Ports - Check to use standard port numbers for the Telnet and HTTP servers.</p>
TLS/SSL Encryption Setup	<p>Enable SSL 3.0 and / or TLS 1.0/1.1/1.2 - Check the box to enable the function of SSL 3.0 and/or TLS 1.0/1.1/1.2 if required.</p> <p>Due to security consideration, the built-in HTTPS and SSL VPN server of the router had upgraded to TLS1.x protocol. If you are using old browser(eg. IE6.0) or old SmartVPN Client, you may still need to enable SSL 3.0 to make sure you can connect, however, it's not recommended.</p>
Device Management	<p>Check the box to enable the device management function for Vigor2133.</p> <p>Respond to external device - If it is enabled, Vigor2133 will be regarded as slave device. When the external device (master device) sends request packet to Vigor2133, Vigor2133 would send back information to respond the request coming from the external device which is able to manage Vigor2133.</p>

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

For IPv6

System Maintenance >> Management



IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup																																	
<p>Management Access Control</p> <p><input checked="" type="checkbox"/> Allow management from the Internet</p> <ul style="list-style-type: none"> <input type="checkbox"/> Telnet Server (Port : 23) <input type="checkbox"/> HTTP Server (Port : 80) <input type="checkbox"/> HTTPS Server (Port : 443) <input type="checkbox"/> SSH Server (Port : 22) <p><input checked="" type="checkbox"/> Disable PING from the Internet</p> <hr/> <p>Access List from the Internet</p> <table border="1"> <thead> <tr> <th>List</th> <th>index in IPv6 Object</th> <th>IPv6 / Prefix</th> </tr> </thead> <tbody> <tr><td>1</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>2</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>3</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>4</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>5</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>6</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>7</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>8</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>9</td><td><input type="text"/></td><td><input type="text"/></td></tr> <tr><td>10</td><td><input type="text"/></td><td><input type="text"/></td></tr> </tbody> </table> <p>Note : Telnet / Http server port is the same as IPv4.</p> <p style="text-align: center;">OK</p>			List	index in IPv6 Object	IPv6 / Prefix	1	<input type="text"/>	<input type="text"/>	2	<input type="text"/>	<input type="text"/>	3	<input type="text"/>	<input type="text"/>	4	<input type="text"/>	<input type="text"/>	5	<input type="text"/>	<input type="text"/>	6	<input type="text"/>	<input type="text"/>	7	<input type="text"/>	<input type="text"/>	8	<input type="text"/>	<input type="text"/>	9	<input type="text"/>	<input type="text"/>	10	<input type="text"/>	<input type="text"/>
List	index in IPv6 Object	IPv6 / Prefix																																	
1	<input type="text"/>	<input type="text"/>																																	
2	<input type="text"/>	<input type="text"/>																																	
3	<input type="text"/>	<input type="text"/>																																	
4	<input type="text"/>	<input type="text"/>																																	
5	<input type="text"/>	<input type="text"/>																																	
6	<input type="text"/>	<input type="text"/>																																	
7	<input type="text"/>	<input type="text"/>																																	
8	<input type="text"/>	<input type="text"/>																																	
9	<input type="text"/>	<input type="text"/>																																	
10	<input type="text"/>	<input type="text"/>																																	

Available settings are explained as follows:

Item	Description
Management Access Control	<p>Allow management from the Internet - Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.</p> <p>Disable PING from the Internet - Check the checkbox to disable all PING packets from the Internet. For security issue, this function is enabled by default.</p>
Access List from the Internet	<p>You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.</p> <p>Index in IPv6 Object- Type the index number of the IP object profile. Related IP address will appear automatically.</p>

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

For LAN

System Maintenance >> Management



IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup
<input checked="" type="checkbox"/> Allow management from LAN		
<input checked="" type="checkbox"/> FTP Server		
<input checked="" type="checkbox"/> HTTP Server <input type="checkbox"/> Enforce HTTPS Access		
<input checked="" type="checkbox"/> HTTPS Server		
<input checked="" type="checkbox"/> Telnet Server		
<input checked="" type="checkbox"/> TR069 Server		
<input checked="" type="checkbox"/> SSH Server		
Apply To Subnet		Index in IP Object
<input checked="" type="checkbox"/> LAN1		<input type="checkbox"/> <input type="text"/>
<input checked="" type="checkbox"/> LAN2		<input type="checkbox"/> <input type="text"/>
<input checked="" type="checkbox"/> LAN3		<input type="checkbox"/> <input type="text"/>
<input checked="" type="checkbox"/> LAN4		<input type="checkbox"/> <input type="text"/>
<input checked="" type="checkbox"/> IP Routed Subnet		<input type="checkbox"/> <input type="text"/>

Note:

If an IP Object is specified in a LAN Subnet, the setting will be applied to the selected IP only.

OK

Available settings are explained as follows:

Item	Description
Allow management from LAN	Enable the checkbox to allow system administrators to login from LAN interface. There are several servers provided by the system which allow you to manage the router from LAN interface. Check the box(es) to specify.
Apply To Subnet	Check the LAN interface for the administrator to use for accessing into web user interface of Vigor router. Index in IP Object - Type the index number of the IP object profile. Related IP address will appear automatically.

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

VI-1-11 Panel Control

The behavior of the LEDs, buttons, USB ports and LAN ports on the front panel of the Vigor router can be customized as desired.

For LED

By default, the LEDs are enabled, and will illuminate or blink continuously to show the status of the various functions in the router. However, they can be configured to remain off at all times, or remain off until a button is pressed to wake them up.

System Maintenance >> Panel Control

LED	Button	USB	LAN Port	Refresh
<input checked="" type="checkbox"/> Enable LED <input type="checkbox"/> Enable Sleep Mode Turn off LED after <input type="text" value="1"/> minutes (Default: 1 minute)				

Note:

Enable the Sleep Mode will make the functions of "Wireless Button" and "Factory Reset Button" on the front panel as below:

LED Status	LED On	LED Off
Wireless Button	Wireless On/Off/WPS	Turn LED On*
Factory Reset Button	Press 1 second: Turn LED off immediately* Press till the ACT light flashing: Reset router	

*Still functional even the buttons are disabled.

OK

System Maintenance >> Panel Control

LED	Button	USB	LAN Port	Refresh
<input checked="" type="checkbox"/> Enable LED <input checked="" type="checkbox"/> Enable Sleep Mode Turn off LED after <input type="text" value="1"/> minutes (Default: 1 minute) Status : Awake, sleep after 1 minutes <input type="button" value="LED sleep immediately"/>				

Note:

Enable the Sleep Mode will make the functions of "Wireless Button" and "Factory Reset Button" on the front panel as below:

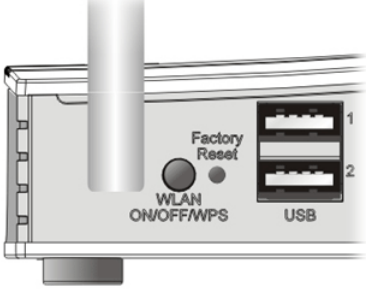
LED Status	LED On	LED Off
Wireless Button	Wireless On/Off/WPS	Turn LED On*
Factory Reset Button	Press 1 second: Turn LED off immediately* Press till the ACT light flashing: Reset router	

*Still functional even the buttons are disabled.

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 front panel LEDs. <ul style="list-style-type: none"> ● Enable Sleep Mode/Turn off LED after _ minutes - Available when Enable LED is selected. Select this

	<p>option to turn off the LEDs after the specified number of minutes.</p> <ul style="list-style-type: none"> When sleep mode is enabled, LEDs can be woken up by pressing either the Wireless LAN ON/OFF/WPS button or the Factory Reset button on the front panel, or by clicking the Wake up LED button on this page. When LEDs are lit, they can be put to sleep by briefly pressing the Factory Reset button, or by clicking the LED sleep immediately button on this page. 
<p>Status</p>	<p>Shows the status of the LEDs. Such field will be displayed after clicking Enable LED, Enable Sleep Mode and clicking OK. Later, the LED Sleep immediately will be shown on the page first.</p> <p>Status : Sleep <input type="button" value="Wake up LED"/> – LEDs are in sleep mode. To wake them up, do one of the following:</p> <ul style="list-style-type: none"> press the Wake up LED button on this page press the Wireless On/Off/WPS button on the front panel press the Factory Reset button on the front panel. <p>Status : Awake, sleep after 1 minutes <input type="button" value="LED sleep immediately"/></p> <p>– LEDs are awake. To put them to sleep immediately.</p> <ul style="list-style-type: none"> press the LED sleep immediately button on this page. press the Factory Reset button on the front panel for 1 second.

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

For Button

The **Factory Reset** and **Wireless ON/OFF/WPS** buttons on the front panel are enabled by default and can be enabled or disabled if required. Disabling the **Factory Reset** button will prevent tampering by unauthorized parties, or to avoid accidental triggering of a router reset when being used wake up LEDs. Disabling the wireless button will prevent changing the wireless setting when **LED Sleep Mode** is enabled, and the buttons are primarily used to turn the LEDs on and off.

Click the **Button** tab to get the following page.

System Maintenance >> Panel Control

LED	Button	USB	LAN Port	Refresh						
<table border="1"> <thead> <tr> <th>Enable</th> <th>Button</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>Factory Reset</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>Wireless</td> </tr> </tbody> </table>					Enable	Button	<input checked="" type="checkbox"/>	Factory Reset	<input checked="" type="checkbox"/>	Wireless
Enable	Button									
<input checked="" type="checkbox"/>	Factory Reset									
<input checked="" type="checkbox"/>	Wireless									

Available settings are explained as follows:

Item	Description
Refresh	Click to refresh the page to display the latest information.
Enable Factory Reset Button	The default value is Enabled. Deselect to disable the reset function of the factory reset button. Disabling the Factory Reset button only prevents it from being used to reboot Vigor router with default settings. It can still be used to wake up the LEDs when LED sleep mode is enabled.
Enable Wireless Button	The default value is Enabled. Deselect to disable the ability of the Wireless button to control WLAN and WPS functions. Disabling the wireless button only prevents it from being used to control WLAN functions. It can still be used to wake up the LEDs when LED sleep mode is enabled.

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

For USB

The USB ports can be individually enabled or disabled. When a USB port is disabled, attached devices will not be recognized by the router.

System Maintenance >> Panel Control

LED	Button	USB	LAN Port	Refresh									
<table border="1"> <thead> <tr> <th>Port</th> <th>Enable</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>1</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>No Device</td> </tr> <tr> <td>2</td> <td style="text-align: center;"><input type="checkbox"/></td> <td>---</td> </tr> </tbody> </table>					Port	Enable	Status	1	<input checked="" type="checkbox"/>	No Device	2	<input type="checkbox"/>	---
Port	Enable	Status											
1	<input checked="" type="checkbox"/>	No Device											
2	<input type="checkbox"/>	---											

OK

Available settings are explained as follows:

Item	Description
Refresh	Click to refresh the page to display the latest information.
Port	The number corresponds to the USB port number shown on the front panel.
Enable	Deselect to disable the USB port. The default value is enabled.

Status	Shows the status of the USB port. No device - no USB device is connected to the port. Connected - a USB device is connected to the port. --- - the USB port is disabled.
---------------	---

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

For LAN Port

The 4 LAN ports can be individually enabled or disabled. When a LAN port is disabled, attached devices will not be recognized by the router.

System Maintenance >> Panel Control

LED	Button	USB	LAN Port	Refresh																				
<table border="1"> <thead> <tr> <th>Port</th> <th>Enable</th> <th>Status</th> <th>Speed</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input checked="" type="checkbox"/></td> <td>Link Up</td> <td>1000Mbps</td> </tr> <tr> <td>2</td> <td><input checked="" type="checkbox"/></td> <td>Link Down</td> <td>---</td> </tr> <tr> <td>3</td> <td><input checked="" type="checkbox"/></td> <td>Link Down</td> <td>---</td> </tr> <tr> <td>4</td> <td><input checked="" type="checkbox"/></td> <td>Link Down</td> <td>---</td> </tr> </tbody> </table>					Port	Enable	Status	Speed	1	<input checked="" type="checkbox"/>	Link Up	1000Mbps	2	<input checked="" type="checkbox"/>	Link Down	---	3	<input checked="" type="checkbox"/>	Link Down	---	4	<input checked="" type="checkbox"/>	Link Down	---
Port	Enable	Status	Speed																					
1	<input checked="" type="checkbox"/>	Link Up	1000Mbps																					
2	<input checked="" type="checkbox"/>	Link Down	---																					
3	<input checked="" type="checkbox"/>	Link Down	---																					
4	<input checked="" type="checkbox"/>	Link Down	---																					
<input type="button" value="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.

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

VI-1-12 Self-Signed Certificate

A self-signed certificate is a *unique* identification for the device (e.g., Vigor router) which generates the certificate by itself to ensure the router security. Such self-signed certificate is signed with its own private key.

The self-signed certificate will be applied in SSL VPN, HTTPS, and so on. In addition, it can be created for free by using a wide variety of tools.

System Maintenance >> Self-Signed Certificate

Self-Signed Certificate Information

Certificate Name :	self-signed
Issuer :	C=TW, ST=HsinChu, L=HuKou, O=DrayTek Corp., OU=DrayTek Support, CN=Vigor Router
Subject :	C=TW, ST=HsinChu, L=HuKou, O=DrayTek Corp., OU=DrayTek Support, CN=Vigor Router
Subject Alternative Name :	
Valid From :	Mar 29 17:35:45 2017 GMT
Valid To :	Mar 29 17:35:45 2047 GMT
PEM Format Content :	<pre>-----BEGIN CERTIFICATE----- MIIDcTCCAlmgAwIBAgIJJAIGEftnTsrWQMAOGCSqGSIb3DQEBCwUAMHgx CzAJBgNV BAYTA1RXMRAdDgYDVRQQIDAdIc2luQ2hlMQ4wDAYDVQQHDAVidUtvdTEUMBQGA1UE CgwNRHJheVRlayBDb3JwLjEYMBYGA1UECwwPRHJheVRlayBEdXBw3JOMRUwEwYD VQQDDAxWwWdvcjB3V0ZXIwHhcNMTcwMzI5MTczNTQ1WhcNNDcwMzI5MTczNTQ1 WjB4MqswCQYDVQQGEwJUVzEQMA4GA1UECAwHSHNpbkNodTEOMAwGA1UEBwwFSHVl b3Ux FjAUBgNVBAoMDURyYXl1UzWsgQ29ycC4xGDAWBgNVBAsMDORyYXl1UzWsgU3Vw cG9ydEVMBMGA1UEAwmMvmlnb3IqUm91dGVyMIIBIjANBgkqhkiG9w0BAQEFAAOC AQ8AMIIBCgKCAQEAtOHReraoNGKu9xCn9h7DpBw2q41XG/lyBIYMD/Be14Sxolzf 4NqxxIQxLYf16jUNU+rYg2oNPxk6bl2Z+Py0a+2TmjhVW12uwcKujy6pIt/MQT3 NnpqjYJTvhsnRkqjsemPo9VYTEabWS4Wehw/xVDtwnQiyVCTF8crTjQEQPnEGMBfk cTckQ4hAvcIm51/0Rw1Hv74glap70WLOB8ykaZxSCnarZ21+HHVWahNFI0Q1tELq ifLlp//6Bon0tggVzR3Aj3HvNwHvaThpd5sT61v2CON0chvcEyBJ8RW4c/BtCa8a w/sJDVmgAQIYxzm5M3xkdtIgodcv/DMNJLMr9QIDAQAABMAOGCSqGSIb3DQEBCwUA A4IQAQBPlwaHY3AVzW38tyBYxbNYd9dh5DdxZUb50CFsbarVcaqSK+8fMQYKXXi Hrqt1viCybVEc6NKWrf8ZGzaGMRSAU88xDkCA4wwNbQHCustXqny0sGNCnfZMULL gB3V0ZQ7TVLX8I3Qzvvb8Xah5ekszedIU39Uq4oq34eKmfJVMNNoDLgBRDStc7Hj FzND3vdtTiql+v8qEs/qZZJI9RaTc5ErWrAMHCC1G0LSMTEUa0Bfvq3A1lp8TdhE bxDO5iXu9BcFpPHSS4bRP5hX3hhNxBGI4TavdvwHPCm7/Uax2YZDDYgmHP1pCTfj /P2U13nfeexTHh+aCwcRe2RApldZ -----END CERTIFICATE-----</pre>

Note:

1. Please setup the **System Maintenance >> Time and Date** correctly before you try to regenerate a self-signed certificate!!
2. The Time Zone MUST be setup correctly!!

Regenerate

Click **Regeneration** to open **Regenerate Self-Signed Certificate** window. Type in all the information that the window request such as certificate name (used for identifying different certificate), subject alternative name type and relational settings for subject name. Then click **GENERATE**.

Regenerate Self-Signed Certificate

Certificate Name	self-signed
Subject Alternative Name	
Type	IP Address ▾
IP	<input type="text"/>
Subject Name	
Country (C)	<input type="text"/>
State (ST)	<input type="text"/>
Location (L)	<input type="text"/>
Organization (O)	<input type="text"/>
Organization Unit (OU)	<input type="text"/>
Common Name (CN)	<input type="text"/>
Email (E)	<input type="text"/>
Key Type	RSA ▾
Key Size	2048 Bit ▾

VI-1-13 Reboot System

The Web user interface may be used to restart your router. Click **Reboot System** from **System Maintenance** to open the following page.

System Maintenance >> Reboot System

Reboot System

Do you want to reboot your router ?

Using current configuration
 Using factory default configuration

Auto Reboot Time Schedule

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

Note:
Action and Idle Timeout settings will be ignored.

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

If you want to reboot the router using the current configuration, check **Using current configuration** and click **Reboot Now**. To reset the router settings to default values, check **Using factory default configuration** and click **Reboot Now**. The router will take 5 seconds to reboot the system.




Info

When the system pops up Reboot System web page after you configure web settings, please click Reboot Now to reboot your router for ensuring normal operation and preventing unexpected errors of the router in the future.

VI-1-14 Firmware Upgrade

Click **System Maintenance >> Firmware Upgrade** to proceed to firmware upgrade.

System Maintenance >> Firmware Upgrade 

Web Firmware Upgrade

Select a firmware file.

未選擇檔案

Click Upgrade to upload the file.

TFTP Firmware Upgrade from LAN

Current Firmware Version: 3.8.7

Firmware Upgrade Procedures:


1. Click "OK" to start the TFTP server.
2. Open the Firmware Upgrade Utility or other 3-party TFTP client software.
3. Check that the firmware filename is correct.
4. Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade.
5. After the upgrade is complete, the TFTP server will automatically stop running.

Do you want to upgrade firmware ?

Note:

Upgrade using the ALL file will retain existing router configuration, whereas using the RST file will reset the configuration to factory defaults.

Click **Select** to specify the one you just download.

System Maintenance >> Firmware Upgrade 

Web Firmware Upgrade

Model Name: v2133
firmware version: 3.8.8

When the above page appears, click **Upgrade**. The system will upgrade the firmware of the router automatically.

VI-1-15 Activation

There are three ways to activate WCF on vigor router, using **Service Activation Wizard**, by means of **CSM>>Web Content Filter Profile** or via **System Maintenance>>Activation**.

After you have finished the setting profiles for WCF (refer to **Web Content Filter Profile**), it is the time to activate the mechanism for your computer.

Click **System Maintenance>>Activation** to open the following page for accessing <http://myvigor.draytek.com>.

System Maintenance >> Activation **Activate via interface :** auto-selected ▼

Web-Filter License **Activate**
[Status:Not Activated]

Authentication Message

Note:

1. If you want to use email alert or syslog, please configure the [SysLog/Mail Alert Setup](#) page.
2. If you change the service provider, the configuration of the function will be reset.

Available settings are explained as follows:

Item	Description
Activate via Interface	Choose WAN interface used by such device for activating Web Content Filter.
Activate	The Activate link brings you accessing into www.vigorpro.com to finish the activation of the account and the router.
Authentication Message	As for authentication information of web filter, the process of authenticating will be displayed on this field for your reference.

Below shows the successful activation of Web Content Filter:

System Maintenance >> Activation

Activate via interface: auto-selected ▾

Web-Filter License

[Activate](#)

[Status: **Commtouch**] [Start Date: **2011-03-28** Expire Date: **2011-04-27**]

```
Authentication Message
WebFilter, Activation authenticate fail, contact with support@draytek.com, 20
01 00:00:24
```

Note: If you want to use email alert or syslog, please configure the [SysLog/Mail Alert Setup](#) page.

If you change the service provider, the configuration of the function will be reset.

VI-2 Bandwidth Management

Sessions Limit

A PC with private IP address can access to the Internet via NAT router. The router will generate the records of NAT sessions for such connection. The P2P (Peer to Peer) applications (e.g., BitTorrent) always need many sessions for procession and also they will occupy over resources which might result in important accesses impacted. To solve the problem, you can use limit session to limit the session procession for specified Hosts.

Bandwidth Limit

The downstream or upstream from FTP, HTTP or some P2P applications will occupy large of bandwidth and affect the applications for other programs. Please use Limit Bandwidth to make the bandwidth usage more efficient.

Quality of Service (QoS)

Deploying QoS (Quality of Service) management to guarantee that all applications receive the service levels required and sufficient bandwidth to meet performance expectations is indeed one important aspect of modern enterprise network.

One reason for QoS is that numerous TCP-based applications tend to continually increase their transmission rate and consume all available bandwidth, which is called TCP slow start. If other applications are not protected by QoS, it will detract much from their performance in the overcrowded network. This is especially essential to those are low tolerant of loss, delay or jitter (delay variation).

Another reason is due to congestions at network intersections where speeds of interconnected circuits mismatch or traffic aggregates, packets will queue up and traffic can be throttled back to a lower speed. If there's no defined priority to specify which packets should be discarded (or in another term "dropped") from an overflowing queue, packets of sensitive applications mentioned above might be the ones to drop off. How this will affect application performance?

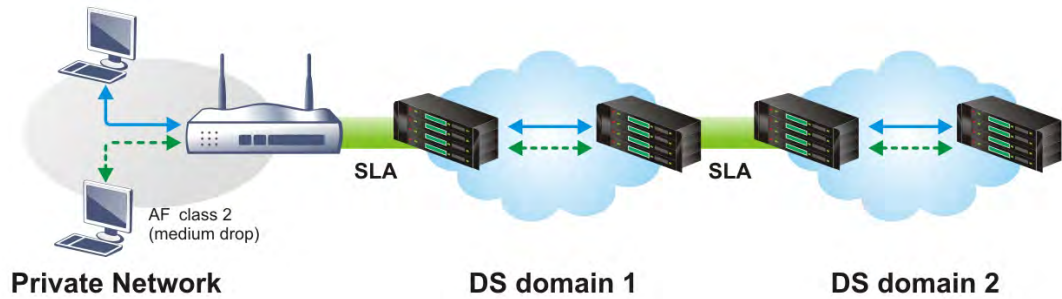
There are two components within Primary configuration of QoS deployment:

- Classification: Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.
- Scheduling: Based on classification of service level to assign packets to queues and associated service types

The basic QoS implementation in Vigor routers is to classify and schedule packets based on the service type information in the IP header. For instance, to ensure the connection with the headquarter, a teleworker may enforce an index of QoS Control to reserve bandwidth for HTTPS connection while using lots of application at the same time.

One more larger-scale implementation of QoS network is to apply DSCP (Differentiated Service Code Point) and IP Precedence disciplines at Layer 3. Compared with legacy IP Precedence that uses Type of Service (ToS) field in the IP header to define 8 service classes, DSCP is a successor creating 64 classes possible with backward IP Precedence compatibility. In a QoS-enabled network, or Differentiated Service (DiffServ or DS) framework, a DS domain owner should sign a Service License Agreement (SLA) with other DS domain owners to define the service level provided toward traffic from different domains. Then each DS node in these domains will perform the priority treatment. This is called per-hop-behavior (PHB). The definition of PHB includes Expedited Forwarding (EF), Assured Forwarding (AF), and Best Effort (BE). AF defines the four classes of delivery (or forwarding) classes and three levels of drop precedence in each class.

Vigor routers as edge routers of DS domain shall check the marked DSCP value in the IP header of bypassing traffic, to allocate certain amount of resource execute appropriate policing, classification or scheduling. The core routers in the backbone will do the same checking before executing treatments in order to ensure service-level consistency throughout the whole QoS-enabled network.



However, each node may take different attitude toward packets with high priority marking since it may bind with the business deal of SLA among different DS domain owners. It's not easy to achieve deterministic and consistent high-priority QoS traffic throughout the whole network with merely Vigor router's effort.

Web User Interface

Below shows the menu items for Bandwidth Management.



VI-2-1 Sessions Limit

In the Bandwidth Management menu, click Sessions Limit to open the web page.

Bandwidth Management >> Sessions Limit

IPv4
IPv6

Enable
 Disable

Default Max Sessions:

Limitation List

Index	Start IP	End IP	Max Sessions

Specific Limitation

Start IP: End IP:

Maximum Sessions:

Administration Message (Max 255 characters)

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

Time Schedule

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

Note:
Action and Idle Timeout settings will be ignored.

To activate the function of limit session for IPv4 and/or IPv6, simply click Enable and set the default session limit.

Available settings are explained as follows:

Item	Description
Session Limit	<p>Enable - Click this button to activate the function of limit session.</p> <p>Disable - Click this button to close the function of limit session.</p>

	Default Max Sessions - Defines the default session number used for each computer in LAN.
Limitation List	Displays a list of specific limitations that you set on this web page.
Specific Limitation	<p>Start IP- Defines the start IP address for limit session.</p> <p>End IP - Defines the end IP address for limit session.</p> <p>Maximum Sessions - Defines the available session number for each host in the specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index.</p> <p>Add - Adds the specific session limitation onto the list above.</p> <p>Edit - Allows you to edit the settings for the selected limitation.</p> <p>Delete - Remove the selected settings existing on the limitation list.</p>
Administration Message	<p>Type the words which will be displayed when reaches the maximum number of Internet sessions permitted.</p> <p>Default Message - Click this button to apply the default message offered by the router.</p>
Time Schedule	Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page.

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

VI-2-2 Bandwidth Limit

In the Bandwidth Management menu, click **Bandwidth Limit** to open the web page.

Bandwidth Management >> Bandwidth Limit

IPv4
IPv6

Enable
 IP Routed Subnet
 Disable

Default TX Limit Per User: Kbps
 Default RX Limit Per User: Kbps

Limitation List

Index	Start IP/Group	End IP/Object	TX limit	RX limit	Shared

Specific Limitation IP Object

Start IP: End IP:

Each Shared
 TX Limit: Kbps
 RX Limit: Kbps

Allow auto adjustment to assign available bandwidth equally to active user.

Smart Bandwidth Limit

For any LAN IP Not in Limitation List, whose session number exceeds

TX Limit : Kbps
 RX Limit : Kbps

Note:

- For TX/RX, a setting of "0" means unlimited bandwidth.
- Available bandwidth is calculated according to the maximum bandwidth detected or the Line Speed defined in WAN >> **General Setup** when in "According to Line Speed" Load Balance mode.

Time Schedule

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

Note:
Action and Idle Timeout settings will be ignored.

To activate the function of limit bandwidth for IPv4 and /or IPv6, simply click **Enable** and set the default upstream and downstream limit.

Available settings are explained as follows:

Item	Description
Bandwidth Limit	<p>Enable - Click this button to activate the function of limit bandwidth.</p> <p>IP Routed Subnet - Check this box to apply the bandwidth limit to the second subnet specified in LAN>>General Setup. It is available for IPv4 settings only.</p> <p>Disable - Click this button to close the function of limit bandwidth.</p> <p>Default TX limit Per User- Define the default speed of the upstream for each computer in LAN.</p> <p>Default RX limit Per User- Define the default speed of the downstream for each computer in LAN.</p>
Limitation List	Display a list of specific limitations that you set on this web page.
Specific Limitation	Start IP - Define the start IP address for limit bandwidth.

	<p>End IP - Define the end IP address for limit bandwidth.</p> <p>Each /Shared - Select Each to make each IP within the range of Start IP and End IP having the same speed defined in TX limit and RX limit fields; select Shared to make all the IPs within the range of Start IP and End IP share the speed defined in TX limit and RX limit fields.</p> <p>TX limit - Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.</p> <p>RX limit - Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.</p> <p>Add - Add the specific speed limitation onto the list above.</p> <p>Edit - Allow you to edit the settings for the selected limitation.</p> <p>Delete - Remove the selected settings existing on the limitation list.</p>
Allow auto adjustment...	Check this box to make the best utilization of available bandwidth.
Smart Bandwidth Limit	<p>Check this box to have the bandwidth limit determined by the system automatically.</p> <p>TX limit - Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.</p> <p>RX limit - Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.</p>
Time Schedule	Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page.

VI-2-3 Quality of Service

In the Bandwidth Management menu, click Quality of Service to open the web page.


Bandwidth Management >> Quality of Service

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

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

Class Rule

Index	Name	Rule	Service Type
Class 1		Edit	
Class 2		Edit	Edit
Class 3		Edit	

Enable the First Priority for VoIP SIP/RTP: 

SIP UDP Port: (Default:5060)

Available settings are explained as follows:

Item	Description
General Setup	<p>Index - Display the WAN interface number that you can edit.</p> <p>Status - Display if the WAN interface is available for such function or not.</p> <p>Bandwidth - Display the inbound and outbound bandwidth setting for the WAN interface.</p> <p>Direction - Display which direction that such function will influence.</p> <p>Class 1/Class2/Class 3/Others - Display the bandwidth percentage for each class.</p> <p>UDP Bandwidth Control - Display the UDP bandwidth control is enabled or not.</p> <p>Online Statistics - Display an online statistics for quality of service for your reference.</p> <p>Setup - Allow to configure general QoS setting for WAN interface.</p>
Class Rule	<p>Index - Display the class number that you can edit.</p> <p>Name - Display the name of the class.</p> <p>Rule - Allow to configure detailed settings for the selected Class.</p> <p>Service Type - Allow to configure detailed settings for the service type.</p>
Enable the First Priority for VoIP SIP/RTP	<p>When this feature is enabled, the VoIP SIP/UDP packets will be sent with highest priority.</p> <p>SIP UDP Port - Set a port number used for SIP.</p>

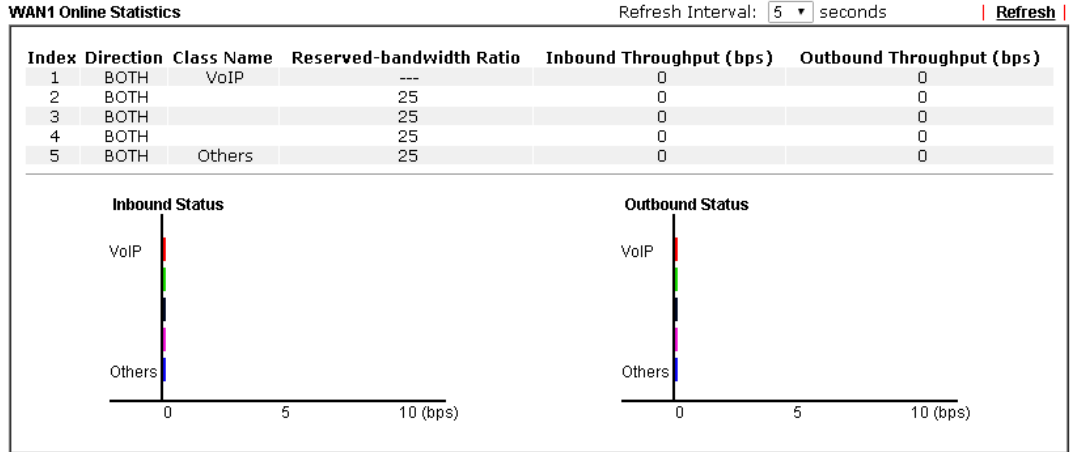
This page displays the QoS settings result of the WAN interface. Click the **Setup** link to access into next page for the general setup of WAN interface. As to class rule, simply click the **Edit** link to access into next for configuration.

You can configure general setup for the WAN interface, edit the Class Rule, and edit the Service Type for the Class Rule for your request.

Online Statistics

Display an online statistics for quality of service for your reference. This feature is available only when the Quality of Service for WAN interface is enabled.

Bandwidth Management >> Quality of Service



Cancel

General Setup for WAN Interface

When you click **Setup**, you can configure the bandwidth ratio for QoS of the WAN interface. There are four queues allowed for QoS control. The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. Yet, the last one is reserved for the packets which are not suitable for the user-defined class rules.

Bandwidth Management >> Quality of Service

General Setup

Enable the QoS Control BOTH ▾

WAN Inbound Bandwidth	100	<input type="radio"/> Kbps	<input checked="" type="radio"/> Mbps
WAN Outbound Bandwidth	100	<input type="radio"/> Kbps	<input checked="" type="radio"/> Mbps

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

Enable UDP Bandwidth Control Limited_bandwidth Ratio %

Outbound TCP ACK Prioritize

Note:

1. Before enable QoS, you should test the real bandwidth first. QoS may not work properly if the bandwidth is not accurate.
2. You can do speed test by <http://speedtest.net> or contact with your ISP for speed test program.

Available settings are explained as follows:

Item	Description
Enable the QoS Control	The factory default for this setting is checked. Please also define which traffic the QoS Control settings will apply to. IN- apply to incoming traffic only. OUT-apply to outgoing traffic only. BOTH- apply to both incoming and outgoing traffic. Check this box and click OK , then click Setup link again. You will see the Online Statistics link appearing on this page.
WAN Inbound Bandwidth	It allows you to set the connecting rate of data input for other WAN. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 1000kbps for this box. The default value is 10000kbps.
WAN Outbound Bandwidth	It allows you to set the connecting rate of data output for other WAN. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 256kbps for this box. The default value is 10000kbps.
Reserved Bandwidth Ratio	It is reserved for the group index in the form of ratio of reserved bandwidth to upstream speed and reserved bandwidth to downstream speed.
Enable UDP Bandwidth Control	Check this and set the limited bandwidth ratio on the right field. This is a protection of TCP application traffic since UDP application traffic such as streaming video will exhaust lots of bandwidth.
Outbound TCP ACK Prioritize	The difference in bandwidth between download and upload are great in ADSL2+ environment. For the download speed

	might be impacted by the uploading TCP ACK, you can check this box to push ACK of upload faster to speed the network traffic.
Limited_bandwidth Ratio	The ratio typed here is reserved for limited bandwidth of UDP application.



Info

The rate of outbound/inbound must be smaller than the real bandwidth to ensure correct calculation of QoS. It is suggested to set the bandwidth value for inbound/outbound as 80% - 85% of physical network speed provided by ISP to maximize the QoS performance.

Edit the Class Rule for QoS

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

Bandwidth Management >> Quality of Service

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

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

Class Rule

Index	Name	Rule	Service Type
Class 1		Edit	
Class 2		Edit	Edit
Class 3		Edit	

Enable the First Priority for VoIP SIP/RTP:
 SIP UDP Port: (Default: 5060)

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

Bandwidth Management >> Quality of Service

Class Index #1

Name Tag Outbound Packets as:

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Empty	-	-	-	-

- For adding a new rule, click **Add** to open the following page.

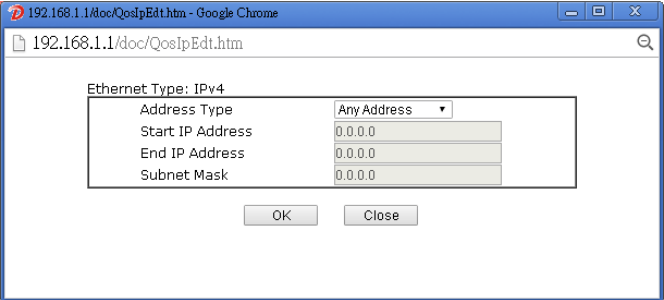
Bandwidth Management >> Quality of Service

Rule Edit

<input checked="" type="checkbox"/> ACT	<input type="checkbox"/> Hardware Acceleration
Ethernet Type	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Local Address	Any <input type="button" value="Edit"/>
Remote Address	Any <input type="button" value="Edit"/>
DiffServ CodePoint	ANY
Service Type	---Predefined---

Note:
Please choose/setup the **Service Type** first.

Available settings are explained as follows:

Item	Description
ACT	Check this box to invoke these settings.
Hardware Acceleration	Check this box to enable the hardware acceleration when such rule is applied.
Ethernet Type	Please specify which protocol (IPv4 or IPv6) will be used for this rule.
Local Address	Click the Edit button to set the local IP address (on LAN) for the rule.
Remote Address	Click the Edit button to set the remote IP address (on LAN/WAN) for the rule. 
DiffServ CodePoint	All the packets of data will be divided with different levels and will be processed according to the level type by the system. Please assign one of the levels of the data for processing with QoS control.
Service Type	It determines the service type of the data for processing with QoS control. It can also be edited. You can choose the predefined service type from the Service Type drop down list. Those types are predefined in factory. Simply choose the one that you want for using by current QoS.

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

By the way, you can set up to 20 rules for one Class. If you want to edit an existed rule, please select the radio button of that one and click **Edit** to open the rule edit page for modification.

Bandwidth Management >> Quality of Service

Class Index #1
 Name Tag Outbound Packets as:

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

Edit the Service Type for Class Rule

- To add a new service type, edit or delete an existed service type, please click the Edit link under Service Type field.

Bandwidth Management >> Quality of Service

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

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

Class Rule

Index	Name	Rule	Service Type
Class 1		Edit	
Class 2		Edit	Edit
Class 3		Edit	

Enable the First Priority for VoIP SIP/RTP:
 SIP UDP Port: (Default:5060)

- After you click the Edit link, you will see the following page.

Bandwidth Management >> Quality of Service

User Defined Service Type

NO	Name	Protocol	Port
1	Empty	-	-

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

Bandwidth Management >> Quality of Service

Service Type Edit

Service Name	<input type="text"/>
Service Type	TCP <input type="text" value="6"/>
Port Configuration	<input checked="" type="radio"/> Single <input type="radio"/> Range
Type	<input type="text" value="0"/> - <input type="text" value="0"/>
Port Number	<input type="text" value="0"/> - <input type="text" value="0"/>

Available settings are explained as follows:

Item	Description
Service Name	Type in a new service for your request. The maximum length of the name you can set is 11 characters.
Service Type	Choose the type (TCP, UDP or TCP/UDP or other) for the new service.
Port Configuration	<p>Type - Click Single or Range as the Type. If you select Range, you have to type in the starting port number and the end porting number on the boxes below.</p> <p>Port Number - Type in the starting port number and the end porting number here if you choose Range as the type.</p>

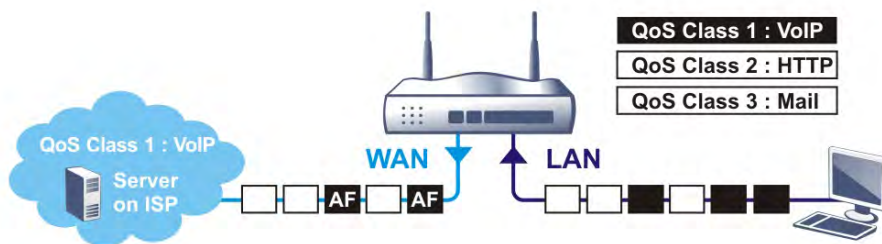
- After finishing all the settings here, please click **OK** to save the configuration.

By the way, you can set up to 10 service types. If you want to edit/delete an existed service type, please select the radio button of that one and click **Edit/Edit** for modification.

Retag the Packets for Identification

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

For example, in the following illustration, the VoIP packets in LAN go into Vigor router without any header. However, when they go forward to the Server on ISP through Vigor router, all of the packets are tagged with AF (configured in Bandwidth >>QoS>>Class) automatically.



Bandwidth Management >> Quality of Service

Class Index #1

Name: Tag packets as:

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Active	Any	Any	ANY	ANY

VI-2-4 APP QoS

The QoS function is used to do bandwidth management for the services with certain IP or port number. However, there is no effect of bandwidth management on the service such as VNC or PPTV without fixed IP or port number.

APP QoS employs the function of APP Enforcement to detect the types of software in application layer. By combining the function of QoS (adjustment on Inbound/Outbound bandwidth and bandwidth ratio), Vigor router can perform the bandwidth management for the protocols, streaming, remote control, web HD and so on.

Click **Bandwidth Management >> APP QoS** to open the following page.

Bandwidth Management >> APP QoS

APP QoS

Enable Disable

Traceable **Untraceable**

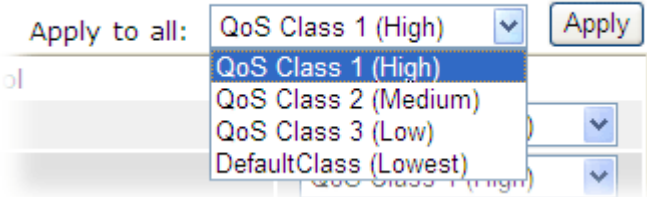
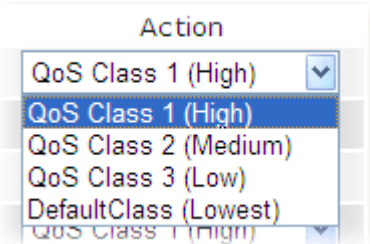
 Apply to all:

Enable	Protocol	Version	Action
<input type="checkbox"/>	DNS		QoS Class 1 (High) ▼
<input type="checkbox"/>	FTP		QoS Class 1 (High) ▼
<input type="checkbox"/>	HTTP	1.1	QoS Class 1 (High) ▼
<input type="checkbox"/>	IMAP	4.1	QoS Class 1 (High) ▼
<input type="checkbox"/>	IMAP STARTTLS	4.1	QoS Class 1 (High) ▼
<input type="checkbox"/>	IRC	2.4.0	QoS Class 1 (High) ▼
<input type="checkbox"/>	NNTP		QoS Class 1 (High) ▼
<input type="checkbox"/>	POP3		QoS Class 1 (High) ▼
<input type="checkbox"/>	POP3 STARTTLS		QoS Class 1 (High) ▼
<input type="checkbox"/>	QUIC	Q025	QoS Class 1 (High) ▼
<input type="checkbox"/>	SMB	3.0	QoS Class 1 (High) ▼
<input type="checkbox"/>	SMTP		QoS Class 1 (High) ▼
<input type="checkbox"/>	SMTP STARTTLS		QoS Class 1 (High) ▼
<input type="checkbox"/>	SNMP	2C	QoS Class 1 (High) ▼
<input type="checkbox"/>	SSH	2	QoS Class 1 (High) ▼
<input type="checkbox"/>	SSL/TLS	3.0/1.2	QoS Class 1 (High) ▼
<input type="checkbox"/>	TELNET		QoS Class 1 (High) ▼

Note:
Please remember to adjust Inbound/Outbound bandwidth of your network in "Quality of Service". This will help QoS to work more efficient.

Available settings are explained as follows:

Item	Description
Enable/Disable	Click Enable to activate APP QoS function. Click Disable to deactivate APP QoS function.
Traceable	The protocol listed below is traceable by Vigor router. Each tab offers different types of protocols to fit your request.
Untraceable	The protocol listed below is not easy to be traced by Vigor router. Each tab offers different types of protocols to fit your request.

Select All	Click it to select all of the protocols.
Clear All	Click it to de-select all of the protocols.
Apply to all	<p>Choose one of the actions from the drop down list. It is prepared for applying to all protocols.</p>  <p>Apply - Click it to make the selected action be applied all of the selected protocols immediately.</p>
Action	<p>There are many protocols which can be specified with different QoS Class.</p> 

Application Notes

A-1 How to Optimize the Bandwidth through QoS Technology

Have you ever gotten any problems in uploading/downloading files (Voice, video or email/data only) with the narrow/districted bandwidth you may share from the common Internet connection line? The advanced bandwidth management technology-QoS (Quality of Service) helps you to well allocate the bandwidth upon your demand of Voice, Video, or Data transferring. Let's see how to get the optimum bandwidth per your request by using DrayTek Vigor router as below.

Scenario: The Internet connection you got from ISP line is 2MB/512Kb. There are VoIP telephony network, IPTV set top box and data server at your home. Assume you want to allocate 30% of the bandwidth you got to VoIP demand, 50% for IPTV, 15% for mail/data, 5% for others. Let's see how easily it is to do the setting as below:

1. Open Bandwidth Management>> Quality of Service.



2. You will get the following page. Click the Edit link for Class 1.


Bandwidth Management >> Quality of Service

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

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

Class Rule

Index	Name	Rule	Service Type
Class 1		Edit	
Class 2		Edit	Edit
Class 3		Edit	

Enable the First Priority for VoIP SIP/RTP:
SIP UDP Port: (Default:5060) 

3. In the following page, type a name (e.g., VoIP) for such class and click Add.

Bandwidth Management >> Quality of Service

Class Index #1
Name Tag Outbound Packets as:

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Empty	-	-	-	-

4. Check the box of ACT. Click Edit to specify the local address.

Bandwidth Management >> Quality of Service

Rule Edit

ACT Hardware Acceleration

Ethernet Type IPv4 IPv6

Local Address Any

Remote Address Any

DiffServ CodePoint ANY

Service Type ---Predefined---

Note:
Please choose/setup the **Service Type** first.

5. In the pop-up window, choose Range Address as the Address Type and type the start IP address and end IP address in relational fields. Click OK to save the settings and exit the window.

192.168.1.1/doc/QosIpEdt.htm - Google Chrome

192.168.1.1/doc/QosIpEdt.htm

Ethernet Type: IPv4

Address Type Range Address

Start IP Address 172.16.1.240

End IP Address 172.16.1.241

Subnet Mask 0.0.0.0

6. Click OK again to save the settings.

Bandwidth Management >> Quality of Service

Rule Edit

ACT Hardware Acceleration

Ethernet Type IPv4 IPv6

Local Address 172.16.1.240~172.16.1.241

Remote Address Any

DiffServ CodePoint ANY

Service Type ---Predefined---

Note:
Please choose/setup the **Service Type** first.

7. The class rule for VoIP has been set. Click OK to return to previous page.

Bandwidth Management >> Quality of Service

Class Index #1

Name VoIP Tag Outbound Packets as: Default

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Active	172.16.1.240 ~ 172.16.1.241	Any	ANY	ANY

8. Do the same steps to add class rules for IPTV and Data/Email with IP addresses as shown below.

Bandwidth Management >> Quality of Service

Class Index #2
 Name Tag Outbound Packets as:

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 <input type="radio"/>	Inactive	Any	Any	ANY	undefined
2 <input type="radio"/>	Active	172.16.1.242 ~ 172.16.1.249	Any	ANY	ANY

and

Bandwidth Management >> Quality of Service

Class Index #3
 Name Tag Outbound Packets as:

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 <input type="radio"/>	Active	Any	Any	IP precedence 2	DNS(TCP/UDP:53)

9. Assuming you get 2MB/512Kb Internet line. You can click the **Setup** link of WAN1 to set up the bandwidth for different groups among VoIP, IPTV and Data/Email.

Bandwidth Management >> Quality of Service

General Setup [Set to Factory Default](#)

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

Class Rule

Index	Name	Rule	Service Type
Class 1	VoIP	Edit	
Class 2	IPTV	Edit	Edit
Class 3	Data/Email	Edit	

Enable the First Priority for VoIP SIP/RTP:
 SIP UDP Port: (Default: 5060)

10. In the Setup page, check the box of **Enable the QoS Control**. Type 30, 50 and 15 in the boxes for VoIP, IPTV and Data/Email respectively. Check the box of **Enable UDP Bandwidth Control**.

Bandwidth Management >> Quality of Service

General Setup

Enable the QoS Control OUT ▾

WAN Inbound Bandwidth Kbps Mbps
 WAN Outbound Bandwidth Kbps Mbps

Index	Class Name	Reserved Bandwidth Ratio
Class 1	VoIP	<input type="text" value="30"/> %
Class 2	IPTV	<input type="text" value="50"/> %
Class 3	Data/Email	<input type="text" value="15"/> %
	Others	<input type="text" value="5"/> %

Enable UDP Bandwidth Control Limited_bandwidth Ratio %
 Outbound TCP ACK Prioritize

Note:

1. Before enable QoS, you should test the real bandwidth first. QoS may not work properly if the bandwidth is not accurate.
2. You can do speed test by <http://speedtest.net> or contact with your ISP for speed test program.

11. Click OK to save the settings. The class rules for WAN1 are defined as shown below.

Bandwidth Management >> Quality of Service

General Setup

[Set to Factory Default](#)

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics
WAN1	Disable	100000Kbps/100000Kbps	Both	<input type="text" value="30"/> %	<input type="text" value="50"/> %	<input type="text" value="15"/> %	<input type="text" value="5"/> %	Inactive	Status Setup
WAN3	Disable	100000Kbps/100000Kbps	Both	<input type="text" value="25"/> %	<input type="text" value="25"/> %	<input type="text" value="25"/> %	<input type="text" value="25"/> %	Inactive	Status Setup

Class Rule

Index	Name	Rule	Service Type
Class 1	VoIP	Edit	
Class 2	IPTV	Edit	Edit
Class 3	Data/Email	Edit	

Enable the First Priority for VoIP SIP/RTP:
 SIP UDP Port: (Default:5060) 

VI-3 Hotspot Web Portal

The Hotspot Web Portal feature allows you to set up profiles so that LAN users could either be redirected to specific URLs, or be shown messages when they first connect to the Internet through the router. Users could be required to read and agree to terms and conditions, or authenticate themselves, prior to gaining access to the Internet. Other potential uses include the serving of advertisements and promotional materials, and broadcast of public service announcements.

Web User Interface

LAN
Hotspot Web Portal
Profile Setup
Load Balance/Route Policy

VI-3-1 Profile Setup

Select **Profile Setup** to create or modify Portal profiles. Up to 4 profiles can be created to meet different requirements according to LAN subnets, WLAN SSIDs, origin and destination IP addresses, etc.

Hotspot Web Portal >> Profile Setup



Hotspot Web Portal Profile:

Index	Enable	Comments	Login Mode	Applied Interface	
1.	<input type="checkbox"/>		Click-through	None	Preview
2.	<input type="checkbox"/>		Click-through	None	Preview
3.	<input type="checkbox"/>		Click-through	None	Preview
4.	<input type="checkbox"/>		Click-through	None	Preview

Note:

1. The router must connect to the Internet before webpage redirection will work.
2. If the LAN clients are using another DNS server on LAN, please make sure the DNS query for domain name "portal.draytek.com" will be resolved by the router.

[OK](#)

Available settings are explained as follows:

Item	Description
Index	Click the index number link to view or update the profile settings.
Enable	Check the box to enable the profile.
Comments	Shows the description of the profile.
Login Mode	Shows the login mode used by the profile. See the section <i>Login Mode</i> for details.
Applied Interface	Shows the interfaces to which this profile applies.
Preview	Click this button to preview the Hotspot Web Portal page that will be displayed to users.

VI-4-1-1 Login Modes

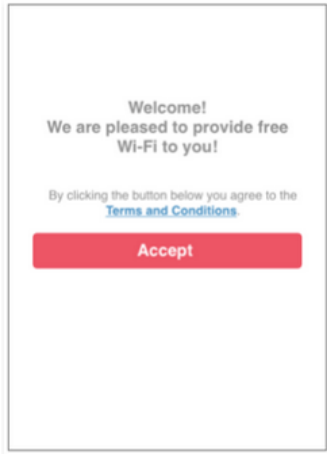
There are five login modes to choose from for authenticating network clients: **Skip Login**, **Click Through**, **Social Login**, **PIN Login**, and **Social or PIN Login**. Each login mode will present a different web page to users when they connect to the network.

Skip Login

This mode does not perform any authentication. The user will be redirected to the landing page. The user can then leave the landing page to visit other websites.

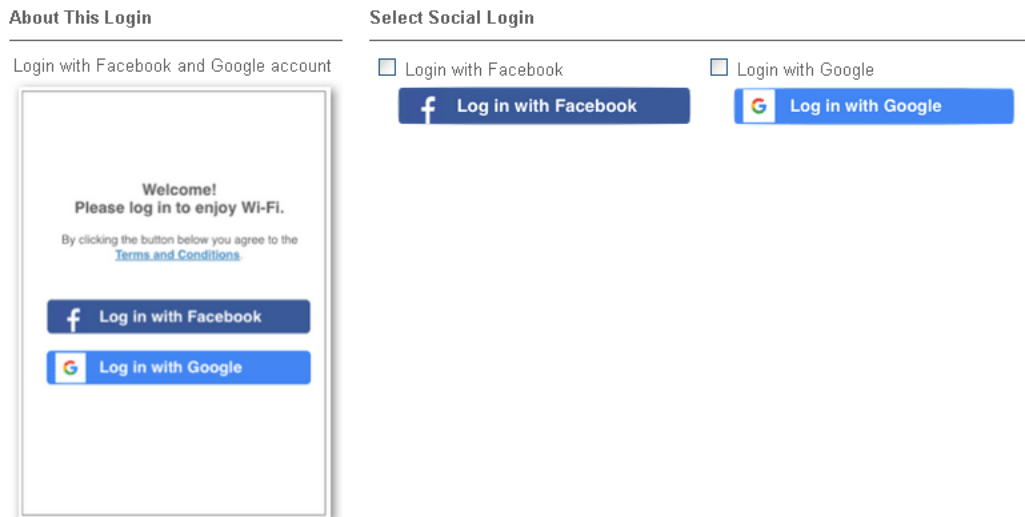
Click-through

The following page will be shown to the users when they first attempt to access the Internet through the router. After clicking **Accept** on the page, users will be directed to the landing page and be granted access to the Internet.



Social Login

The following page will appear when users attempt to access the Internet for the first time via the router. After authenticating themselves using either a Facebook or Google account, they will be directed to the landing page and be granted access to the Internet.



PIN Code Login

When users attempt to connect to the Internet for the first time, they will be prompted to enter a mobile number to receive a PIN by SMS. After they have authenticated themselves by entering the PIN, they will be redirected to the landing page, indicating that they have been granted Internet access.

About This Login

Router can generate PIN and send to clients via SMS.

Welcome!
Please log in to enjoy WiFi.

By clicking the button below you agree to the [Terms and Conditions](#).

Receive PIN Via SMS

Already have PIN?

Enter Existing PIN

Receive PIN via SMS

Second page for entering mobile number to receive PIN

< Back

PIN Code will be sent over via SMS.

+ 886

Send PIN

Enter PIN

Social or PIN Login

This login mode presents both Social Login and PIN Code Login modes to the users, and allows them to select their preferred mode of authentication.

About This Login

Provide all kinds of login methods for Wi-Fi clients to choose.

Welcome!
Please log in to enjoy Wi-Fi.

By clicking the button below you agree to the [Terms and Conditions](#).

Log in with Facebook

Log in with Google

Or log in with PIN code.

Receive PIN via SMS

Enter Existing PIN

Select Social Login

Log in with Facebook

Log in with Google

PIN Login

Second page for entering mobile number to receive PIN

< Back

PIN Code will be sent over via SMS.

+ 886

Send PIN

Enter PIN

VI-4-1-2 Steps for Configuring a Web Portal Profile

1. Login Method

Click the index link (e.g., #1) of the selected profile to display the following page.

Hotspot Web Portal >> Profile Setup

The screenshot shows a five-step process flow: 1. Login Method (highlighted in red), 2. Background, 3. Login Page Setup, 4. Whitelist Setting, and 5. More Options. Below the flow, there is a checkbox for 'Enable this profile' which is checked, and a 'Comments' field containing 'Floor_1'. Under the heading 'Choose Login Method', there are five buttons: 'Skip Login' (red), 'Click Through', 'Social Login', 'PIN Login', and 'Social or PIN Login'. At the bottom, there are 'Save and Next' and 'Cancel' buttons.

Available settings are explained as follows:

Item	Description
Enable this profile	Check to enable this profile.
Comments	Enter a brief description to identify this profile.
Choose Login Method	Select the desired Login Mode.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to save the configuration on this page and proceed to the next page.

If you have chosen **Skip Login** as the Login Mode, skip to step 4 *Whitelisting* below.

Otherwise, proceed to configure the login page by following steps 2 and 3.

2. Background

If you have selected a Login Mode that requires authentication, select a background for the login page.

Hotspot Web Portal >> ProfileSetup



Choose Login Background

Color Background

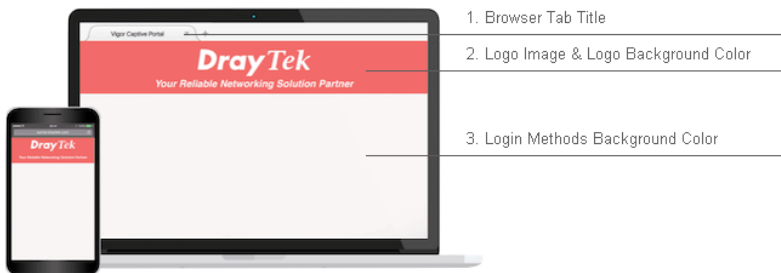


Image Background



Login Page URL

Browser Table Title

Logo Image



Logo Background Color

(format : FFFFFFFF)

Login Method Background Color

(format : FFFFFFFF)

Available settings are explained as follows:

Item	Description
Choose Login Background	Select either Color Background or Image Background as the login page background scheme.
Login Page URL	Enter the URL for the login page.
Browser Tab Title	Enter the text to be shown as the webpage title in the browser.
Logo Image	The DrayTek Logo will be displayed by default. However, you can enter HTML text or upload an image to replace the default logo.
Logo Background Color	Select the background color of the logo from the predefined color list, or select Customize Color and enter the RGB values. Click Preview to preview the selected color.
Login Method Background Color	Select the background color of the login panel from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.
Opacity (10 ~ 100)	Available when Image Background is selected. Set the opacity of the background image.
Background Image	Available when Image Background is selected. Click Browse... to select an image file (.JPG or .PNG format), then click Upload to upload it to the router.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

If you have selected **Skip Login** as the Login Mode, proceed to Step 4 *Whitelist Setting*; otherwise, continue to Step 3 *Login Page Setup*.

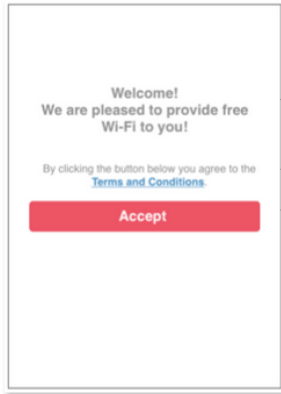
3. Login Page Setup

In this step you can configure settings for the login page.

Click Through

This section describes the Login Page setup if you have selected **Click Through** as the Login Mode.

Configure Login Method and Details



Welcome Message

Terms and Conditions Description and Content

Accept Button Description and Color

Welcome Message

Welcome!
We are pleased to provide free Wi-Fi to you!

(Max 1360 characters)

Default

Terms and Conditions Description

By clicking the button below you agree to the Terms and Conditions.

(Max 170 characters)

Default

Terms and Conditions Content

(Max 170 characters)

Accept Button Description

accept

(Max 170 characters)

Default

Accept Button Color

Customize Color

A2A2A2

(format : FFFFFFFF)

Preview

Default

Save and Next

Cancel

Available settings are explained as follows:

Item	Description
Welcome Message	Enter the text to be displayed as the welcome message.
Terms and Conditions Description	Enter the text to be displayed as the Terms and Conditions hyperlink text.
Terms and Conditions Content	Enter the text to be displayed in the Terms and Conditions pop-up window.
Accept Button Description	Enter the text to be displayed on the accept button
Accept Button Color	Select the color of the accept button from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.

Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

Social Login and PIN Login

This section describes the Login Page setup step if you have selected PIN Login and/or Social Login as the Login Mode. You will see only settings that are relevant to the selected login mode(s).



Configure Login Method and Details

- Welcome Message
- Terms and Conditions Description and Content
- Facebook Login
- Google Login
- Hint Message
- Receiving PIN via SMS Description
- Enter PIN and Submit Button

Welcome Message

Welcome!
We are pleased to provide free Wi-Fi to you!

(Max 1360 characters) Default

Terms and Conditions Description

By clicking the button below you agree to the Terms and Conditions.

(Max 170 characters) Default

Terms and Conditions Content

(Max 170 characters)

Settings that are common to Facebook, Google and PIN authentication are:

Item	Description
Welcome Message	Enter the text to be displayed as the welcome message.

Terms and Conditions Description	Enter the text to be displayed as the Terms and Conditions hyperlink text.
Terms and Conditions Content	Enter the text to be displayed in the Terms and Conditions pop-up window.

If you have selected Facebook login, these settings will appear:

Facebook Login Description (Max 170 characters)

Facebook APP ID

Facebook APP Secret

Item	Description
Facebook Login Description	Enter the text to be displayed on the Facebook login button.
Facebook APP ID	Enter a valid Facebook developer app ID. If you do not already have an app ID, refer to section A-1 <i>How to create a Facebook App ID for Web Portal Authentication</i> for instructions on obtaining an APP ID.
Facebook APP Secret	Enter the secret configured for the APP ID entered above. Refer to section A-1 <i>How to create a Facebook App ID for Web Portal Authentication</i> for details.

If you have selected Google login, these settings will appear:

Google Login Description (Max 170 characters)

Google App ID

Google App Secret

Item	Description
Google Login Description	Enter the text to be displayed on the Google login button.
Google App ID	Enter a valid Google app ID. If you do not already have an app ID, refer to section A-2 <i>How to create a Google App ID for Web Portal Authentication</i> for instructions on obtaining an APP ID.
Google App Secret	Enter the secret configured for the APP ID entered above. Refer to section A-2 <i>How to create a Google APP ID for Web Portal Authentication</i> for details.

If you have selected PIN login, these settings will appear:

Hint Message
(Max 170 characters)

Receiving PIN via SMS Description
(Max 170 characters)

Receiving PIN via SMS Content
(Max 150 characters)

Receiving PIN via SMS Provider Set SMS Provider in *Objects Setting >> SMS / Mail Service Object*

Enter PIN Description
(Max 170 characters)

Submit Button Description
(Max 170 characters)

Submit Button Color (format : FFFFFFFF)

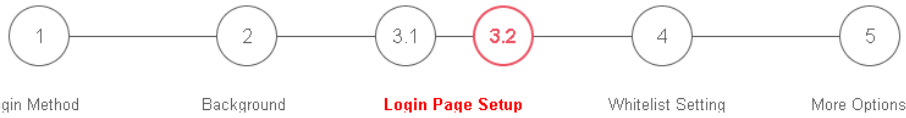
Item	Description
Hint Message	Enter the text used to suggest users to choose SMS authentication.
Receiving PIN via SMS Description	Enter the text to be displayed on the button that the user clicks to receive an SMS PIN.
Receiving PIN via SMS Content	Enter the message to be sent by SMS to inform the user of the PIN. The PIN variable is specified by <PIN> within the message.
Receiving PIN via SMS Provider	Select the SMS Provider used to send PIN notifications SMS providers are configured in Objects Setting >> SMS / Mail Service Object .
Enter PIN Description	Enter message to be displayed in the PIN textbox to prompt the user to enter the PIN.
Submit Button Description	Enter the text to be displayed on the submit PIN button
Submit Button Color	Select the color of the submit button from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.
Enter PIN Description	Enter message to be displayed in the PIN textbox to prompt the user to enter the PIN.

And finally, the save and cancel buttons are always displayed.

Item	Description
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

2nd-stage Page for PIN Login

If you have selected PIN Login as the login mode, you will also need to configure the page that is displayed to users when they request a PIN.



Configure 2nd-stage Page for SMS Login

< Back

PIN Code will be sent over via SMS.

+ 886 enter your mobile number

Send PIN

Enter PIN Submit

Back Button

PIN Code Message

Default Country Code, Enter Mobile Number Description

Send Button Description and Color

Send Succeeded Message

Enter PIN and Submit Button

Back Button Description

Back

(Max 170 characters) Default

PIN Code Message

PIN code will be sent over via SMS.

(Max 170 characters) Default

Default Country Code

+ 93 Afghanistan

Enter Mobile Number Description

enter your mobile number

(Max 170 characters) Default

Send Button Description

Send PIN

(Max 170 characters) Default

Send Button Color

Customize Color

A2A2A2 (format : FFFFFFFF) Preview Default

Send Succeeded Message

PIN Code has been sent.Click Send PIN again if not receiving PIN in 3 minutes.

(Max 170 characters) Default

Save and Next
Cancel

Available settings are explained as follows:

Item	Description
Back Button Description	Enter text for the label of the hyperlink to return to the previous page.
PIN Code Message	Enter text to be displayed as the body text on the page.
Default Country Code	Select the default country code to be displayed using the dropdown menu.

Enter Mobile Number Description	Enter message to be displayed in the mobile number textbox to prompt the user to enter the mobile number.
Send Button Description	Enter the label text of the send button.
Send Button Color	Select the color of the send button from the predefined color list, or select Customize Color and enter the RGB value. Click Preview to preview the selected color.
Send Succeeded Message	Enter text to be displayed to notify the user after the PIN has been sent.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

4. Whitelist Setting

In this step you can configure the whitelist settings. Users are allowed to send and receive traffic that satisfies whitelist settings.

Hotspot Web Portal >> Profile Setup



NAT Rules	Dest Domain	Dest IP	Dest Port	Source IP
Always allow outbound connections from hosts in		<input type="checkbox"/> NAT >> Port Redirection		
		<input type="checkbox"/> NAT >> Open Ports		
		<input type="checkbox"/> NAT >> DMZ		

Save and Next Cancel

Available settings are explained as follows:

Item	Description
NAT Rules	To prevent web portal settings from conflicting with NAT rules resulting in unexpected behavior, select the NAT rules that are allowed to bypass the web portal. Hosts listed in selected NAT rules can always access the Internet without being intercepted by the web portal.
Dest Domain	Enter up to 30 destination domains that are allowed to be accessed.
Dest IP	Enter up to 30 destination IP addresses that are allowed to be accessed.
Dest Port	Enter up to 30 destination protocols and ports that are allowed through the router.
Source IP	Enter up to 30 source IP addresses that are allowed through the router.

Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

5. More Options

In this step you can configure advanced options for the Hotspot Web Portal.

Hotspot Web Portal >> Profile Setup



Web Portal Options

Expired Time After Activation days hours min

HTTPS Redirection Enable

When an unauthenticated client opening a HTTPS page, redirect will work but certificate errors may be shown.
Disable this function to redirect only HTTP pages. HTTPS browsing will timeout without redirection and also no certificate errors.

Captive Portal Detection Enable

Trigger the unauthenticated client to automatically pop-up the Web Portal page when connects to Wi-Fi.
This function is not available when using **Social Login** because the page may not be shown correctly due to the limitation of the OS built-in Captive Portal Detection.

Landing Page After Authentication

Fixed URL

User Requested URL

Bulletin Message

(Max 511 characters)

Default Message

Note:

Landing Page may not be shown correctly when using OS built-in Captive Portal Detection.

Applied Interfaces

- Subnet LAN1 LAN2 LAN3 LAN4 LAN5 LAN6 LAN7 LAN8
- WLAN 2.4G SSID1 (DrayTek)
 SSID2 (DrayTek_Guest)
 SSID3
 SSID4
- 5G SSID1 (DrayTek_5G)
 SSID2 (DrayTek_5G_Guest)
 SSID3
 SSID4

Available settings are explained as follows:

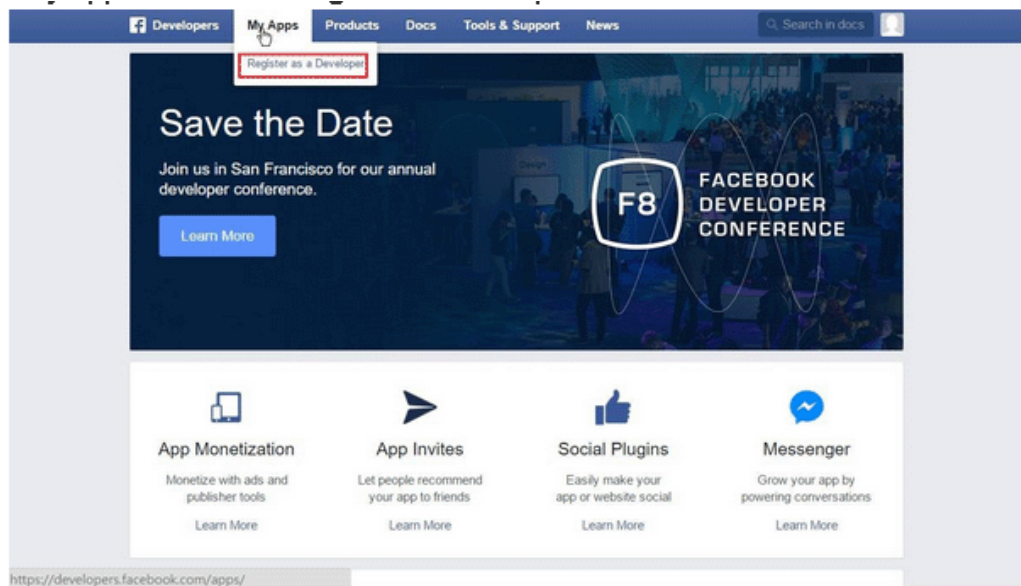
Item	Description
Expired Time After Activation	Enter the time duration that users are allowed to have Internet access after logging in.
HTTPS Redirection	If this option is selected, unauthenticated clients accessing HTTPS websites will be redirected to the login page, but the browser may alert the user of certificate errors. If this option is not selected, attempts to access to HTTPS website will time out without redirection.
Captive Portal Detection	If this option is selected, the web portal page is triggered automatically when an unauthenticated client tries to access the Internet. This function is not available when the Login Mode is Social Login , as the web portal page may not be shown correctly due to the limitations of the operating system's built-in Captive Portal Detection.
Landing Page After Authentication	Specifies the webpage that will be displayed after the user has successfully authenticated. Fixed URL - The user will be redirected to the specified URL. This could be used for displaying advertisements to users, such as guests requesting wireless Internet access in a hotel. User Requested URL - The user will be redirected to the URL they initially requested. Bulletin Message -The message configured here will be briefly shown for a few seconds to the user. Default Message - This button is enabled when Bulletin Message is selected. Click to load the default text into the bulletin message textbox.
Applied Interfaces	Subnet - The current Hotspot Web Portal profile will be in effect for the selected subnets. WLAN - The current Hotspot Web Portal profile will be in effect for the selected WLAN SSIDs.
Cancel	Click to abort the configuration process and return to the profile summary page.
Finish	Click to complete the configuration.

Application Notes

A-1 How to create Facebook APP for Web Portal Authentication?

The new web portal feature support social login as authentication method, and allows network administrator to authenticate LAN clients by their Google or Facebook account. This document introduces how to create Facebook APP, and generate the APP ID and APP secret that can be used in Web Portal setup.

1. Register as FB Developer: Go to <https://developers.facebook.com/> and login the FB account.
2. Register the Facebook account as a Developer (If the account has been verified previously, this step can be skipped.)
3. Click My Apps then choose Register as Developer.



4. Switch to YES then click Next on pop-up window.



5. Choose country then type phone number, click Send as Text in Get Confirmation Code. Wait confirmation code message received then enter the confirmation code. Click Register to finish the register process.

Register as a Facebook Developer ✕

We need to verify your account to complete your registration. Your Phone number will be added to your timeline but won't be visible to your friends.

Country: Taiwan (+886) Phone number: 0912345678

Get Confirmation Code

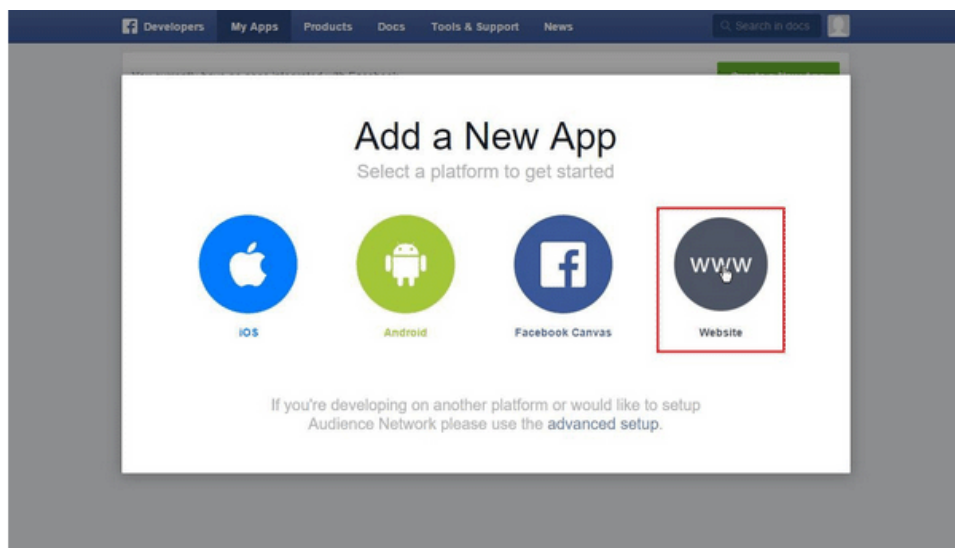
Send as Text Send via Phone Call

Confirmation code: 625535

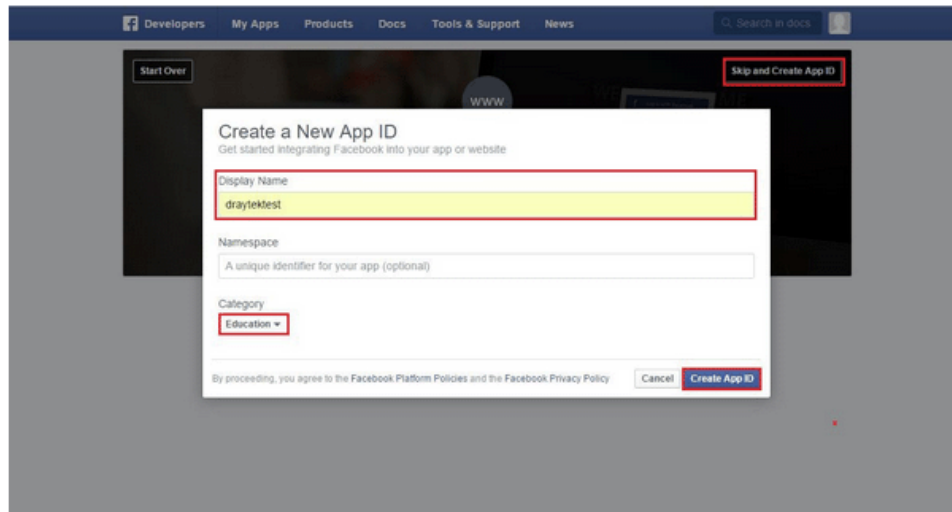
You can also verify your account by adding a credit card. [?]

Go Back Register

6. Add a New App. Click on My Apps > Add a New App. Choose Website platform.



7. Click Skip and Create App ID on first use. Type Display Name. Choose Category. Click Create App ID.



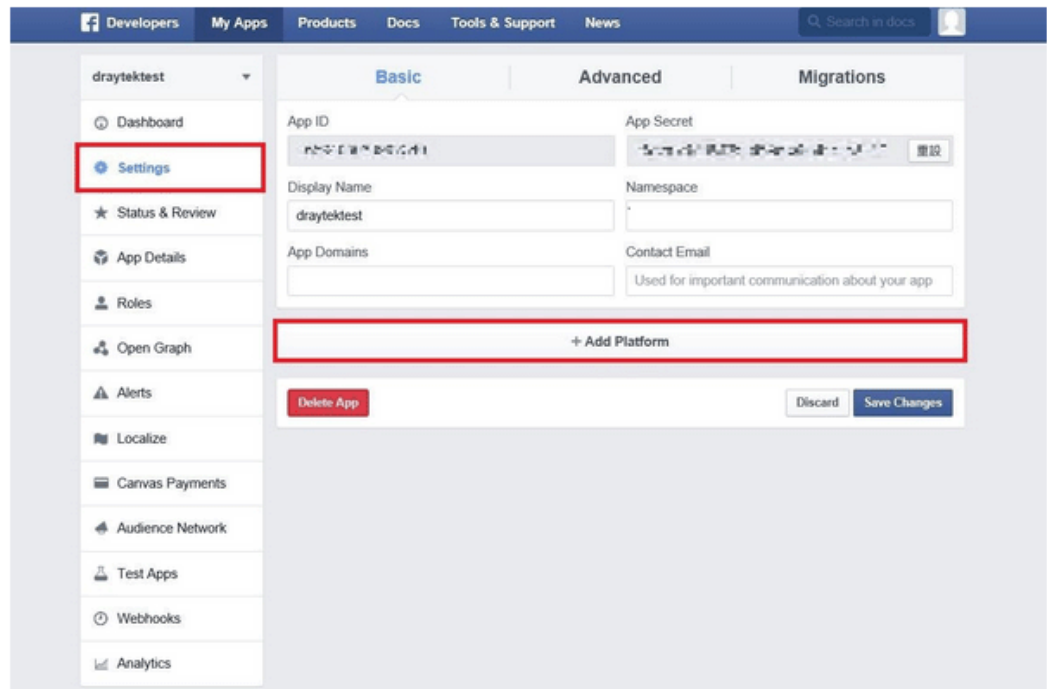
8. Pops up security check window, select the answer, and then click Submit to finish the process.



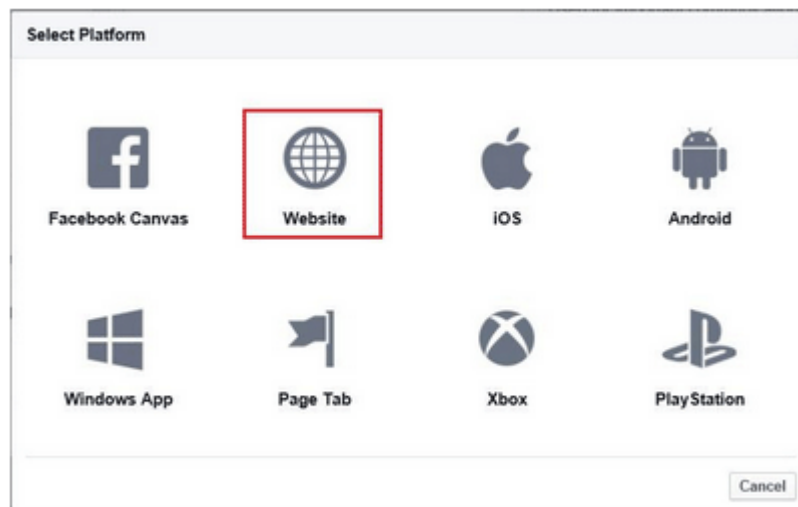
- On Dashboard, user can get **App ID** and **App Secret**, these information will be used in Vigor Router's Web Portal Setup.



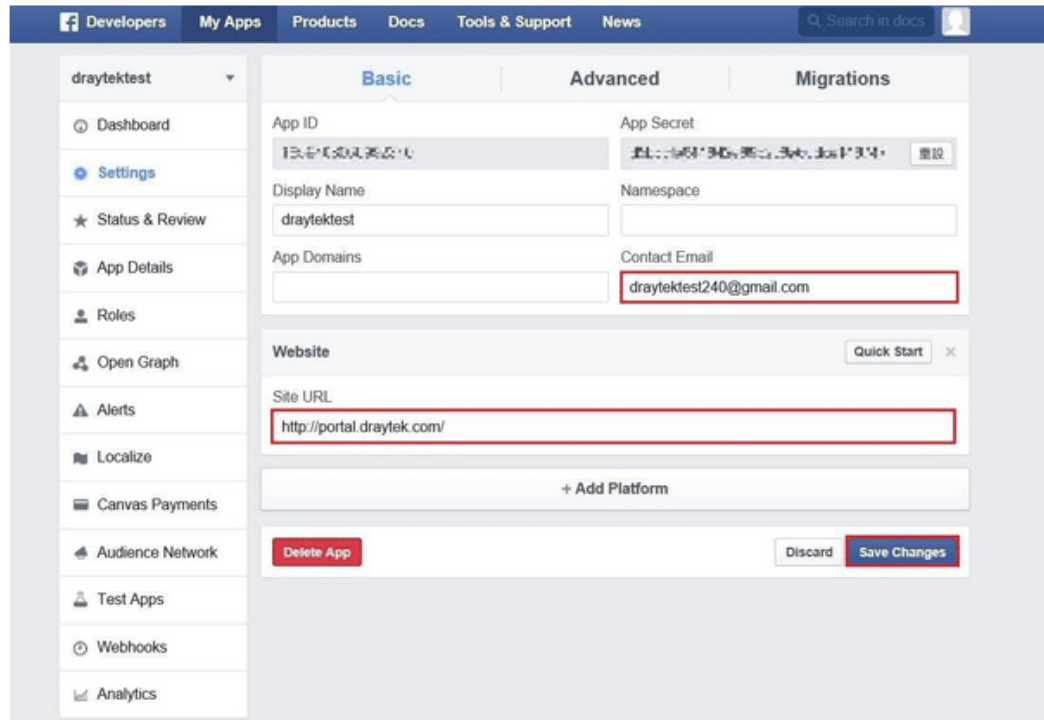
- Add Platform on My Apps. Go to Settings then click **Add Platform**.



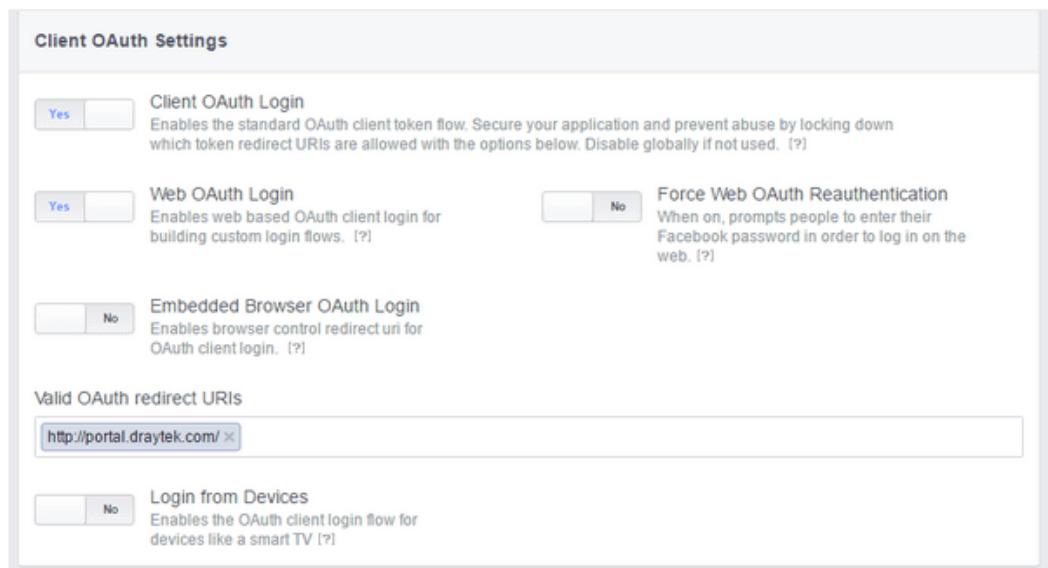
- Choose **Website** in Select Platform window.



- Enter the Site URL as <http://portal.draytek.com>. (Note: If you change http port in the vigor, please add http port in URLs. For example, we use 8080 as http port and we'll put <http://portal.draytek.com:8080>). Enter the Contact Email. And click Save Change.



13. Set up Client OAuth. Go to Settings >> Advanced >> Client OAuth Settings, enter "http://portal.draytek.com" in Valid OAuth redirect URIs, and save changes.



14. Go to My Apps >> Status & Review, and switch available status to YES to activate the APP.

Facebook Developers navigation bar: Developers, My Apps, Products, Docs, Tools & Support, News. Search in docs.

Left sidebar for 'draytektest': Dashboard, Settings, **Status & Review**, App Details, Roles, Open Graph, Alerts, Localize, Carvas Payments, Audience Network.

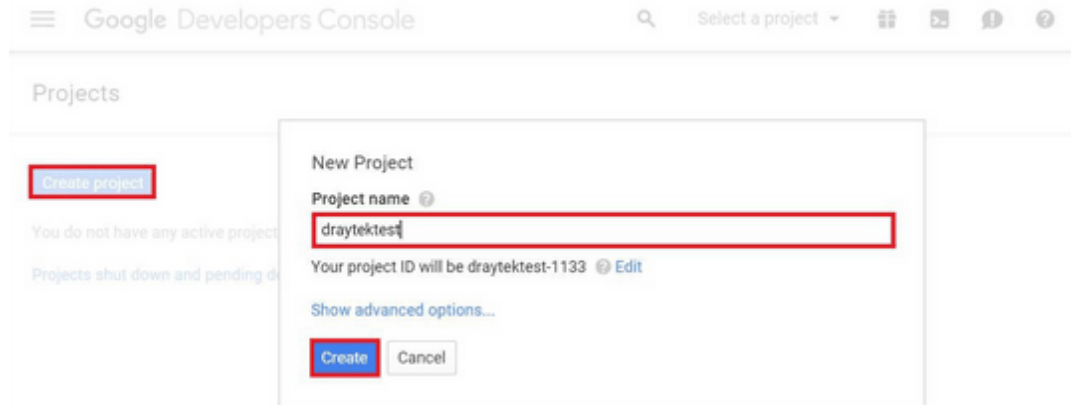
Main content area:

- Status** | **Items in Review**
- draytektest logo and name.
- Question: "Do you want to make this app and all its live features available to the general public?" with a **YES** button.
- Submit Items for Approval** section with a "Start a Submission" button and a note about Facebook integrations requiring approval.
- Approved Items** section with a "(?)" icon.
- LOGIN PERMISSIONS** section.

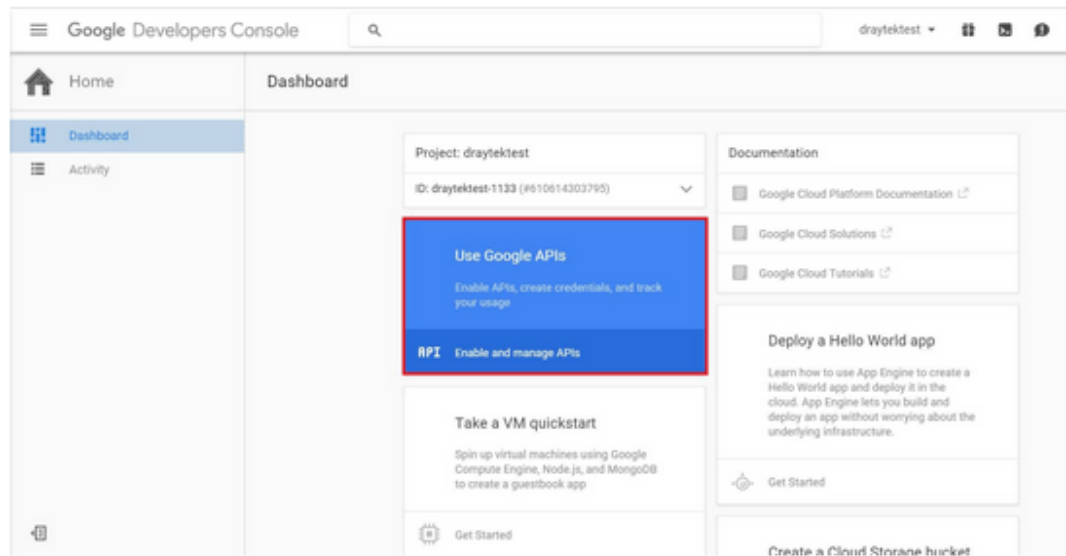
A-2 How to create Google APP for Web Portal Authentication?

The new web portal feature support social login as authentication method, and allows network administrator to authenticate LAN clients by their Google or Facebook account. This document introduces how to create Facebook APP, and generate the APP ID and APP secret that can be used in Web Portal setup.

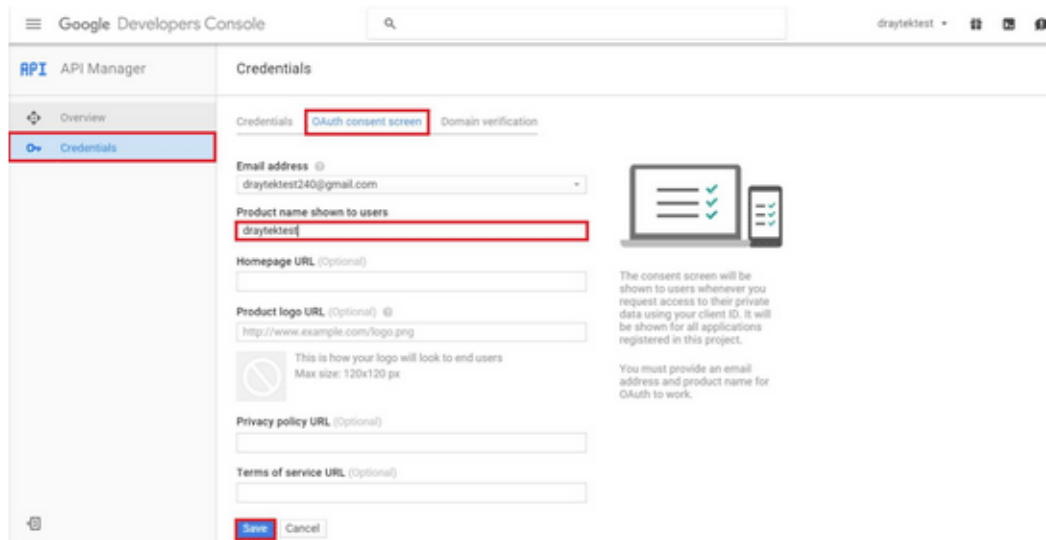
1. Create Developer project. Go to <https://code.google.com/apis/console>, login with a Google account then click Create project. Type project name then click Create.



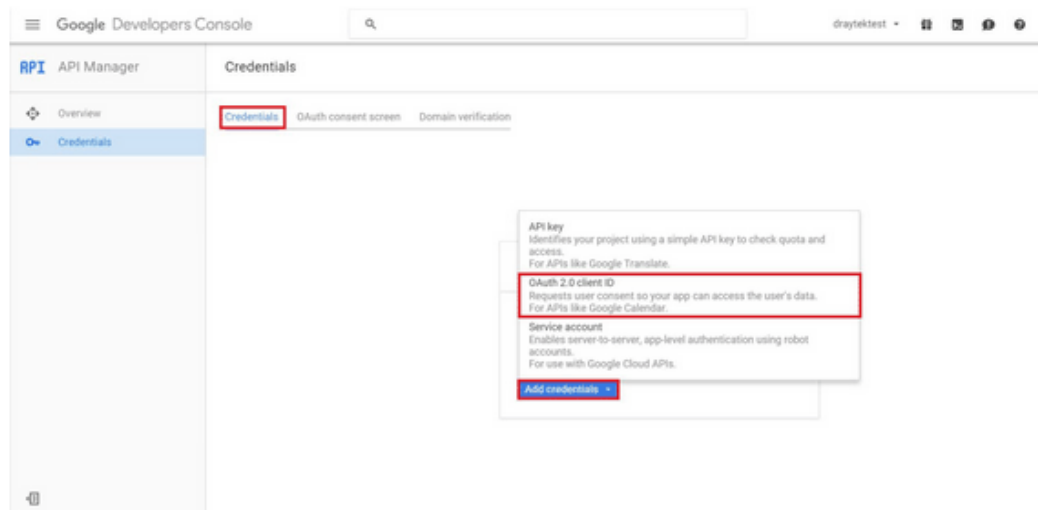
2. On Dashboard, choose Use Google APIs.



3. Edit Auth Consent screen. Go to Credentials > Auth consent screen. Enter your email, product name and other optional item then click on Save.



4. Create Client ID. Click Credentials and Click Add credentials > OAuth2.0 client ID.



5. Choose **Web application** as Application Type, then enter **name**. Set **Authorized JavaScript origins** and **Authorized redirect URLs** as `http://portal.draytek.com`, and click **Create**. (*Note: If you change http port in the vigor, please add http port in URLs. For example, we use 8080 as http port and we'll put `http://portal.draytek.com:8080`*).
6. Get client ID and client secret. Such information will be used in Vigor Router's Web Portal Setup page.



VI-4 Central Management (AP)

Vigor2133 can manage the access points supporting AP management via Central AP Management.

AP Map

AP Map is helpful to determine the best location for VigorAP in a room. A floor plan of a room is required to be uploaded first. By dragging and dropping available VigorAP icon from the list to the floor plan, the placement with the best wireless coverage will be clearly indicated through simulated signal strength

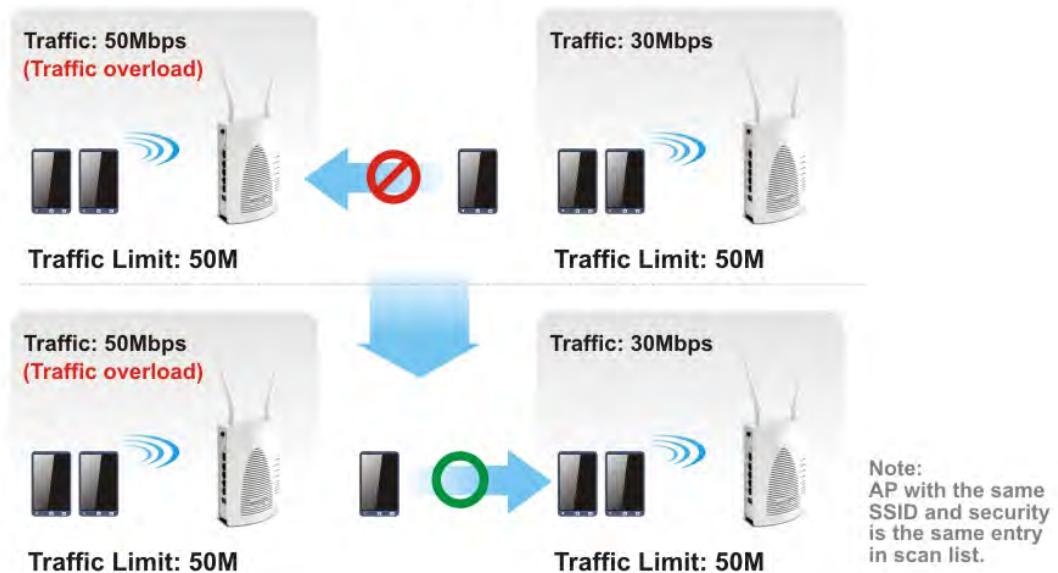
AP Maintenance

Vigor router can execute configuration backup, configuration restoration, firmware upgrade and remote reboot for the APs managed by the router. It is very convenient for the administrator to process maintenance without accessing into the web user interface of the access point.

Load Balance for AP

The parameters configured for Load Balance can help to distribute the traffic for all of the access points registered to Vigor router. Thus, the bandwidth will not be occupied by certain access points.

AP Load Balance (Traffic overload)



Web User Interface



VI-4-1 Status

This page displays current status (online, offline or SSID hidden, IP address, encryption, channel, version, password and etc.) of the access points managed by Vigor router. Please open Central AP Management>>Function Support List to check what AP Models are supported.

Central Management >> AP >> Status

Index	Device Name	IP Address	SSID	Ch.	STA List	AP List	Uptime	Ver.	Password
-------	-------------	------------	------	-----	----------	---------	--------	------	----------

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

Note:

 : Online  : Offline  : Hidden SSID

Maximum support 2 APs.

When AP Devices connect via an intermediary switch, please ensure that **UDP:4944** port and the **HTTP** port of AP Devices are not blocked so that the AP status can be retrieved.

Available settings are explained as follows:

Item	Description
Index	Click the index number link for viewing the settings summary of the access point.
Device Name	The name of the AP managed by Vigor router will be displayed here.
IP Address	Display the true IP address of the access point.
SSID	Display the SSID configured for the access point(s) connected to Vigor2133.
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	Vigor2133 can get related information of the access point by accessing into the web user interface of the access point. This button is used to modify the logging password of the connected access point.

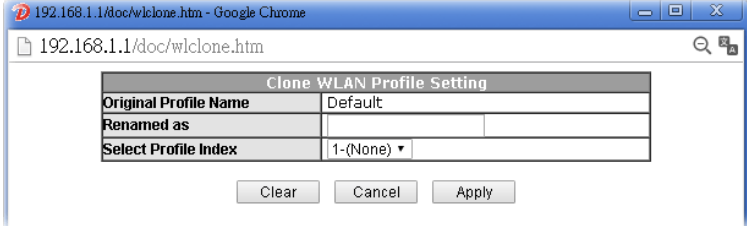
VI-4-2 WLAN Profile

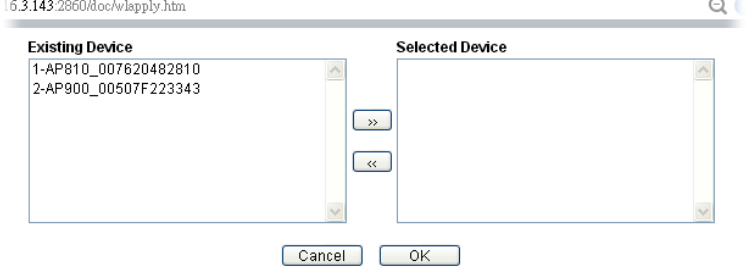
WLAN profile is used to apply to a selected access point. It is very convenient for the administrator to configure the setting for access point without opening the web user interface of the access point.

Central Management >> AP >> WLAN Profile

Profile	Name	Main SSID	Security	Multi-SSID	WLAN ACL	Rate Ctrl	Clone	To AP	To Local
1	Default	DrayTek-LAN-A	WPA+WPA2/PSK	Enable	None	None			
2	---	---	---	---	---	---	---	---	---
3	---	---	---	---	---	---	---	---	---
4	---	---	---	---	---	---	---	---	---
5	---	---	---	---	---	---	---	---	---

Click the number link of the selected profile to modify the content of the profile. Available settings are explained as follows:

Item	Description
Profile	There are five WLAN profiles offered to be configured. Simply click the index number link to open the modification page.
Name	Display the name of the profile. The default profile cannot be renamed.
Main SSID	Display the SSID configured by such wireless profile.
Security	Display the security mode selected by such wireless profile.
Multi-SSID	Enable means multiple SSIDs (more than one) are active. Disable means only SSID1 is active.
WLAN ACL	Display the name of the access control list.
Rate Ctrl	Display the upload and/or download transmission rate.
Clone	<p>It can copy settings from an existing WLAN profile to another WLAN profile.</p> <p>First, you have to check the box of the existing profile as the original profile. Second, click Clone. The following dialog will appear.</p>  <p>Third, choose the profile index to accept the settings from the original profile. Forth, type a new name in the field of Renamed as. Last, click Apply to save the settings on this dialog.</p> <p>The new profile has been created with the settings coming from the original profile.</p>
To AP	Click it to apply the selected wireless profile to the specified Access Point.

	 <p>Simply choose the device you want from Existing Device field. Click >> to move the device to Selected Device field. Then, click OK.</p> <p>The selected WLAN profile will be applied to the selected access point immediately. Later the access point will reboot.</p>
<p>To Local</p>	<p>WLAN Profile configured in this page is specified for VigorAP connected to Vigor router.</p> <p>If required, these settings also can be applied to Vigor router. Select and check one of wireless profiles and click this button to apply the settings onto the WI-Fi wireless settings configured for such Vigor router.</p>

How to edit the wireless LAN profile?

1. Select the WLAN profile (index number 1 to 5) you want to edit.
2. Click the index number link to display the following page.

Central Management >> AP >> WLAN Profile

WLAN Profile Edit

Device Settings	
Profile Name	Default <input type="checkbox"/> Auto Provision
Administrator	admin
Password	****
2nd Subnet	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

2.4G WLAN General Settings	
Wireless LAN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Limit Client	<input type="checkbox"/> Enable <input type="text" value="64"/> (3 ~ 128) (Default: 64)
Operation Mode	AP
2.4G Mode	Mixed(11b+11g+11n)
2.4G Channel	2462MHz (Channel 11)
Airtime Fairness	<input type="checkbox"/> Enable Airtime Fairness: Triggering Client Number <input type="text" value="2"/> (2 ~ 128) (Default: 2)
Band Steering	<input type="checkbox"/> Enable Band Steering: Check Time for WLAN Client 5G Cap. <input type="text" value="15"/> sec(s) (1 ~ 60) (Default: 15)
Roaming	<input type="checkbox"/> Minimum Basic Rate <input type="text" value="1"/> Mbps
	<input checked="" type="radio"/> Disable RSSI Requirement
	<input type="radio"/> Strictly Minimum RSSI - <input type="text" value="73"/> dbm (<input type="text" value="42"/> %) (Default: -73)
	<input type="radio"/> Minimum RSSI - <input type="text" value="66"/> dbm (<input type="text" value="60"/> %) (Default: -66) with Adjacent AP RSSI over <input type="text" value="5"/> dB (Default: 5)



Info

The function of Auto Provision is available for the default WLAN profile.

- After finished the general settings configuration, click **Next** to open the following page for 2.4G wireless security settings.

Central Management >> AP >> WLAN Profile

SSID1	SSID2	SSID3	SSID4
2.4G SSID			
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
SSID	DrayTek-LAN-A	LAN-A ▾	<input type="checkbox"/> Hide SSID
VLAN	0 (0:untag)		
Isolate	<input type="checkbox"/> From Member		
Security Settings			
Encryption	WPA+WPA2/PSK ▾		
	Set up RADIUS Server if 802.1X is enabled.		
	WPA		
	WPA Algorithms	<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES	
	Pass Phrase	*****	
Key Renewal Interval	3600	Seconds	
WEP	Setup WEP Key if WEP is enabled.		
	802.1X WEP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Access Control			
Mode	None ▾		
List			
	Client's MAC Address : [] : [] : [] : [] : []		
	<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/>		
Bandwidth Limit			
Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		Auto Adjustment <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Upload	0 Kbps	Download	0 Kbps
<input type="button" value="Back"/> <input type="button" value="Cancel"/> <input type="button" value="Next"/>			
Backup ACL Cfg : <input type="button" value="Backup"/>		Upload From File: <input type="button" value="選擇檔案"/> 未選擇任何檔案 <input type="button" value="Restore"/>	

- After finished the above web page configuration, click **Next** to open the following page for 5G wireless security settings.

Central Management >> AP >> WLAN Profile

5G SSID1	5G SSID2	5G SSID3	5G SSID4
5G SSID			
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
SSID	DrayTek-5G	LAN-A ▾	<input type="checkbox"/> Hide SSID
VLAN	0 (0:untag)		
Isolate	<input type="checkbox"/> From Member		
Security Settings			
	Disable ▾		
	Set up RADIUS Server if 802.1X is enabled.		
Encryption	WPA		
	WPA Algorithms	<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES	
	Pass Phrase	<input type="text"/>	
	Key Renewal Interval	3600	Seconds
	WEP		
	Setup WEP Key if WEP is enabled.		
	802.1X WEP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Access Control			
Mode	None ▾		
List	<div style="border: 1px solid gray; height: 40px;"></div>		
	Client's MAC Address : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>		
	<input type="button" value="Add"/>	<input type="button" value="Delete"/>	<input type="button" value="Edit"/> <input type="button" value="Cancel"/>
Bandwidth Limit			
Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		Auto Adjustment <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Upload	0	Kbps	Download 0 Kbps

Note:

5G SSID Configuration only work with VigorAP800 v1.1.1 and newer APM Client.

Backup ACL Cfg : <input type="button" value="Backup"/>	Upload From File: <input type="button" value="選擇檔案"/> 未選擇任何檔案	<input type="button" value="Restore"/>
--	---	--

- When you finished the above web page configuration, click **Finish** to exit and return to the first page. The modified WLAN profile will be shown on the web page.

Central Management >> AP >> WLAN Profile

										Set to Factory Default
Profile	Name	Main SSID	Security	Multi-SSID	WLAN ACL	Rate Ctrl	Clone	To AP	To Local	
1	Default	DrayTek-LAN-A	WPA+WPA2/PSK	Enable	None	None				
2	123	DrayTek	Disable	Disable	None	None				
3	---	---	---	---	---	---	---	---	---	---
4	---	---	---	---	---	---	---	---	---	---
5	---	---	---	---	---	---	---	---	---	---

VI-4-3 AP Maintenance

Vigor router can execute configuration backup, configuration restoration, firmware upgrade and remote reboot for the APs managed by the router. It is very convenient for the administrator to process maintenance without accessing into the web user interface of the access point.



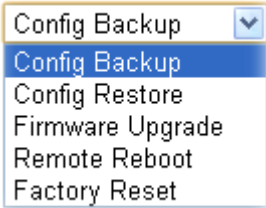
Info

Config Backup can be performed to one AP at one time. Others functions (e.g., Config Restore, Firmware Upgrade, Remote Reboot) can be performed to more than one AP at one time by using Vigor2133.

Central Management >> AP >> AP Maintenance

AP Maintenance

Available settings are explained as follows:

Item	Description
Action	<p>There are four actions provided by Vigor router to manage the access points.</p>  <p>Vigor router can backup the configuration of the selected AP, restore the configuration for the selected AP, perform the firmware upgrade of the selected AP, reboot the selected AP remotely and perform the factory reset for the selected AP.</p>
File/Path	Specify the file and the path which will be used to perform Config Restore or Firmware Upgrade .
Select Device	Display all the available access points managed by Vigor router. Simply click << or >> to move the device(s) between

	Select Device and Selected Device areas.
Selected Device	Display the access points that will be applied by such function after clicking OK.

After finishing all the settings here, please click **OK** to perform the action.

VI-4-4 Traffic Graph

Click **Traffic Graph** to open the web page. Choose one of the managed Access Points, LAN-A or LAN-B, daily or weekly for viewing data transmission chart. Click **Refresh** to renew the graph at any time.

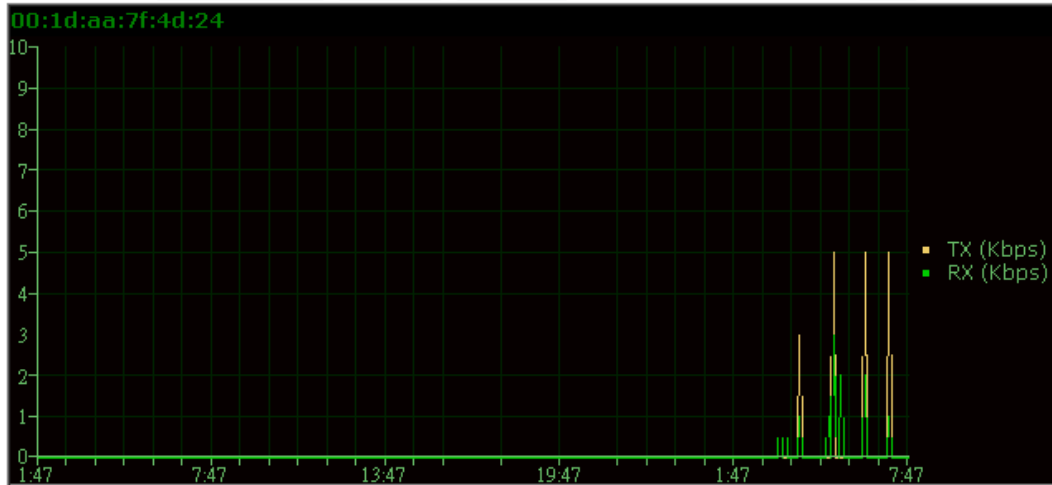
Central Management >> AP >> Traffic Graph

Enable

Show Chart: VigorAP910C LAN-A Daily

Refresh Min(s): 1

Refresh



Note:

Enabling/Disabling AP Traffic Graph will also Enable/Disable the External Devices Function.

The horizontal axis represents time; the vertical axis represents the transmission rate (in kbps).



Info

Enabling/Disabling such function will also enable/disable the External Devices function.

VI-4-5 Load Balance

The parameters configured for Load Balance can help to distribute the traffic for all of the access points registered to Vigor router. Thus, the bandwidth will not be occupied by certain access points.

Central Management >> AP >> Load Balance

AP Load Balance By Station Number or Traffic ▾

Station Number Threshold

Wireless LAN (2.4GHz) (3-64)
 Wireless LAN (5GHz) (3-64)

Traffic Threshold

Upload Limit bps (Default unit: K)
 Download Limit bps (Default unit: K)

Action When Threshold Exceeded

Stop accepting new connections
 Dissociate existing station by longest idle time
 Dissociate existing station by worst signal strength if it is less than dBm (%)

Note:

The maximum station number of Wireless LAN (2.4GHz) will be applied to both Wireless LAN (2.4GHz) and Wireless LAN (5GHz) if the firmware version of AP900 is less than or equal to 1.1.4.1.

Available settings are explained as follows:

Item	Description
AP Load Balance	It is used to determine the operation mode when the system detects overload between access points. Disable - Disable the function of AP load balance. 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

	<p>web page, Vigor router will stop any new connection asked by other access point.</p> <p>Dissociate existing station by longest idel time - When the access point is overload (e.g., reaching the limit of station number or limit of network traffic), it will terminate the network connection of the client's station which is idle for a longest time.</p> <p>Dissociate existing station by worst signal strength if it is less than - When the access point is overload (e.g., reaching the limit of station number or limit of network traffic), it will terminate the network connection of the client's station with the weakest signal.</p>
--	---

After finishin0g all the settings here, please click OK to save the configuration.

VI-4-6 Function Support List

Click the **Client** tab to list the AP management functions that the Access Points support under different firmware versions.

Click the **Server** tab to list the AP management functions that Vigor router supports under different firmware versions.

Central AP Management >> Function Support List

Model Name	AP710	AP800	AP810	AP900	AP902	AP910C
FW Version	1.2.0	1.1.6	1.1.6.1	1.1.7	1.1.7	1.1.6
Register						
DHCP	•	•	•	•	•	•
Static IP	•	•	•	•	•	•
Profile						
2.4GHz	•	•	•	•	•	•
5GHz		• (with N65)		•	•	•
AP Mode	•	•	•	•	•	•
Auto Provision	•	•	•	•	•	•
WLAN Enable/Disable	•	•	•	•	•	•
Limit Client	•		•	•	•	•
Airtime Fairness	•		•	•	•	•
Band Steering				•	•	•
Fast Roaming	•		•	•	•	•
Access Control List	•	•	•	•	•	•
Bandwidth Limit	•	•	•	•	•	•
Centralized AP Management						
AP Maintenance	•		•	•	•	•
AP Map	•		•	•	•	•
Traffic Graph	•	•	•	•	•	•
Rogue AP Detection	•		•	•	•	•
Event Log	•		•	•	•	•
Total Traffic	•		•	•	•	•
Station Number	•		•	•	•	•
Load Balance	•		•	•	•	•

VI-5 Central Management (External Devices)

Vigor router can be used to connect with many types of external devices. In order to control or manage the external devices conveniently, open **External Devices** to make detailed configuration.

VI-5-1 All Devices

External Device >> All Devices

- External Device Syslog
- External Device Auto Discovery

External Devices Connected

| **Refresh** |

Below shows available devices that connected externally:

On Line VigorAP900, VigorAP900, Connection Uptime:02:05:36 IP Address: 192.168.1.11	<input type="button" value="Account"/>	<input type="button" value="Clear"/>
---	--	--------------------------------------

For security reason:

If you have changed the administrator password on External Device, please click the **Account** button to retype new username and password. Otherwise, the router will be unable to monitor the External Device device properly. Click the **Clear** button to Clear the off-line information and account information.

Available settings are explained as follows:

Item	Description
External Device Syslog	Check this box to display information of the detected device on Syslog.
External Device Auto Discovery	Check this box to detect the external device automatically and display on this page.

From this web page, check the box of **External Device Auto Discovery**. Later, all the available devices will be displayed in this page with icons and corresponding information. You can change the device name if required or remove the information for off-line device whenever you want.

External Device >> All Devices

- External Device Syslog
- External Device Auto Discovery

External Devices Connected

Below shows available devices that connected externally:

On Line VigorAP900, VigorAP900, Connection Uptime:18:15:27 IP Address: 10.28.60.12	<input type="button" value="Account"/>	<input type="button" value="Clear"/>
On Line P2261, Connection Uptime:18:15:17 IP Address: 192.168.1.226	<input type="button" value="Account"/>	<input type="button" value="Clear"/>

For security reason:

If you have changed the administrator password on External Device, please click the **Account** button to retype new username and password. Otherwise, the router will be unable to monitor the External Device device properly. Click the **Clear** button to Clear the off-line information and account information.

When you finished the configuration, click **OK** to save it.



Info

Only DrayTek products can be detected by this function.

This page is left blank.

Part VII Others



Objects Settings



USB

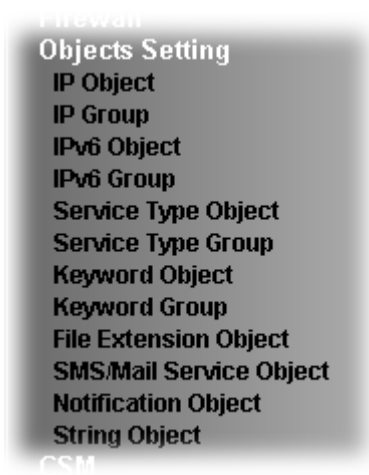
Define objects such as IP address, service type, keyword, file extension and others. These pre-defined objects can be applied in CSM.

USB device connected on Vigor router can be regarded as a server or WAN interface. By way of Vigor router, clients on LAN can access, write and read data stored in USB storage disk with different applications.

VII-1 Objects Settings

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

Web User Interface



VII-1-1 IP Object

For IPs in a range and service ports in a limited range usually will be applied in configuring router's settings, therefore we can define them with *objects* and bind them with *groups* for using conveniently. Later, we can select that object/group that can apply it. For example, all the IPs in the same department can be defined with an IP object (a range of IP address).

You can set up to 192 sets of IP Objects with different conditions.

Objects Setting >> IP Object

[Create from ARP Table](#)
[Create from Routing Table](#)

IP Object Profiles:

[Set to Factory Default](#)

View:

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

<< [1-32](#) | [33-64](#) | [65-96](#) | [97-128](#) | [129-160](#) | [161-192](#) >>

[Next](#) >>

<p>Export IP Object</p> <ul style="list-style-type: none"> <input checked="" type="radio"/> Backup the current IP Objects with a CSV file <input type="radio"/> Download the default CSV template to edit <input type="button" value="Download"/>	<p>Restore IP Object</p> <p><input type="button" value="選擇檔案"/> 未選擇任何檔案</p> <input type="button" value="Restore"/>
--	---

Note:
 For better compatibility, it's suggested to edit IP Objets with the provided default CSV template.

Available settings are explained as follows:

Item	Description
View	Use the drop down list to choose a type (Single Address, Range Address, Subnet Address, Mac Address or all) that IP object with the selected type will be shown on this page.
Set to Factory Default	Clear all profiles.
Search	Type a string of the IP object that you want to search.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.
Address	Display the IP address configured for the object profile.

Export IP Object	<p>Usually, the IP objects can be created one by one through the web page of Objects>>IP Object. However, to a user who wants to save more time in bulk creating IP objects, a quick method is offered by Vigor router to modify the IP objects with a single file, a CSV file.</p> <p>All of the IP objects (or the template) can be exported as a file by clicking Download. Then the user can open the CSV file through Microsoft Excel and modify all the IP objects at the same time.</p> <p>Backup the current IP Objects with a CSV file - Click it to backup current IP objects as a CSV file. Such file can be restored for future use.</p> <p>Download the default CSV template to edit - After clicking it, press Download to store the default CSM template (a table without any input data) to your hard disk.</p> <p>Download - Download the CSV file from Vigor router and store in your hard disk.</p>
Restore IP Object	<p>Select - Click it to specify a predefined CSV file.</p> <p>Restore - Import the selected CSV file onto Vigor router.</p>

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

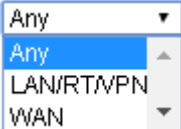
1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:

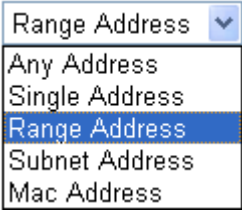
Objects Setting >> IP Object

Profile Index : 1

Name:	RD Department
Interface:	Any
Address Type:	Range Address
Mac Address:	00 : 00 : 00 : 00 : 00 : 00
Start IP Address:	192.168.1.59 <input type="button" value="Select"/>
End IP Address:	192.168.1.65 <input type="button" value="Select"/>
Subnet Mask:	
Invert Selection:	<input type="checkbox"/>

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Interface	<p>Choose a proper interface.</p>  <p>For example, the Direction setting in Edit Filter Rule will ask you specify IP or IP range for WAN or LAN/DMZ/RT/VPN or any IP address. If you choose LAN/DMZ/RT/VPN as the Interface here, and choose LAN/DMZ/RT/VPN as the direction setting in Edit Filter Rule, then all the IP addresses specified with LAN/DMZ/RT/VPN interface will be opened for you to choose in Edit Filter Rule page.</p>

Address Type	<p>Determine the address type for the IP address. Select Single Address if this object contains one IP address only. Select Range Address if this object contains several IPs within a range. Select Subnet Address if this object contains one subnet for IP address. Select Any Address if this object contains any IP address. Select Mac Address if this object contains Mac address.</p> 
MAC Address	Type the MAC address of the network card which will be controlled.
Start IP Address	Type the start IP address for Single Address type.
End IP Address	Type the end IP address if the Range Address type is selected.
Subnet Mask	Type the subnet mask if the Subnet Address type is selected.
Invert Selection	If it is checked, all the IP addresses except the ones listed above will be applied later while it is chosen.

- After finishing all the settings here, please click OK to save the configuration. Below is an example of IP objects settings.

Objects Setting >> IP Object

IP Object Profiles:

Index	Name	Index
<u>1.</u>	RD Department	<u>17.</u>
<u>2.</u>	Financial Dept	<u>18.</u>
<u>3.</u>	HR Department	<u>19.</u>
<u>4.</u>		<u>20.</u>
<u>5.</u>		<u>21.</u>
6.		22.

VII-1-2 IP Group

This page allows you to bind several IP objects into one IP group.

Objects Setting >> IP Group

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

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

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.

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

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:

Objects Setting >> IP Group

Profile Index : 1

Name:

Interface:

Available IP Objects

- 1-RD Department
- 2-Financial Dept
- 3-HR Department

>>

<<

Selected IP Objects

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Interface	Choose WAN, LAN or Any to display all the available IP objects with the specified interface.
Available IP Objects	All the available IP objects with the specified interface chosen above will be shown in this box.
Selected IP Objects	Click >> button to add the selected IP objects in this box.

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

VII-1-3 IPv6 Object

You can set up to 64 sets of IPv6 Objects with different conditions.

Objects Setting >> IPv6 Object

IPv6 Object Profiles: | [Set to Factory Default](#) |

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

<< [1-32](#) | [33-64](#) >> [Next](#) >>

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.

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

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:

Objects Setting >> IPv6 Object

Profile Index : 1

Name:	<input type="text"/>
Address Type:	Subnet Address ▾
Mac Address:	00 : 00 : 00 : 00 : 00 : 00
Start IP Address:	<input type="text"/> <input type="button" value="Select"/>
End IP Address:	<input type="text"/> <input type="button" value="Select"/>
Prefix Length:	<input type="text" value="0"/>
Invert Selection:	<input type="checkbox"/>

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Address Type	Determine the address type for the IPv6 address. Select Single Address if this object contains one IPv6 address only. Select Range Address if this object contains several IPv6s within a range. Select Subnet Address if this object contains one subnet for IPv6 address. Select Any Address if this object contains any IPv6 address. Select Mac Address if this object contains Mac address.
Mac Address	Type the MAC address of the network card which will be controlled.
Start IP Address	Type the start IP address for Single Address type.
End IP Address	Type the end IP address if the Range Address type is selected.
Prefix Length	Type the number (e.g., 64) for the prefix length of IPv6 address.
Invert Selection	If it is checked, all the IPv6 addresses except the ones listed above will be applied later while it is chosen.

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

VII-1-4 IPv6 Group

This page allows you to bind several IPv6 objects into one IPv6 group.

Objects Setting >> IPv6 Group

IPv6 Group Table:

[Set to Factory Default](#)

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

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.

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

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:

Objects Setting >> IPv6 Group

Profile Index : 1

Name:

Available IPv6 Objects

>>

<<

Selected IPv6 Objects

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Available IPv6 Objects	All the available IPv6 objects with the specified interface chosen above will be shown in this box.
Selected IPv6 Objects	Click >> button to add the selected IPv6 objects in this box.

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

VII-1-5 Service Type Object

You can set up to 96 sets of Service Type Objects with different conditions.

Objects Setting >> Service Type Object

Service Type Object Profiles: | [Set to Factory Default](#) |

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

<< [1-32](#) | [33-64](#) | [65-96](#) >> [Next](#) >>

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.

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

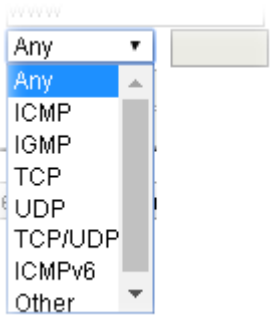
1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:

Objects Setting >> Service Type Object Setup

Profile Index : 1

Name	www
Protocol	Any
Source Port	= 1 ~ 65535
Destination Port	= 1 ~ 65535

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Protocol	Specify the protocol(s) which this profile will apply to. 
Source/Destination Port	<p>Source Port and the Destination Port columns are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number.</p> <p>(=) - when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this profile.</p> <p>(!=) - when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.</p> <p>(>) - the port number greater than this value is available.</p> <p>(<) - the port number less than this value is available for this profile.</p>

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

Objects Setting >> Service Type Object

Service Type Object Profiles:

Index	Name	Index
<u>1.</u>	www	<u>17.</u>
<u>2.</u>	SIP	<u>18.</u>
<u>3.</u>		<u>19.</u>
<u>4.</u>		<u>20.</u>

VII-1-6 Service Type Group

This page allows you to bind several service types into one group.

Objects Setting >> Service Type Group

Service Type Group Table:

| [Set to Factory Default](#) |

Group	Name	Group	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.

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

1. Click the number (e.g., #1) under Group column for configuration in details.
2. The configuration page will be shown as follows:

Objects Setting >> Service Type Group Setup

Profile Index : 1

Name:

Available Service Type Objects

- 1-www
- 2-SIP

Selected Service Type Objects

>> <<

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Available Service Type Objects	All the available service objects that you have added on Objects Setting>>Service Type Object will be shown in this box.
Selected Service Type Objects	Click >> button to add the selected IP objects in this box.

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

VII-1-7 Keyword Object

You can set 200 keyword object profiles for choosing as black /white list in CSM >>URL Web Content Filter Profile.

Objects Setting >> Keyword Object

Keyword Object Profiles: | [Set to Factory Default](#) |

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

<< [1-32](#) | [33-64](#) | [65-96](#) | [97-128](#) | [129-160](#) | [161-192](#) | [193-200](#) >> [Next](#) >>

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.

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

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:

Objects Setting >> Keyword Object Setup

Profile Index : 1

Name	<input type="text"/>
Contents	<input type="text"/>
Limit of Contents: Max 3 Words and 63 Characters. Each word should be separated by a single space.	
You can replace a character with %HEX. Example: Contents: backdoo%72 virus keep%20out	
Result: 1. backdoor 2. virus 3. keep out	

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile, e.g., game. Maximum 15 characters are allowed.
Contents	Type the content for such profile. For example, type <i>gambling</i> as Contents. When you browse the webpage, the page with gambling information will be watched out and be passed/blocked based on the configuration on Firewall settings.

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

VII-1-8 Keyword Group

This page allows you to bind several keyword objects into one group. The keyword groups set here will be chosen as black /white list in CSM >>URL /Web Content Filter Profile.

Objects Setting >> Keyword Group

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

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

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.

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

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:

Objects Setting >> Keyword Group Setup

Profile Index : 1

Name:

Available Keyword Objects	Selected Keyword Objects(Max 16 Objects)
1-Key-1 2-Key-2	

Available settings are explained as follows:

Item	Description
Name	Type a name for this group. Maximum 15 characters are allowed.
Available Keyword Objects	You can gather keyword objects from Keyword Object page within one keyword group. All the available Keyword objects that you have created will be shown in this box.
Selected Keyword Objects	Click <input type="button" value=">>"/> button to add the selected Keyword objects in this box.

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

VII-1-9 File Extension Object

This page allows you to set eight profiles which will be applied in **CSM>>URL Content Filter**. All the files with the extension names specified in these profiles will be processed according to the chosen action.

Objects Setting >> File Extension Object

File Extension Object Profiles: | [Set to Factory Default](#) |

Profile	Name	Profile	Name
<u>1.</u>		<u>5.</u>	
<u>2.</u>		<u>6.</u>	
<u>3.</u>		<u>7.</u>	
<u>4.</u>		<u>8.</u>	

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.

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

1. Click the number (e.g., #1) under Profile column for configuration in details.
2. The configuration page will be shown as follows:

Objects Setting >> File Extension Object Setup

Profile Index: 1 Profile Name:

Categories	File Extensions
Image	
<input type="button" value="Select All"/>	<input type="checkbox"/> .bmp <input type="checkbox"/> .dib <input type="checkbox"/> .gif <input type="checkbox"/> .jpeg <input type="checkbox"/> .jpg <input type="checkbox"/> .jpg2 <input type="checkbox"/> .jp2
<input type="button" value="Clear All"/>	<input type="checkbox"/> .pct <input type="checkbox"/> .pcx <input type="checkbox"/> .pic <input type="checkbox"/> .pict <input type="checkbox"/> .png <input type="checkbox"/> .tif <input type="checkbox"/> .tiff
Video	
<input type="button" value="Select All"/>	<input type="checkbox"/> .asf <input type="checkbox"/> .avi <input type="checkbox"/> .mov <input type="checkbox"/> .mpe <input type="checkbox"/> .mpeg <input type="checkbox"/> .mpg <input type="checkbox"/> .mp4
<input type="button" value="Clear All"/>	<input type="checkbox"/> .qt <input type="checkbox"/> .rm <input type="checkbox"/> .wmv <input type="checkbox"/> .3gp <input type="checkbox"/> .3gpp <input type="checkbox"/> .3gpp2 <input type="checkbox"/> .3g2
	<input type="checkbox"/> .flv <input type="checkbox"/> .swf
Audio	
<input type="button" value="Select All"/>	<input type="checkbox"/> .aac <input type="checkbox"/> .aiff <input type="checkbox"/> .au <input type="checkbox"/> .mp3 <input type="checkbox"/> .m4a <input type="checkbox"/> .m4p <input type="checkbox"/> .ogg
<input type="button" value="Clear All"/>	<input type="checkbox"/> .ra <input type="checkbox"/> .ram <input type="checkbox"/> .vox <input type="checkbox"/> .wav <input type="checkbox"/> .wma
Java	
<input type="button" value="Select All"/>	<input type="checkbox"/> .class <input type="checkbox"/> .jad <input type="checkbox"/> .jar <input type="checkbox"/> .jav <input type="checkbox"/> .java <input type="checkbox"/> .jcm <input type="checkbox"/> .js
<input type="button" value="Clear All"/>	<input type="checkbox"/> .jse <input type="checkbox"/> .jsp <input type="checkbox"/> .jtk
ActiveX	

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for this profile. The maximum length of the name you can set is 7 characters.

3. Type a name for such profile and check all the items of file extension that will be processed in the router. Finally, click **OK** to save this profile.

VII-1-10 SMS/Mail Service Object

SMS Service Object

This page allows you to set ten profiles which will be applied in **Application>>SMS/Mail Alert Service**.

Object Settings >> SMS / Mail Service Object

SMS Provider		Mail Server	Set to Factory Default
Index	Profile Name	SMS Provider	
<u>1.</u>		kotsms.com.tw (TW)	
<u>2.</u>		kotsms.com.tw (TW)	
<u>3.</u>		kotsms.com.tw (TW)	
<u>4.</u>		kotsms.com.tw (TW)	
<u>5.</u>		kotsms.com.tw (TW)	
<u>6.</u>		kotsms.com.tw (TW)	
<u>7.</u>		kotsms.com.tw (TW)	
<u>8.</u>		kotsms.com.tw (TW)	
<u>9.</u>	Custom 1		
<u>10.</u>	Custom 2		

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.
Index	Display the profile number that you can configure.
Profile	Display the name for such SMS profile.
SMS Provider	Display the service provider which offers SMS service.

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

1. Click the **SMS Provider** tab, and click the number (e.g., #1) under Index column for configuration in details.

Object Settings >> SMS / Mail Service Object

SMS Provider		Mail Server
Index	Profile Name	
<u>1.</u>		
<u>2.</u>		
<u>3.</u>		
<u>4.</u>		

2. The configuration page will be shown as follows:

Objects Setting >> SMS / Mail Service Object


Profile Index: 1

Profile Name	<input type="text" value="Line_down"/>
Service Provider	<input type="text" value="kotsms.com.tw (TW)"/>
Username	<input type="text" value="line1"/>
Password	<input type="password" value="***"/>
Quota	<input type="text" value="10"/>
Sending Interval	<input type="text" value="3"/> (seconds)

Note:

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

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such SMS profile. The maximum length of the name you can set is 31 characters.
Service Provider	Use the drop down list to specify the service provider which offers SMS service. 
Username	Type a user name that the sender can use to register to selected SMS provider. The maximum length of the name you can set is 31 characters.
Password	Type a password that the sender can use to register to selected SMS provider. The maximum length of the password you can set is 31 characters.
Quota	Type the number of the credit that you purchase from the service provider chosen above. Note that one credit equals to one SMS text message on the standard route.
Sending Interval	To avoid quota being exhausted soon, type time interval for sending the SMS.

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

Object Settings >> SMS / Mail Service Object

SMS Provider		Mail Server	Set to Factory Default
Index	Profile Name	SMS Provider	
<u>1.</u>	Line_down	kotsms.com.tw (TW)	
<u>2.</u>		kotsms.com.tw (TW)	
<u>3.</u>		kotsms.com.tw (TW)	
<u>4.</u>		kotsms.com.tw (TW)	

Customized SMS Service

Vigor router offers several SMS service provider to offer the SMS service. However, if your service provider cannot be found from the service provider list, simply use Index 9 and Index 10 to make customized SMS service. The profile name for Index 9 and Index 10 are fixed.

Object Settings >> SMS / Mail Service Object

SMS Provider		Mail Server	Set to Factory Default
Index	Profile Name	SMS Provider	
<u>1.</u>		kotsms.com.tw (TW)	
<u>2.</u>		kotsms.com.tw (TW)	
<u>3.</u>		kotsms.com.tw (TW)	
<u>4.</u>		kotsms.com.tw (TW)	
<u>5.</u>		kotsms.com.tw (TW)	
<u>6.</u>		kotsms.com.tw (TW)	
<u>7.</u>		kotsms.com.tw (TW)	
<u>8.</u>		kotsms.com.tw (TW)	
<u>9.</u>	Custom 1		
<u>10.</u>	Custom 2		

You can click the number (e.g., #9) under Index column for configuration in details.

Objects Setting >> SMS / Mail Service Object

Profile Index: 9

Profile Name	<input type="text" value="Custom 1"/>
Service Provider	<input type="text"/>
<div style="border: 1px solid black; height: 50px; width: 100%;"></div>	
Please contact with your SMS provide to get the exact URL String eg:bulksms.vsms.net:5567/eapi/submission/send_sms/2/2.0? username=###txtUser### &password=###txtPwd###&msisdn=###txtDest###&message=###txtMsg###	
Username	<input type="text"/>
Password	<input type="text"/>
Quota	<input type="text" value="10"/>
Sending Interval	<input type="text" value="3"/> (seconds)

Note:

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

Available settings are explained as follows:

Item	Description
Profile Name	Display the name of this profile. It cannot be modified.
Service Provider	Type the website of the service provider. Type the URL string in the box under the filed of Service Provider. You have to contact your SMS provider to obtain the exact URL string.
Username	Type a user name that the sender can use to register to selected SMS provider. The maximum length of the name you can set is 31 characters.
Password	Type a password that the sender can use to register to selected SMS provider. The maximum length of the password you can set is 31 characters.
Quota	Type the total number of the messages that the router will send out.
Sending Interval	Type the shortest time interval for the system to send SMS.

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

Mail Service Object

This page allows you to set ten profiles which will be applied in **Application>>SMS/Mail Alert Service**.

Object Settings >> SMS / Mail Service Object

SMS Provider		Mail Server	Set to Factory Default
Index	Profile Name		
<u>1.</u>			
<u>2.</u>			
<u>3.</u>			
<u>4.</u>			
<u>5.</u>			
<u>6.</u>			
<u>7.</u>			
<u>8.</u>			
<u>9.</u>			
<u>10.</u>			

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.
Index	Display the profile number that you can configure.
Profile	Display the name for such mail server profile.

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

1. Click the **Mail Server** tab, and click the number (e.g., #1) under Index column for configuration in details.

Object Settings >> SMS / Mail Service Object

SMS Provider	Mail Server
Index	
<u>1.</u>	
<u>2.</u>	
<u>3.</u>	
<u>4.</u>	

2. The configuration page will be shown as follows:

Objects Setting >> SMS / Mail Service Object

Profile Index: 1

Profile Name	Mail_Notify
SMTP Server	192.168.1.98
SMTP Port	25
Sender Address	carrie_ni@draytek.com
<input type="checkbox"/> Use SSL	
<input checked="" type="checkbox"/> Authentication	
Username	john
Password	*****
Sending Interval	0 (seconds)

Note:

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

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such mail service profile. The maximum length of the name you can set is 31 characters.
SMTP Server	Type the IP address of the mail server.
SMTP Port	Type the port number for SMTP server.
Sender Address	Type the e-mail address of the sender.
Use SSL	Check this box to use port 465 for SMTP server for some e-mail server uses https as the transmission method.
Authentication	The mail server must be authenticated with the correct username and password to have the right of sending message out. Check the box to enable the function. Username - Type a name for authentication. The maximum length of the name you can set is 31 characters. Password - Type a password for authentication. The maximum length of the password you can set is 31 characters.
Sending Interval	Define the interval for the system to send the SMS out.

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

Object Settings >> SMS / Mail Service Object

SMS Provider		Mail Server	Set to Factory Default
Index	Profile Name		
<u>1.</u>	Mail_Notify		
<u>2.</u>			
<u>3.</u>			

VII-1-11 Notification Object

This page allows you to set ten profiles which will be applied in **Application>>SMS/Mail Alert Service**.

You can set an object with different monitoring situation.

Object Settings >> Notification Object

Index	Profile Name	Settings	Set to Factory Default
<u>1.</u>			
<u>2.</u>			
<u>3.</u>			
<u>4.</u>			
<u>5.</u>			
<u>6.</u>			
<u>7.</u>			
<u>8.</u>			

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

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

Object Settings >> Notification Object

Index	Profile Name
<u>1.</u>	
<u>2.</u>	
<u>3.</u>	
<u>4.</u>	
<u>5.</u>	

- The configuration page will be shown as follows:

Objects Setting >> Notification Object

Profile Index: 1

Profile Name

Category		Status
WAN	<input type="checkbox"/> Disconnected	<input type="checkbox"/> Reconnected
VPN Tunnel	<input type="checkbox"/> Disconnected	<input type="checkbox"/> Reconnected
Temperature Alert	<input type="checkbox"/> Out of Range	
WAN Budget	<input type="checkbox"/> Limit Reached	

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such notification profile. The maximum length of the name you can set is 15 characters.
Category	Display the types that will be monitored.
Status	Display the status for the category. You can check the box to be monitored.

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

Object Settings >> Notification Object

[Set to Factory Default](#)

Index	Profile Name	Settings
1.	Notify_attack	WAN VPN
2.		
3.		

VII-1-12 String Object

This page allows you to set string profiles which will be applied in route policy (domain name selection for destination) and etc.

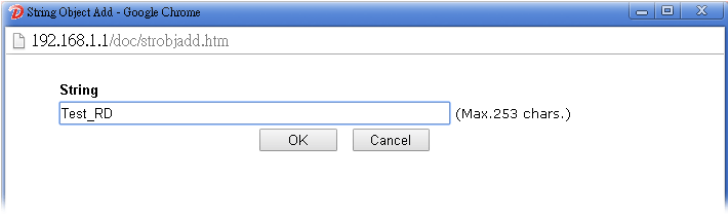
Objects Setting >> String Object

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

Index	String	
1	123	<input type="checkbox"/>
2	TEST_RD	<input type="checkbox"/>

Add

Available settings are explained as follows:

Item	Description
Add	Click it to open the following page for adding a new string object. 
Set to Factory Default	Click it to clear all of the settings in this page.
Index	Display the number link of the string profile.
String	Display the string defined.
Clear	Choose the string that you want to remove. Then click this check box to delete the selected string.

Below shows an example to apply string object (in Route Policy):

Load-Balance/Route Policy

Index: 1

Enable

Comment [Delete](#)

Criteria

Protocol

Source Any Src IP Range Src IP Subnet

Destination Any Dest IP Range Dest IP Subnet Domain Name

[Select](#) [Delete](#)

[Add](#)

Destination Port Any Dest Port Start ~ Dest Port End

Send via if Criteria Matched

Application Notes

A-1 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection

Follow the steps listed below:

1. Log into the web user interface of Vigor router.
2. Configure relational objects first. Open Object Settings>>SMS/Mail Server Object to get the following page.

Object Settings >> SMS / Mail Service Object

Index	Profile Name	SMS Provider
1.		kotsms.com.tw (TW)
2.		kotsms.com.tw (TW)
3.		kotsms.com.tw (TW)
4.		kotsms.com.tw (TW)
5.		kotsms.com.tw (TW)
6.		kotsms.com.tw (TW)
7.		kotsms.com.tw (TW)
8.		kotsms.com.tw (TW)
9.	Custom 1	
10.	Custom 2	

Index 1 to Index 8 allows you to choose the built-in SMS service provider. If the SMS service provider is not on the list, you can configure Index 9 and Index 10 to add the new service provider to Vigor router.

3. Choose any index number (e.g., Index 1 in this case) to configure the SMS Provider setting. In the following page, type the username and password and set the quota that the router can send the message out.

Objects Setting >> SMS / Mail Service Object

Profile Index: 1

Profile Name	<input type="text" value="Local number"/>
Service Provider	<input type="text" value="kotsms.com.tw (TW)"/>
Username	<input type="text" value="abc5026"/>
Password	<input type="password" value="***"/>
Quota	<input type="text" value="3"/>
Sending Interval	<input type="text" value="3"/> (seconds)

Note:

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

- After finished the settings, click **OK** to return to previous page. Now you have finished the configuration of the SMS Provider profile setting.

Object Settings >> SMS / Mail Service Object

SMS Provider		Mail Server	Set to Factory Default
Index	Profile Name	SMS Provider	
1.	Local number	kotsms.com.tw (TW)	
2.		kotsms.com.tw (TW)	
3.		kotsms.com.tw (TW)	
4.		kotsms.com.tw (TW)	
5.		kotsms.com.tw (TW)	
6.		kotsms.com.tw (TW)	
7.		kotsms.com.tw (TW)	
8.		kotsms.com.tw (TW)	
9.	Custom 1		
10.	Custom 2		

- Open **Object Settings>>Notification Object** to configure the event conditions of the notification.

Object Settings >> Notification Object

			Set to Factory Default
Index	Profile Name	Settings	
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			

- Choose any index number (e.g., Index 1 in this case) to configure conditions for sending the SMS. In the following page, type the name of the profile and check the **Disconnected** and **Reconnected** boxes for **WAN** to work in concert with the topic of this paper.

Objects Setting >> Notification Object

Profile Index: 1

Profile Name		WAN_Notify	
Category	Status		
WAN	<input checked="" type="checkbox"/> Disconnected	<input checked="" type="checkbox"/> Reconnected	
VPN Tunnel	<input type="checkbox"/> Disconnected	<input type="checkbox"/> Reconnected	
Temperature Alert	<input type="checkbox"/> Out of Range		

- After finished the settings, click **OK** to return to previous page. You have finished the configuration of the notification object profile setting.

| [Set to Factory Default](#) |

Index	Profile Name	Settings
1.	WAN_Notify	WAN
2.		
3.		
4.		
5.		
6.		
7.		
8.		

8. Now, open **Applications >> SMS / Mail Alert Service**. Use the drop down list to choose SMS Provider and the Notify Profile (specify the time of sending SMS). Then, type the phone number in the field of Recipient (the one who will receive the SMS).

Applications >> SMS / Mail Alert Service

| [Set to Factory Default](#) |

SMS Alert		Mail Alert			
Index	SMS Provider	Recipient Number	Notify Profile	Schedule(1-15)	
1 <input checked="" type="checkbox"/>	1 - Local number ▼	0912345678	1 - WAN_Notify ▼		
2 <input type="checkbox"/>	1 - Local number ▼		1 - WAN_Notify ▼		
3 <input type="checkbox"/>	1 - Local number ▼		1 - WAN_Notify ▼		
4 <input type="checkbox"/>	1 - Local number ▼		1 - WAN_Notify ▼		
5 <input type="checkbox"/>	1 - Local number ▼		1 - WAN_Notify ▼		
6 <input type="checkbox"/>	1 - Local number ▼		1 - WAN_Notify ▼		
7 <input type="checkbox"/>	1 - Local number ▼		1 - WAN_Notify ▼		
8 <input type="checkbox"/>	1 - Local number ▼		1 - WAN_Notify ▼		
9 <input type="checkbox"/>	1 - Local number ▼		1 - WAN_Notify ▼		
10 <input type="checkbox"/>	1 - Local number ▼		1 - WAN_Notify ▼		

Note:

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

OK

Cancel

9. Click OK to save the settings. Later, if one of the WAN connections fails in your router, the system will send out SMS to the phone number specified. If the router has only one WAN interface, the system will send out SMS to the phone number while reconnecting the WAN interface successfully.

Remark: How the customize the SMS Provider

Choose one of the Index numbers (9 or 10) allowing you to customize the SMS Provider. In the web page, type the URL string of the SMS provider and type the username and password. After clicking OK, the new added SMS provider will be added and will be available for you to specify for sending SMS out.

Objects Setting >> SMS / Mail Service Object

Profile Index: 9

Profile Name	<input type="text" value="Custom 1"/>
Service Provider	<input type="text" value="clickatell"/>
<div style="border: 1px solid black; height: 50px; width: 100%;"></div>	
Please contact with your SMS provide to get the exact URL String eg: bulksms.vsms.net:5567/eapi/submission/send_sms/2/2.0? username=###txtUser### &password=###txtPwd###&msisdn=###txtDest###&message=###txtMsg###	
Username	<input type="text" value="ilan123"/>
Password	<input type="password" value="*****"/>
Quota	<input type="text" value="10"/>
Sending Interval	<input type="text" value="3"/> (seconds)

Note:

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

VII-2 USB Application

USB device connected on Vigor router can be regarded as a server or WAN interface. By way of Vigor router, clients on LAN can access, write and read data stored in USB storage disk with different applications. After setting the configuration in **USB Application**, you can type the IP address of the Vigor router and username/password created in **USB Application>>USB User Management** on the client software. Then, the client can use the FTP site (USB storage disk) or share the SMB service through Vigor router.

Web User Interface

- SSL VPN
- USB Application**
- USB General Settings
- USB User Management
- File Explorer
- USB Device Status
- Temperature Sensor
- Modem Support List
- SMB Client Support List
- System Maintenance

VII-2-1 USB General Settings

This page will determine the number of concurrent FTP connection, default charset for FTP server and enable SMB service. At present, the Vigor router can support USB storage disk with formats of FAT16 and FAT32 only. Therefore, before connecting the USB storage disk into the Vigor router, please make sure the memory format for the USB storage disk is FAT16 or FAT32. It is recommended for you to use FAT32 for viewing the filename completely (FAT16 cannot support long filename).

USB Application >> USB General Settings

USB General Settings

General Settings	
Simultaneous FTP Connections	<input type="text" value="5"/> (Maximum 6)
Default Charset	<input type="text" value="English"/>
SMB File Sharing Service (Network Neighborhood)	
<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Access Mode	
<input checked="" type="radio"/> LAN Only <input type="radio"/> LAN And WAN	
NetBios Name Service	
Workgroup Name	<input type="text" value="WORKGROUP"/>
Host Name	<input type="text" value="Vigor"/>
Printer Server	
<input checked="" type="radio"/> Enable <input type="radio"/> Disable	

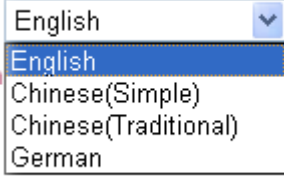
Note:

- 1.If character set is set to "English", only English long file name is supported.
- 2.Multi-session FTP download will be banned by Router FTP server. If your FTP client has a multi-connection mechanism, such as FileZilla, you should limit client connections to 1 to improve performance.
- 3.A workgroup name must be different from the host name. The workgroup name can have up to 15 characters and the host name can have up to 15 characters.Names cannot contain any of the following: . ; : " < > * + = / | ?.

OK

Available settings are explained as follows:

Item	Description
General Settings	Simultaneous FTP Connections - This field is used to specify the quantity of the FTP sessions. The router allows up to 6 FTP sessions connecting to USB storage disk at one time. Default Charset - At present, Vigor router supports four types of character sets. Default Charset is for English based file name.

	
SMB File Sharing Service	Click Enable to invoke SMB service (file sharing) via the router.
Access Mode	<p>LAN Only - Users coming from internet cannot connect to the SMB server of the router.</p> <p>LAN And WAN - Both LAN and WAN users can access SMB server of the router.</p>
NetBios Name Service	<p>For the NetBios service of USB storage disk, you have to specify a workgroup name and a host name. A workgroup name must not be the same as the host name. The workgroup name can have as many as 15 characters and the host name can have as many as 23 characters. Both them cannot contain any of the following--- ; : " < > * + = \ ?.</p> <p>Workgroup Name - Type a name for the workgroup.</p> <p>Host Name - Type the host name for the router.</p>
Printer Server	Enable - Click it to make Vigor router act as a printer server (with USB printer attached).

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

VII-2-2 USB User Management

This page allows you to set profiles for FTP/SMB users. Any user who wants to access into the USB storage disk must type the same username and password configured in this page. Before adding or modifying settings in this page, please insert a USB storage disk first. Otherwise, an error message will appear to warn you.


USB Application >> USB User Management

USB User Management | [Set to Factory Default](#) |

Index	Username	Home Folder	Index	Username	Home Folder
1.			9.		
2.			10.		
3.			11.		
4.			12.		
5.			13.		
6.			14.		
7.			15.		
8.			16.		


Click index number to access into configuration page.

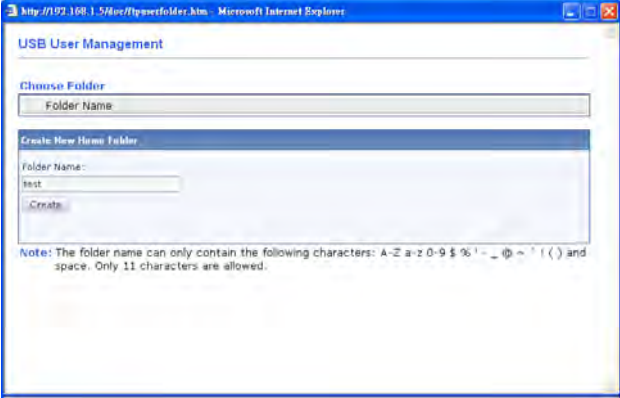
Profile Index: 1

FTP/SMB User	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Username	<input type="text"/>
Password	<input type="text"/> (Maximum 11 Characters)
Confirm Password	<input type="text"/>
Home Folder	<input type="text"/> 
Access Rule	
File	<input type="checkbox"/> Read <input type="checkbox"/> Write <input type="checkbox"/> Delete
Directory	<input type="checkbox"/> List <input type="checkbox"/> Create <input type="checkbox"/> Remove

Note: The folder name can only contain the following characters: A-Z a-z 0-9 \$ % ' - _ @ ~ ` ! () and space.

Available settings are explained as follows:

Item	Description
FTP/SMB User	<p>Enable - Click this button to activate this profile (account) for FTP service or SMB User service. Later, the user can use the username specified in this page to login into FTP server.</p> <p>Disable - Click this button to disable such profile.</p>
Username	<p>Type the username for FTP/SMB users for accessing into FTP server (USB storage disk). Be aware that users cannot access into USB storage disk in anonymity. Later, you can open FTP client software and type the username specified here for accessing into USB storage disk. The length of the name is limited to 11 characters.</p> <p>Note: "Admin" could not be typed here as username, for the word is specified for accessing into web pages of Vigor router only. Also, it is reserved for FTP firmware upgrade usage.</p> <p>Note: FTP Passive mode is not supported by Vigor Router. Please disable the mode on the FTP client.</p>
Password	<p>Type the password for FTP/SMB users for accessing FTP server. Later, you can open FTP client software and type the password specified here for accessing into USB storage disk. The length of the password is limited to 11 characters.</p>
Confirm Password	<p>Type the password again to make confirmation.</p>
Home Folder	<p>It determines the folder for the client to access into. The user can enter a directory name in this field. Then, after clicking OK, the router will create the specific/new folder in the USB storage disk. In addition, if the user types "/" here, he/she can access into all of the disk folders and files in USB storage disk.</p> <p>Note: When write protect status for the USB storage disk is ON, you cannot type any new folder name in this field. Only "/" can be used in such case.</p> <p>You can click  to open the following dialog to add any new folder which can be specified as the Home Folder.</p>

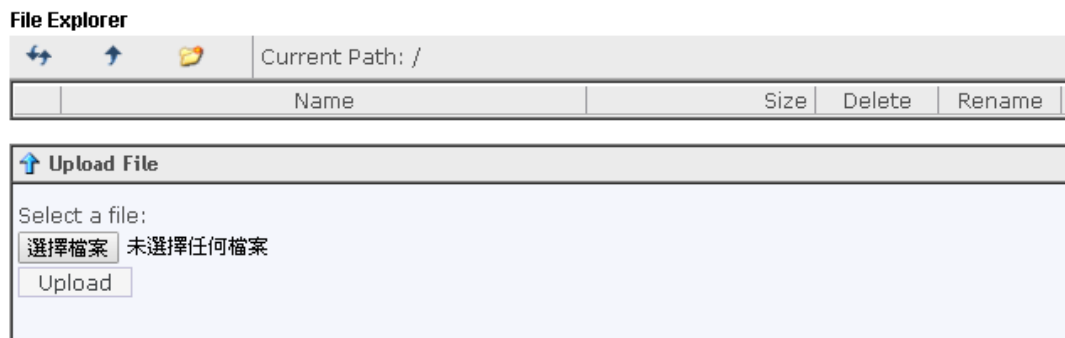
	
<p>Access Rule</p>	<p>It determines the authority for such profile. Any user, who uses such profile for accessing into USB storage disk, must follow the rule specified here.</p> <p>File - Check the items (Read, Write and Delete) for such profile.</p> <p>Directory -Check the items (List, Create and Remove) for such profile.</p>

Before you click OK, you have to insert a USB storage disk into the USB interface of the Vigor router. Otherwise, you cannot save the configuration.

VII-2-3 File Explorer




File Explorer offers an easy way for users to view and manage the content of USB storage disk connected on Vigor router.

USB Application >> File Explorer



Note: The folder can not be deleted when it is not empty.

Available settings are explained as follows:

Item	Description
 Refresh	Click this icon to refresh files list.
 Back	Click this icon to return to the upper directory.
 Create	Click this icon to add a new folder.
Current Path	Display current folder.
Upload	Click this button to upload the selected file to the USB

storage disk. The uploaded file in the USB diskette can be shared for other user through FTP.

VII-2-4 USB Device Status

This page is to monitor the status for USB device connecting to Vigor router. In addition, the status of the USB printer or USB sensor connecting to Vigor router can be checked from such page. If you want to remove the storage disk from USB port in router, please click **Disconnect USB Disk** first. And then, remove the USB device later.

USB Application >> USB Device Status

Disk	Printer	Sensor	Refresh
USB Mass Storage Device Status			
Connection Status: No Disk Connected			<input type="button" value="Disconnect USB Disk"/>
Disk Capacity: 0 MB			
Free Capacity: 0 MB Refresh			
USB Disk Users Connected			
Index	Service	IP Address(Port)	Username

Note:

1. Only support FAT16 and FAT32 format, FAT32 is recommended.
2. Only support to mount single partition, maximum capacity is 500GB. If there are more than one partition, only one of them will be mounted.
3. Single file size can be up to 4GB, which is the limitation of FAT32 format.
4. If the write protect switch of USB disk is turned on, the USB disk is in **READ-ONLY** mode. No data can be written to it.

Available settings are explained as follows:

Item	Description
Connection Status	If there is no USB device connected to Vigor router, "No Disk Connected" will be shown here.
Disk Capacity	It displays the total capacity of the USB storage disk.
Free Capacity	It displays the free space of the USB storage disk. Click Refresh at any time to get new status for free capacity.
Index	It displays the number of the client which connects to FTP server.
IP Address	It displays the IP address of the user's host which connects to the FTP server.
Username	It displays the username that user uses to login to the FTP server.

When you insert USB device into the Vigor router, the system will start to find out such device within several seconds.

USB Application >> USB Device Status

Disk	Printer	Sensor	Refresh
USB Mass Storage Device Status			
Connection Status: Disk Connected			Disconnect USB Disk
Write Protect Status: No			
Disk Capacity: 2009 MB			
Free Capacity: 925 MB Refresh			
USB Disk Users Connected			
Index	Service	IP Address(Port)	Username

Note:

1. Only support FAT16 and FAT32 format, FAT32 is recommended.
2. Only support to mount single partition, maximum capacity is 500GB. If there are more than one partition, only one of them will be mounted.
3. Single file size can be up to 4GB, which is the limitation of FAT32 format.
4. If the write protect switch of USB disk is turned on, the USB disk is in **READ-ONLY** mode. No data can be written to it.

VII-2-5 Temperature Sensor

A USB Thermometer is now available. It complements your installed DrayTek router installations which will help you monitor the server or data communications room environment and notify you if the server room or data communications room is overheating.



During summer in particular, it is important to ensure that your server or data communications equipment are not overheating due to cooling system failures.

The inclusion of a USB thermometer in compatible Vigor routers will continuously monitor the temperature of its environment. When a pre-determined threshold is reached you will be alerted by either an email or SMS so you can undertake appropriate action.

Temperature Sensor Settings

USB Application >> Temperature Sensor Setting

Temperature Chart	Temperature Sensor Settings
Display Settings	
Temperature Calibration	<input type="text" value="0.00"/>
Temperature Unit	<input checked="" type="radio"/> Celsius <input type="radio"/> Fahrenheit
Alarm Settings	
<input type="checkbox"/> Enable Syslog Alarm	
Upper temperature limit	<input type="text" value="30.00"/>
Lower temperature limit	<input type="text" value="18.00"/>
<input type="button" value="OK"/>	

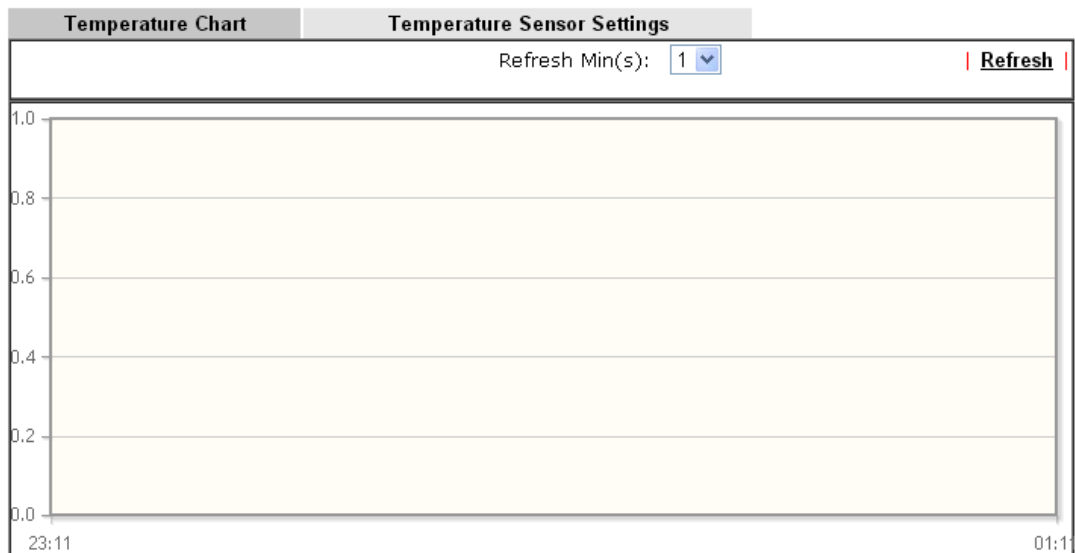
Available settings are explained as follows:

Item	Description
Display Settings	Temperature Calibration - Type a value used for correcting the temperature error. Temperature Unit - Choose the display unit of the temperature. There are two types for you to choose.
Alarm Settings	Enable Syslog Alarm - The temperature log will be recorded on Syslog if it is enabled. Upper temperature limit/Lower temperature limit - Type the upper limit and lower limit for the system to send out temperature alert.

Temperature Chart

Below shows an example of temperature graph:

USB Application >> Temperature Sensor Graph





Manufacturer:
Product:
Current Temperature:
Average Temperature:
Maximum Temperature:
Minimum temperature:

VII-2-6 Modem Support List

Such page provides the information about the brand name and model name of the USB modems which are supported by Vigor router.

USB Application >> Modem Support List

The following compatibility test lists 3.5G/LTE modems **supported by Vigor router under certain environment or countries**. If the LTE modem you have is on the list but cannot work properly, please write an e-mail to support@draytek.com or consult your dealer for further information.

PPP mode	DHCP mode	WiMAX		
Brand	Model	LTE	Status	
4G system	XSPUG P3		Y	
Aiko	Aiko 76E		Y	
Aiko	Aiko 83D		Y	
Alcatel	Alcatel L100V		Y	
Alcatel	Alcatel W100		Y	
Alcatel	Alcatel X080S		Y	
Alcatel	Alcatel X230		Y	
Alcatel	Alcatel X500		Y	
Alfa	ALFA Flyppp		Y	
Amoi	Amoi H01		Y	
AnyDATA	ADU-300		Y	
AnyDATA	ADU-500A		M	

VII-2-7 SMB Client Support List

SMB Client Support List provides the test status information for applications with file sharing operated under different platforms.

USB Application >> SMB Client Support List



The following compatibility test lists suggested SMB clients supported by Vigor router.

Platform	Application	Status
Microsoft® Windows® XP	Built in	I
Microsoft® Windows Vista™	Built in	Y
Microsoft® Windows® 7	Built in	Y
Microsoft® Windows® 8	Built in	M
Microsoft® Windows® 10	Built in	Y
OS X® 10.7.5	Built in	Y
OS X® 10.10	Built in	Y
Ubuntu 14.04	Built in	Y
Android™	AndSMB	Y
Android™	ES File Explorer	Y
Android™	File Expert	Y
Android™	File Manager	Y
Android™	Solid Explorer	Y
Android™	SharesFinder	Y
iOS	exPlayer	Y
iOS	nPlayer	Y

Y: Tested and is supported.

I: Supported but has some issue.

M: Has not been tested but might be supported.

Application Notes

A-1 How can I get the files from USB storage device connecting to Vigor router?

Files on USB storage device can be reviewed by opening **USB Application >> File Explorer**. If it is necessary for you to delete, copy files on the device or write, paste files to the device, it must be done through SMB server or FTP server.

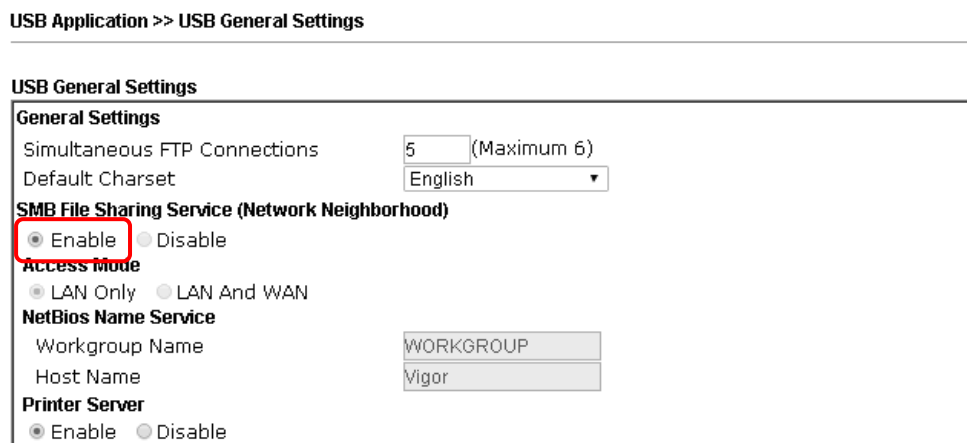
SMB service is based on the original USB FTP service. You will need to setup USB FTP first. We would like to give brief instructions on USB FTP setup here.

1. Plug the USB device to the USB port on the router. Make sure **Disk Connected** appears on the **Connection Status** as the figure shown below:



Note: If the write protect switch of USB disk is turned on, the USB disk is in READ-ONLY mode. No data can be written to it.

2. Then, please open **USB Application >> USB General Settings** to enable SMB service.



- Note:**
- 1.If character set is set to "English", only English long file name is supported.
 - 2.Multi-session FTP download will be banned by Router FTP server. If your FTP client has a multi-connection mechanism, such as FileZilla, you should limit client connections to 1 to improve performance.
 - 3.A workgroup name must be different from the host name. The workgroup name can have up to 15 characters and the host name can have up to 15 characters.Names cannot contain any of the following: . ; : " < > * + = / | ?.

OK

- Setup a user account for the FTP service by using **USB Application >>USB User Management**. Click **Enable** to enable FTP User account. Here we add a new account "user1" and assign authorities "Read", "Write" and "List" to it.

USB Application >> USB User Management

Profile Index: 1

FTP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	user1
Password (Maximum 11 Characters)
Confirm Password
Home Folder	<input type="text"/> 📁
Access Rule	
File	<input type="checkbox"/> Read <input type="checkbox"/> Write <input type="checkbox"/> Delete
Directory	<input type="checkbox"/> List <input type="checkbox"/> Create <input type="checkbox"/> Remove

Note: The folder name can only contain the following characters: A-Z a-z 0-9 \$ % ' - _ @ ~ ` ! () / and space.

OK Clear Cancel

- Click **OK** to save the configuration.
- Make sure the FTP service is running properly. Please open a browser and type *ftp://192.168.1.1*. Use the account "user1" to login.

Log On As

Either the server does not allow anonymous logins or the e-mail address was not accepted.

FTP server: 192.168.1.1

User name: user1

Password:

After you log on, you can add this server to your Favorites and return to it easily.

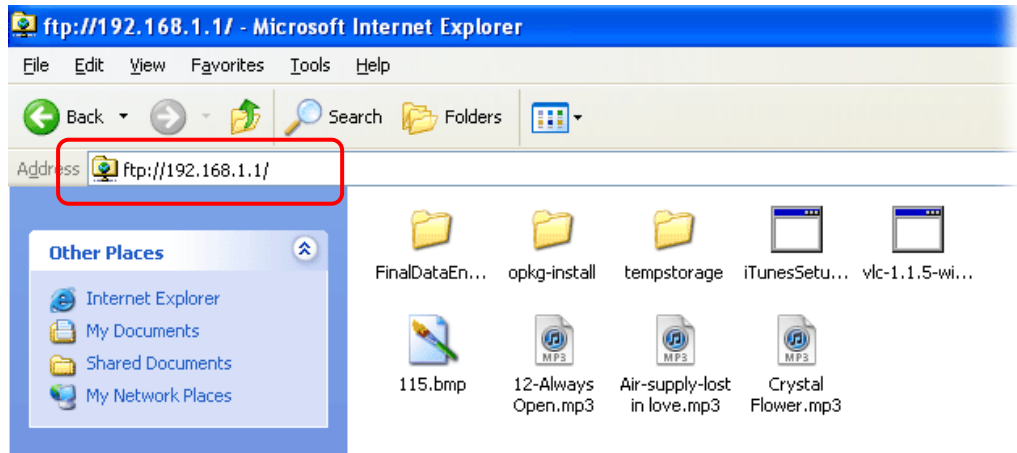
⚠️ FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use Web Folders (WebDAV) instead.

Learn more about [using Web Folders](#).

Log on anonymously Save password

Log On Cancel

- When the following screen appears, it means the FTP service is running properly.



- Return to **USB Application >> USB Disk Status**. The information for FTP server will be shown as below.

USB Application >> USB Disk Status

USB Mass Storage Device Status

Connection Status: **Disk Connected** Disconnect USB Disk

Write Protect Status: **No**

Disk Capacity: 2009 MB

USB Disk Users Connected | Refresh |

Index	Service	IP Address(Port)	Username	
1.	FTP	192.168.1.10(1963)	user1	Drop

Now, users in LAN of Vigor2133 can access into the USB storage device by typing ftp://192.168.1.1 on any browser. They can add or remove files / directories, depending on the Access Rule for FTP account settings in **USB Application >>USB User Management**.

Part VIII Troubleshooting



Troubleshooting

This part will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration.

VIII-1 Diagnostics

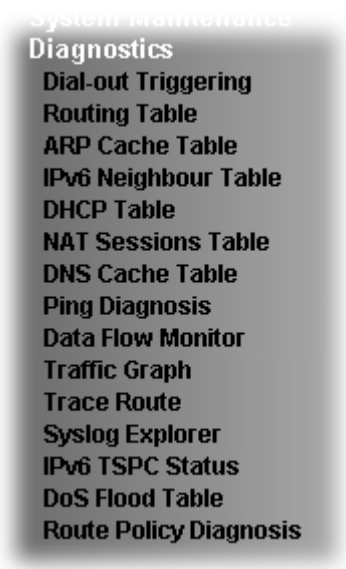
This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

If all above stages are done and the router still cannot run normally, it is the time for you to contact your dealer or DrayTek technical support for advanced help.

Web User Interface

First, take a look at the menu items under Diagnostics. Diagnostic Tools provide a useful way to view or diagnose the status of your Vigor router.



VIII-1-1 Dial-out Triggering

Click **Diagnostics** and click **Dial-out Triggering** to open the web page. The internet connection (e.g., PPPoE) is triggered by a package sending from the source IP address.

Diagnostics >> Dial-out Triggering

Dial-out Triggered Packet Header | [Refresh](#) |

HEX Format:

```
00 00 00 00 00 00-00 00 00 00 00 00-00 00  
  
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
```

Decoded Format:

```
0.0.0.0 -> 0.0.0.0  
Pr 0 len 0 (0)
```

Available settings are explained as follows:

Item	Description
Decoded Format	It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.
Refresh	Click it to reload the page.

VIII-1-2 Routing Table

Click **Diagnostics** and click **Routing Table** to open the web page.

Diagnostics >> View Routing Table

IPv4

Key	Destination	Gateway	Interface
C~	192.168.1.0/ 255.255.255.0	directly connected	LAN1

[Refresh](#)

Key

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

IPv6

Destination	Interface	Flags	Metric	Next Hop
FE80::/64	LAN1	U	256	::
FE80::/64	LAN2	U	256	::
FE80::/64	LAN3	U	256	::
FE80::/64	LAN4	U	256	::
FE80::/64	DMZ	U	256	::
FF00::/8	LAN1	U	256	::
FF00::/8	LAN2	U	256	::
FF00::/8	LAN3	U	256	::
FF00::/8	LAN4	U	256	::
FF00::/8	DMZ	U	256	::

[Refresh](#)

Show Detail

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

VIII-1-3 ARP Cache Table

Click **Diagnostics** and click **ARP Cache Table** to view the content of the ARP (Address Resolution Protocol) cache held in the router. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.

Diagnostics >> View ARP Cache Table

LAN
WAN

Show: ALL LANS and ALL VLANs

Ethernet ARP Cache Table | [Clear](#) | [Refresh](#) |

IP Address	MAC Address	Netbios Name	Interface	VLAN	Port
192.168.1.5	00-05-5D-	A1000351	LAN1	VLAN0	P1

Show Comment

Available settings are explained as follows:

Item	Description
Show	Specify LAN and VLAN to display related information. In default, this page will display all of the information about LAN and VLAN.
Refresh	Click it to reload the page.

VIII-1-4 IPv6 Neighbour Table

The table shows a mapping between an Ethernet hardware address (MAC Address) and an IPv6 address. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **IPv6 Neighbour Table** to open the web page.

[Diagnostics >> View IPv6 Neighbour Table](#)

IPv6 Neighbour Table			Refresh
IPv6 Address	Mac Address	Interface	
FF02::2	33-33-00-00-00-02	LAN	
FF02::1:3	33-33-00-01-00-03	LAN	
FE80::3D5E:E74:8751:A44B	e8-9d-87-87-69-2f	LAN	
FF02::1:FF51:A44B	33-33-ff-51-a4-4b	LAN	
FE80::250:7FFF:FEC9:1E79	00-50-7f-c9-1e-79	LAN	
FE80::250:7FFF:FEC8:4305	00-50-7f-c8-43-05	LAN	
FF02::1	33-33-00-00-00-01	LAN	
FF02::1	00-00-00-00-00-00	USB2	
FF02::1:2	00-00-00-00-00-00	USB2	
FE80::9D5C:CA86:5428:3CA7	00-26-2d-fe-63-4f	LAN	
FF02::1:FF0A:673C	33-33-ff-0a-67-3c	LAN	

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

VIII-1-5 DHCP Table

The facility provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **DHCP Table** to open the web page.

Diagnostics >> View DHCP Assigned IP Addresses

Show :

DHCP IP Assignment Table		Other IP Assignment Table			Refresh
LAN1		: DHCP Server On	IP Pool: 192.168.1.10 ~ 192.168.1.209		
Index	IP Address	MAC Address	Leased Time	HOST ID	

LAN1					
1	192.168.1.10	00-50-7F-F1-05-FD	22:08:44		

Show Comment

DHCPv6 IP Assignment Table

[Refresh](#)

Index	IPv6 Address	IAID	Link-layer Address	Lease

Available settings are explained as follows:

Item	Description
Index	It displays the connection item number.
IP Address	It displays the IP address assigned by this router for specified PC.
MAC Address	It displays the MAC address for the specified PC that DHCP assigned IP address for it.
Leased Time	It displays the leased time of the specified PC.
HOST ID	It displays the host ID name of the specified PC.
Refresh	Click it to reload the page.

VIII-1-6 NAT Sessions Table

Click **Diagnostics** and click **NAT Sessions Table** to open the list page.

Diagnostics >> NAT Sessions Table

NAT Active Sessions Table (Limit: 128 entries) | **Refresh** |

Private IP :Port	#Pseudo Port	Peer IP :Port	Interface
------------------	--------------	---------------	-----------

Available settings are explained as follows:

Item	Description
Private IP:Port	It indicates the source IP address and port of local PC.
#Pseudo Port	It indicates the temporary port of the router used for NAT.
Peer IP:Port	It indicates the destination IP address and port of remote host.
Interface	It displays the representing number for different interface.
Refresh	Click it to reload the page.

VIII-1-8 Ping Diagnosis

Click Diagnostics and click Ping Diagnosis to open the web page.

Diagnostics >> Ping Diagnosis

Ping Diagnosis

IPV4 IPV6

Source IP:

Ping to: IP Address:

Result

Host/ IP
DNS
Gateway

or

Diagnostics >> Ping Diagnosis

Ping Diagnosis

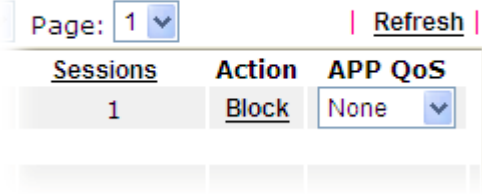
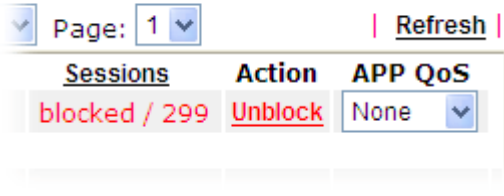
IPV4 IPV6

Ping IPv6 Address:

Result

Available settings are explained as follows:

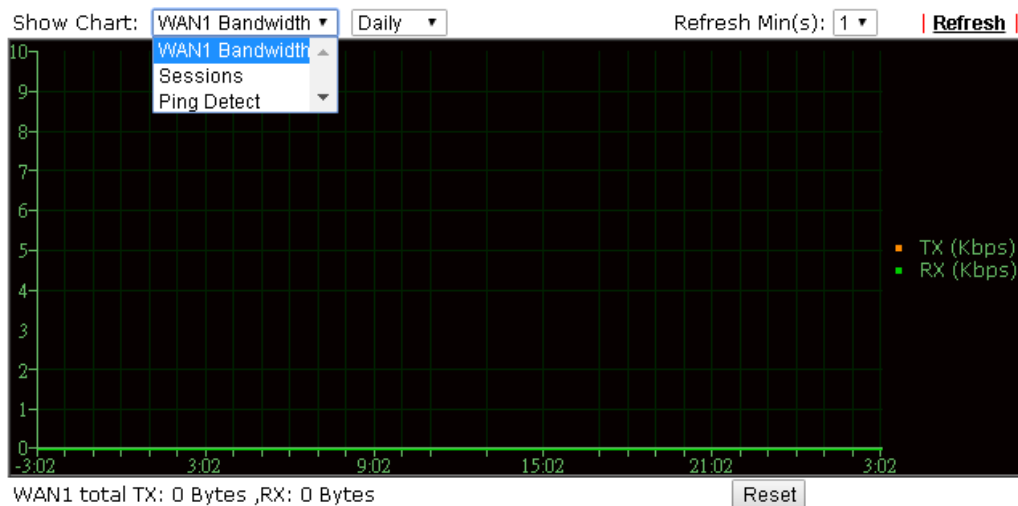
Item	Description
IPV4 /IPV6	Choose the interface for such function.
Ping to	Use the drop down list to choose the destination that you want to ping.
IP Address	Type the IP address of the Host/IP that you want to ping.
Ping IPv6 Address	Type the IPv6 address that you want to ping.
Run	Click this button to start the ping work. The result will be displayed on the screen.
Clear	Click this link to remove the result on the window.

	Refresh Seconds: <input type="text" value="10"/> <input type="button" value="v"/> <input type="text" value="10"/> <input type="text" value="15"/> <input type="text" value="30"/>
Refresh	Click this link to refresh this page manually.
Index	Display the number of the data flow.
IP Address	Display the IP address of the monitored device.
TX rate (kbps)	Display the transmission speed of the monitored device.
RX rate (kbps)	Display the receiving speed of the monitored device.
Sessions	Display the session number that you specified in Limit Session web page.
Action	<p>Block - can prevent specified PC accessing into Internet within 5 minutes.</p>  <p>Unblock -The device with the IP address will be blocked for five minutes. The remaining time will be shown on the session column. Click it to cancel the IP address blocking.</p> 
APP QoS	Use the drop down list to change the priority in data transmission for the specified IP address (host). <input type="text" value="None"/> <input type="text" value="None"/> <input type="text" value="Class 1"/> <input type="text" value="Class 2"/> <input type="text" value="Class 3"/> <input type="text" value="Default"/>
Current /Peak/Speed	<p>Current means current transmission rate and receiving rate for WAN interface.</p> <p>Peak means the highest peak value detected by the router in data transmission.</p> <p>Speed means line speed specified in WAN>>General Setup. If you do not specify any rate at that page, here will display Auto for instead.</p>

VIII-1-10 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to open the web page. Choose WAN1/WAN2/WAN3/WAN4 Bandwidth, Sessions, Ping Detect, daily or weekly for viewing different traffic graph. Click **Reset** to zero the accumulated RX/TX (received and transmitted) data of WAN. Click **Refresh** to renew the graph at any time.

Diagnostics >> Traffic Graph



The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1/WAN2/WAN3/LTE/WAN4 Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

For Sessions chart, the numbers displayed on vertical axis represent the numbers of the NAT sessions during the past.

VIII-1-11 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
Protocol: ICMP ▾
Host / IP Address:

Result | [Clear](#) |

or

Diagnostics >> Trace Route

Trace Route

IPv4 IPv6
Trace Host / IP Address:

Result | [Clear](#) |

Available settings are explained as follows:

Item	Description
IPv4 / IPv6	Click one of them to display corresponding information for it.
Protocol	Use the drop down list to choose the protocol that you want to ping through.
Host/IP Address	It indicates the IP address of the host.
Trace Host/IP Address	It indicates the IPv6 address of the host.

Run	Click this button to start route tracing work.
Clear	Click this link to remove the result on the window.

VIII-1-12 Syslog Explorer

Such page provides real-time syslog and displays the information on the screen.


For Web Syslog

This page displays the time and message for User/Firewall/call/WAN/VPN settings. You can check **Enable Web Syslog**, specify the type of Syslog and choose the display mode you want. Later, the event of Syslog with specified type will be shown for your reference.

Diagnostics >> Syslog Explorer

Web Syslog		USB Syslog	
<input type="checkbox"/> Enable Web Syslog	Syslog Type <input type="text" value="User"/>	Display Mode <input type="text" value="Stop record when full"/>	Export Refresh Clear
Time	Message		

Available settings are explained as follows:

Item	Description
Enable Web Syslog	Check this box to enable the function of Web Syslog.
Syslog Type	Use the drop down list to specify a type of Syslog to be displayed. 
Export	Click this link to save the data as a file.
Refresh	Click this link to refresh this page manually.
Clear	Click this link to clear information on this page.
Display Mode	There are two modes for you to choose. Stop record when fulls - when the capacity of syslog is full, the system will stop recording. Always record the new event - only the newest events will be recorded by the system.
Time	Display the time of the event occurred.
Message	Display the information for each event.

For USB Syslog

This page displays the syslog recorded on the USB storage disk.

Diagnostics >> Syslog Explorer

Web Syslog	USB Syslog
------------	------------

Note:

The syslog will show while the saved syslog file size is over 1MB.

Folder: n/a File: n/a Page: n/a Log Type: n/a

Time	Log Type	Message
------	----------	---------

Available settings are explained as follows:

Item	Description
Time	Display the time of the event occurred.
Log Type	Display the type of the record.
Message	Display the information for each event.

VIII-1-13 IPv6 TSPC Status

IPv6 TSPC status web page could help you to diagnose the connection status of TSPC.

If TSPC has configured properly, the router will display the following page when the user connects to tunnel broker successfully.

Diagnostics >> IPv6 TSPC Status

WAN1	Refresh
TSPC Enabled	
TSPC Connection Status	
Local Endpoint v4 Address :	114.44.54.220
Local Endpoint v6 Address :	2001:05c0:1400:000b:0000:0000:0000:10b9
Router DNS name :	888866666.broker.freenet6.net
Remote Endpoint v4 Address :	81.171.72.11
Remote Endpoint v6 Address :	2001:05c0:1400:000b:0000:0000:0000:10b8
Tspc Prefix :	2001:05c0:1502:0d00:0000:0000:0000:0000
Tspc Prefixlen :	56
Tunnel Broker :	amsterdam.freenet6.net
Tunnel Status :	Connected

Available settings are explained as follows:

Item	Description
Refresh	Click this link to refresh this page manually.

VIII-1-14 DoS Flood Table

This page can display content of IP connection detected by DoS Flooding Defense mechanism. It is useful and convenient for network engineers (e.g., MIS engineer) to inspect the network environment to find out if there is any abnormal connection.

Information of IP traced and destination port used for SYN Flood, UDP Flood and ICMP Flood attacks will be detected and shown respectively on different pages.

Moreover, IP address detected and suspected to attack the network system can be blocked shortly by clicking the **Block** button shown on pages of SYN Flood, UDP Flood and ICMP Flood.

Diagnostics >> DoS Flood Table

IPv4

SYN Flood	UDP Flood	ICMP Flood	White/Black IP List	Refresh
Tracing IP		Destination Port		
-----		-----		
192.168.1.22	80		<input type="button" value="Block"/>	
192.168.1.205	40005(⊗)		<input type="button" value="Block"/>	

IPv6

SYN Flood	UDP Flood	ICMP Flood	White/Black IP List	Refresh
Tracing IP		Destination Port		
-----		-----		



Info

The icon - (⊗) - means there is something wrong (e.g., attacking the system) with that IP address.

However, if an IP address is confirmed to be blocked due to its abnormal behavior, click the **Blocking IP List** tab to block it forever. For example, IP address "192.168.1.123" (displayed on the following web page) will be blocked forever.

Diagnostics >> DoS Flood Table

IPv4

| [Refresh](#) |

White Passing IP List:

Black Blocking IP List:

IPv6

| [Refresh](#) |

White Passing IP List:

Black Blocking IP List:

Available settings are explained as follows:

Item	Description
White Passing IP List / Black Blocking IP List	Type the IP address in this field and click Add . It will be added to the IP List and appear in the right frame. IP list in the right frame will be blocked by Vigor system permanently. Remove - It is used to remove selected IP address from the Blocking IP List.
Refresh	Click this link to refresh current page.

VIII-1-15 Route Policy Diagnosis

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

Diagnostics >> Route Policy Diagnosis

Test how the packets will be routed

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

Packet Information

Protocol

Src IP

Dst IP

Dst Port

Analyze

Available settings are explained as follows:

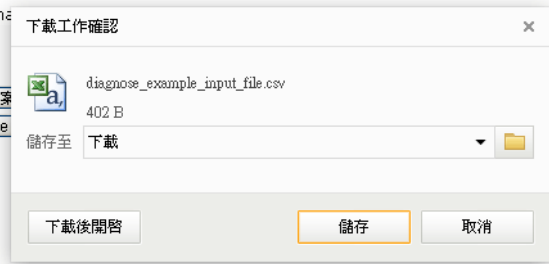
Item	Description
Mode	<p>Analyze a single packet - Choose such mode to make Vigor router analyze how a single packet will be sent by a route policy.</p> <p>Analyze multiple packets... - Choose such mode to make Vigor router analyze how multiple packets in a specified file will be sent by a route policy.</p>
Packet Information	<p>Specify the nature of the packets to be analyzed by Vigor router.</p> <p>ICMP/UDP/TCP/ANY- Specify a protocol for diagnosis.</p> <p>Src IP - Type an IP address as the source IP.</p> <p>Dst IP - Type an IP address as the destination IP.</p> <p>Dst Port - Use the drop down list to specify the destination port.</p> <p>Analyze - Click it to perform the job of analyzing. The analyzed result will be shown on the page..</p>
Input File	<p>It is available when Analyze multiple packets.. is selected as Mode.</p> <p>Select - Click the download link to get a blank example file. Then, click such button to select that blank “.csv” file for saving the result of analysis.</p>

Mode

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

Input File

選擇檔案
Analyze



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

Load Balance/Route Policy >> Diagnose

Mode

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

Input File

選擇檔案 未選擇檔案 (download an example input file)

Analyze

Analysis export analysis

Profile	Input Packet Information			Matched Route		Matched Policy			Final Result		
	Proto	Src IP	Dst IP	Route	Priority	Policy	Priority	Forwarded	Interface	Reason	
LA-branch	ICMP	192.168.1.10	10.10.10.10	N/A	No Match	N/A	No Match	N/A	N/A	N/A	The packet was dropped because neither "route" or "policy" was matched
NI-branch	TCP	192.168.1.20	20.20.20.20	SD60	No Match	N/A	No Match	N/A	N/A	N/A	The packet was dropped because neither "route" or "policy" was matched
											The packet was dropped

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

VIII-2 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

1. Check the power line and WLAN/LAN cable connections. Refer to “I-2 Hardware Installation” for details.
2. Turn on the router. Make sure the **Activity LED** blink once per second and the correspondent **LAN LED** is bright.



3. If not, it means that there is something wrong with the hardware status. Simply back to “I-2 Hardware Installation” to execute the hardware installation again. And then, try again.

VIII-3 Checking If the Network Connection Settings on Your Computer Is OK or Not

Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is still failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows



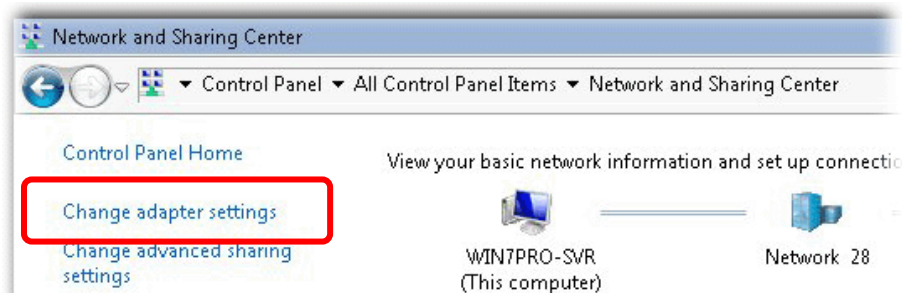
Info

The example is based on Windows 7. As to the examples for other operation systems, please refer to the similar steps or find support notes in www.DrayTek.com.

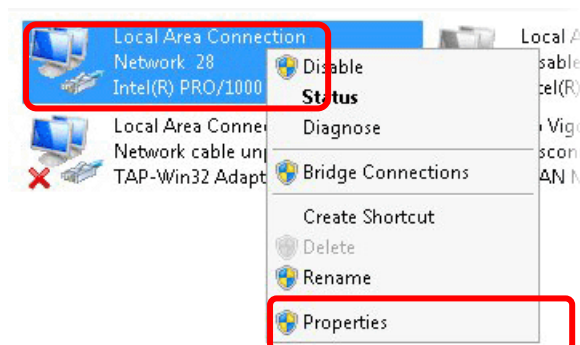
1. Open **All Programs>>Getting Started>>Control Panel**. Click **Network and Sharing Center**.



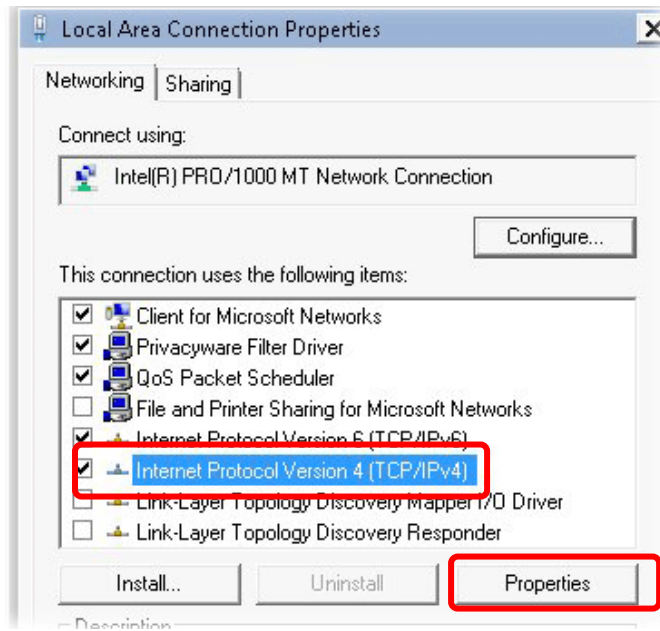
2. In the following window, click **Change adapter settings**.



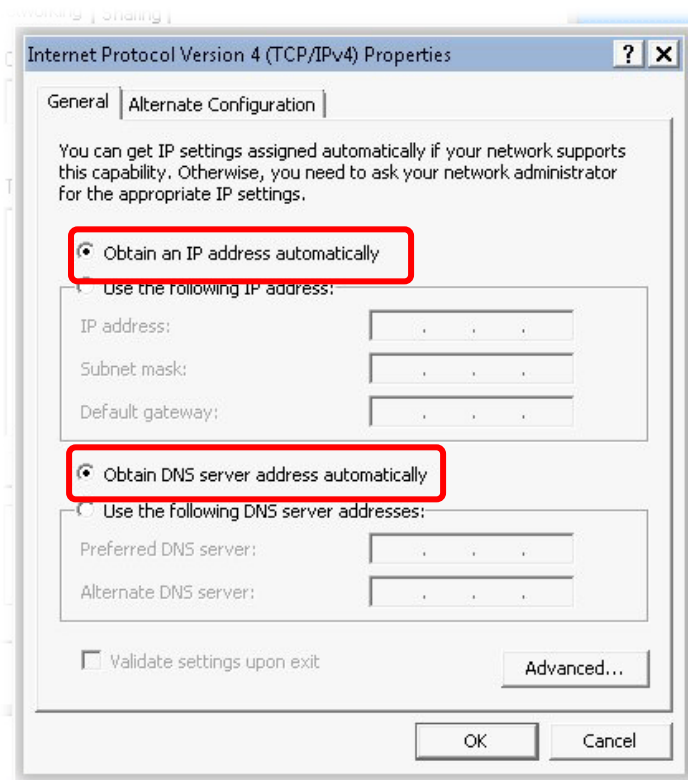
3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



4. Select **Internet Protocol Version 4 (TCP/IP)** and then click **Properties**.

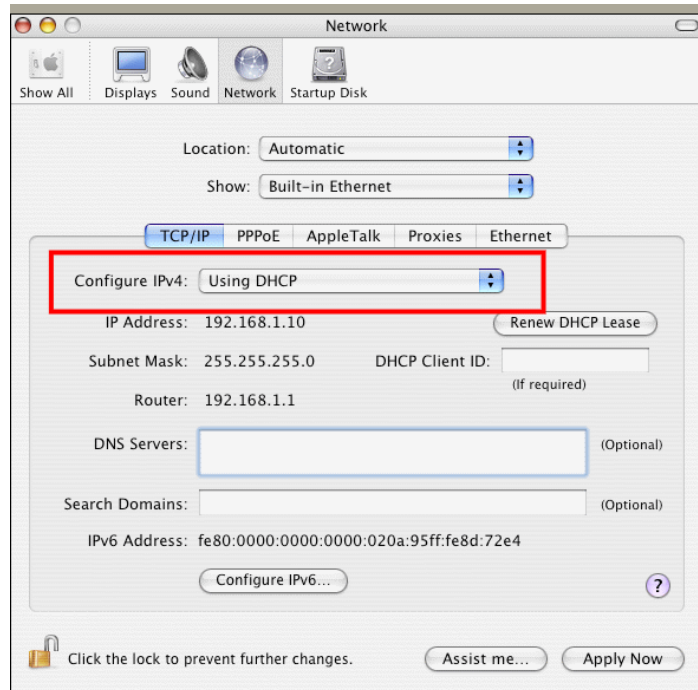


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



For Mac OS

1. Double click on the current used Mac OS on the desktop.
2. Open the **Application** folder and get into **Network**.
3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.



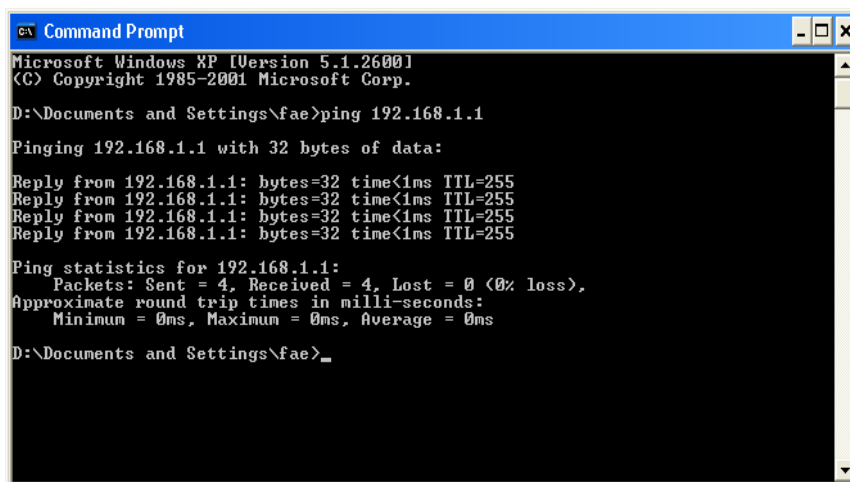
VIII-4 Pinging the Router from Your Computer

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use “ping” command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as get IP automatically. (Please refer to the previous section IX-3)

Please follow the steps below to ping the router correctly.

For Windows

1. Open the **Command Prompt** window (from **Start menu**> **Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista/7). The DOS command dialog will appear.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fae>_
```

3. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of “Reply from 192.168.1.1:bytes=32 time<1ms TTL=255” will appear.
4. If the line does not appear, please check the IP address setting of your computer.

For Mac OS (Terminal)

1. Double click on the current used MacOs on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of “64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms” will appear.

```
Terminal - bash - 80x24
Last login: Sat Jan  3 02:24:18 on ttys1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$
```

VIII-5 Checking If the ISP Settings are OK or Not

If WAN connection cannot be up, check if the LEDs (according to the LED explanations listed on section 1.2) are correct or not. If the LEDs are off, please:

- Change the **Physical Type** from **Auto negotiation** to other values (e.g., 100M full duplex).
- Next, 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 to review the settings that you configured previously.

VIII-6 Backing to Factory Default Setting If Necessary

Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware. Such function is available in **Admin Mode** only.



Info

After pressing factory default setting, you will lose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null.

Software Reset

You can reset the router to factory default via Web page. Such function is available in **Admin Mode** only.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **Reboot Now**. After few seconds, the router will return all the settings to the factory settings.

System Maintenance >> Reboot System

Reboot System

Do you want to reboot your router ?

- Using current configuration
 Using factory default configuration

Reboot Now

Auto Reboot Time Schedule

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

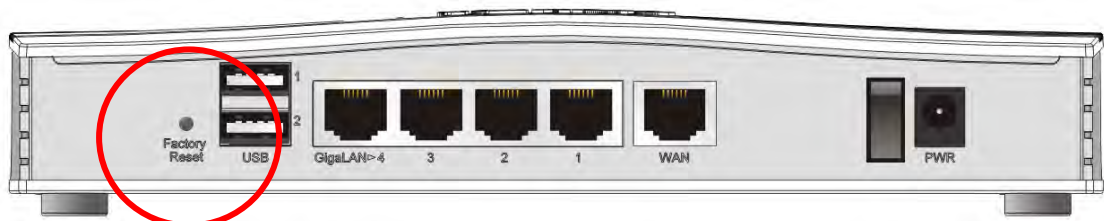
Note: Action and Idle Timeout settings will be ignored.

OK

Cancel

Hardware Reset

While the router is running (ACT LED blinking), press the **Factory Reset** button and hold for more than 5 seconds. When you see the **ACT LED** blinks rapidly, please release the button. Then, the router will restart with the default configuration.



After restore the factory default setting, you can configure the settings for the router again to fit your personal request.

VIII-7 Contacting DrayTek

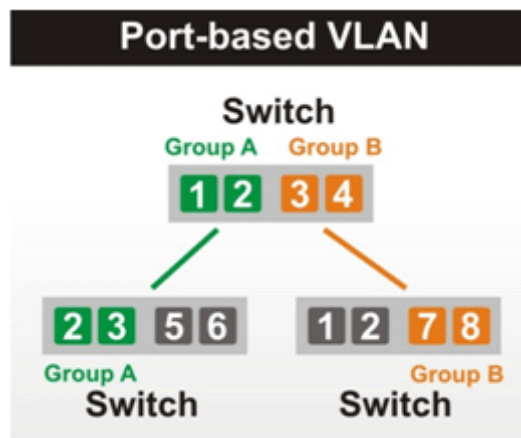
If the router still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@DrayTek.com.

Appendix I: VLAN Applications on Vigor Router

Virtual Local Area Network is so-called VLAN. It offers the logical grouping technique to separate the physical ports of Ethernet switches, thus we can manage our local network easier, more flexible and secure. For instance, you're a networking administrator in your company and you're planning to isolate the visitors' traffics from your private network for security considerations because you cannot ensure that visitors' computer is clean. Or you want to separate your private network into several parts by divisions because there are too many computers in the same network segment and it results in the local traffics heavily. VLAN helps you to solve these situations, and DrayTek's products support bellow two popular types:

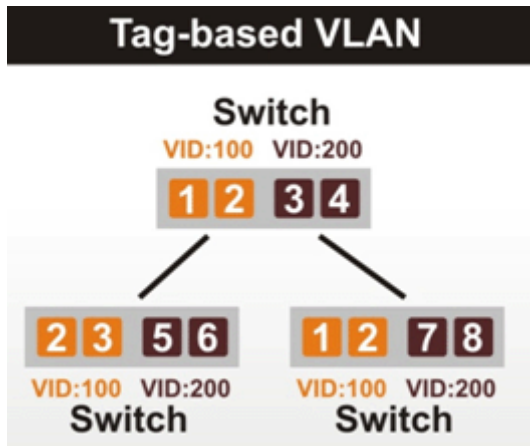
Port-based

It uses a matrix table of the physical ports to define the traffics how to exchange between each port, and the traffics will be isolated from the ports are not being ticked in the same line. It is the easiest way to setup an isolate network, but not a flexible way to maintain a growing network. Because the idea of port-based VLAN is grouping by physical ports, but the difficulty is how to handle the traffics between two or more Ethernet switches. Thus, VLAN is suitable for some circumstances, for example, the rental apartment, SOHO office...and so on. These clients may need two or three isolated networks only and setup a network in a simple way.



Tag-based

The idea of tag-based VLAN is to identify a virtual LAN with a specific ID, therefore, **VLAN ID** introduced by tag-based VLAN. Through VLAN ID, ports with different **VID (VLAN ID)** will be identified as in different LANs, so the traffics also will be isolated from each of VLANs. Many administrators who manage an enterprise network or even the internet service providers (ISP) adopt Tag-based VLAN popularly because it is convenient to maintain and manage a distributed network. Setting a large-scale network is easy by giving each of them with different VID and isolating the traffics at the same time. Besides the VLAN ID, there is another feature, **Trunk**, introduced. While the role of a port on an Ethernet switch is setup as a Trunk port, it means the VLAN ID will be kept while forwarding the packets between switches. By this feature, VLANs are able to distribute over two or more Ethernet switches easily, moreover design a large and secured network is possible through Trunk port. When VLAN is being enabled on Vigor routers, the LAN ports are being turned into Trunk mode automatically. Therefore, a VLAN supported switch, like VigorSwitch G2260/P2261, or VigorSwitch G1240, is needed.



Vigor routers ^[Note] support Tag-based feature both on LAN and WAN interfaces. The next we'll demonstrate our web design and how to configure the settings by introducing the functionalities of Vigor router.

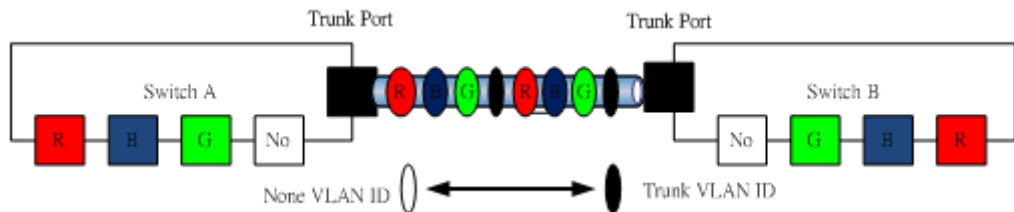
[Note]

Broadband router: Vigor2920/Vigor3200/Vigor2133/Vigo2960/Vigor3900

Modem router: Vigor2850/Vigor2133

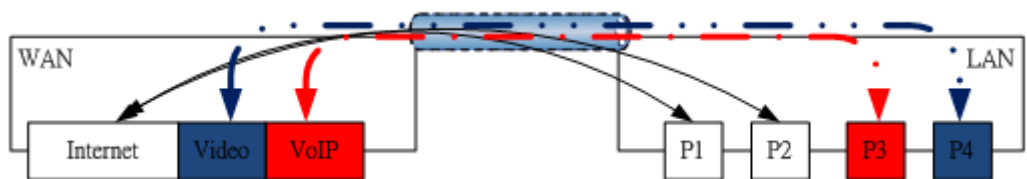
VLAN Packets on Vigor routers

Trunk mode of LAN



Trunk Port can carry the packets with VID but replace the Non-VID packet as the VID of Trunk port while forwarding the packets to another switch.

Bridge mode of WAN



P1 and P2 are doing NAT flow to access to the internet, but P3 and P4 will forward the packets between WAN and LAN ports directly.

Web User Interface

So far, there are two kinds of open system on Vigor router. One is DrayOS, which is DrayTek owned, and another is Linux-like which customized by DrayTek from OpenWRT. Here DrayOS system is going to be introduced to you because it is the most stable and superfast booting system in DrayTek products. If the UI style of yours is different from the following. It may not DrayOS system with new web style or maybe the Linux-like model.

WAN

Multi-VLAN

General

Channel	Enable	WAN Type	VLAN Tag	Port-based Bridge
1	Yes	Ethernet(WAN1)	None	
2	Yes	Ethernet(WAN2)	None	
3	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
4	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
5_WAN5	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
6_WAN6	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
7_WAN7	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
8	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5

Detail settings of channel profile

Multi-VLAN Channel 5: Enable Disable
 WAN Type : Ethernet(WAN1)

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

Open Port-based Bridge Connection for this Channel
 Physical Members
 P1 P2 P3 P4 P5
 Note:3.P1 is reserved for NAT use,and cannot be configured for bridge mode.

Open WAN Interface for this Channel
 WAN for Router-borne Application: Management
 WAN Setup: Static or Dynamic IP

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

VLAN Settings

VLAN Members

Service Binding & WAN Setup

LAN

Enable *Port-based VLAN* by checking the option

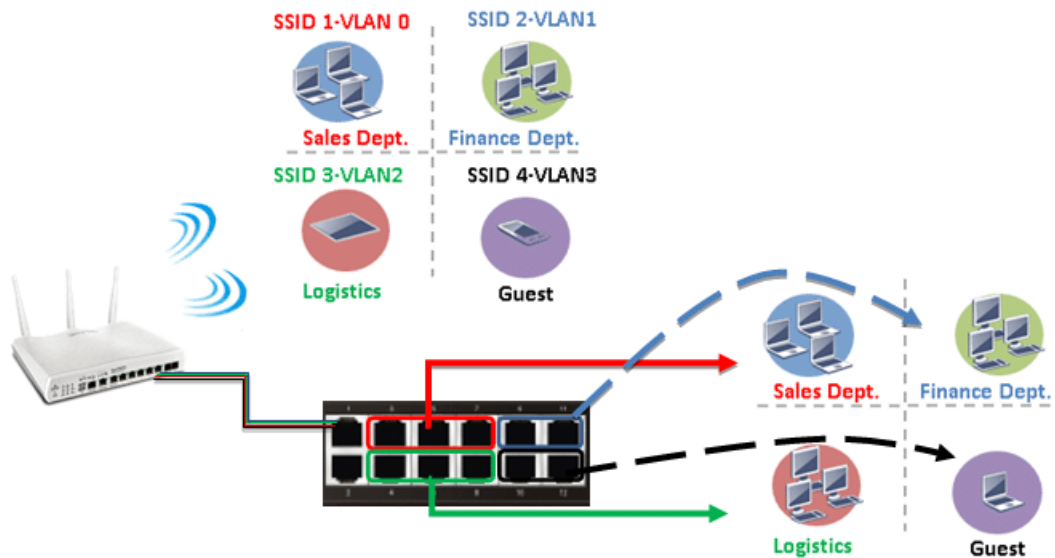
The option of *Tag-based VLAN*

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

Member of *Port-based* or *Tag-based VLAN* | DHCP Pool will be used | VLAN ID assigned | 802.1p field

VLAN applications on Vigor router

- Multi Subnet (VLAN of LAN)



Port-based mode

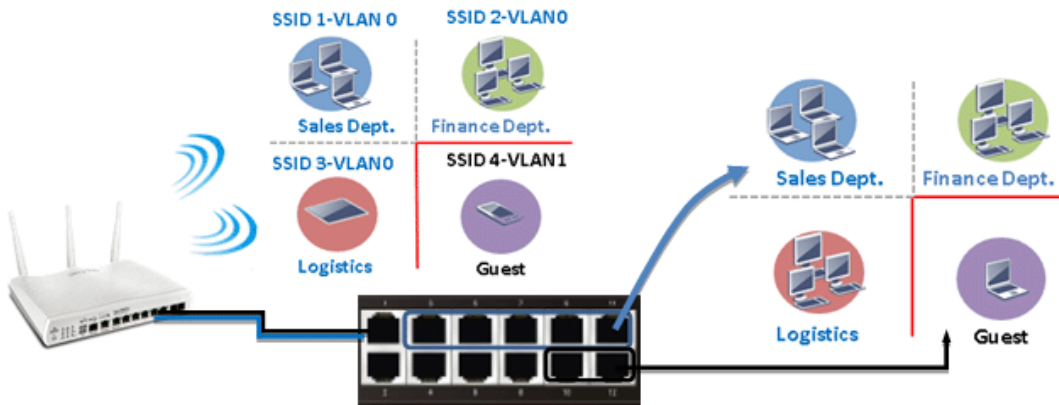
	LAN				Wireless LAN				VLAN Tag			
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
VLAN0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 2	<input type="checkbox"/>	0	0
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	LAN 3	<input type="checkbox"/>	0	0
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	LAN 4	<input type="checkbox"/>	0	0
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0

Tag-based mode

	LAN				Wireless LAN				VLAN Tag			
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
VLAN0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input checked="" type="checkbox"/>	10	0
VLAN1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 2	<input checked="" type="checkbox"/>	20	0
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	LAN 3	<input checked="" type="checkbox"/>	30	0
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	LAN 4	<input checked="" type="checkbox"/>	40	0
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0

By above settings, there are four private networks will be created and computers attached with each of LAN ports or SSIDs which are able to obtain a private IP address from each DHCP server (LAN1/LAN2/LAN3/LAN4). However, the traffics of the LAN port or SSID that are NOT being grouped in the same VLAN are unable to forward to each other. The benefit of Port-based is able to extend the wired ports by installing a cheaper dumb switch as many as you need, but Tag-based offers you a flexible and well-managed network. The networks are isolated, secured and reduce the broadcasting storm effectively in each of networks with VLAN.

- Guest Network



Port-based mode

VLAN Configuration

Enable

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

Tag-based mode

VLAN Configuration

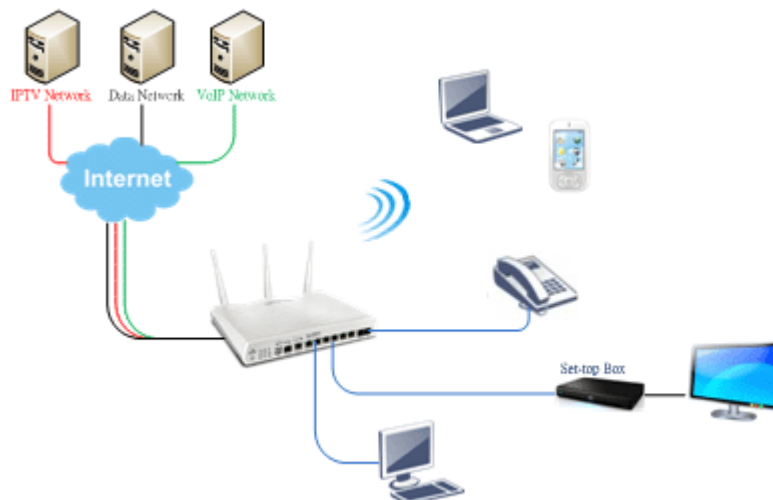
Enable

	LAN				Wireless LAN				Subnet	VLAN Tag		
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4		Enable	VID	Priority
VLAN0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	LAN 2	<input checked="" type="checkbox"/>	10	0
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0

To deploy a guest network, which serves your guests the internet accessibility, but the traffics have to be isolated from your private network due to the security considerations, it can be done by above settings. However, a switch support VLAN function is need if VLAN Tag enabled.

- Triple Play (Multi-WAN)

NAT mode with VLAN



Following settings, the set-top box (STB) is able to attach with any LAN port. Video streaming which your ISP provided will be played on your monitor.

WAN 1

Enable: Yes No

Display Name:

Physical Mode: Ethernet

Physical Type: Auto negotiation

Line Speed(Kbps):

DownLink:

UpLink:

VLAN Tag insertion: Enable Disable (Please configure Internet Access setting first)

Tag value: (0~4095)

Priority: (0~7)

Active Mode: Always On Load Balance:

1. Setup the VLAN ID on WAN1 profiles if WAN is the primary interface of IPTV service.

2. Open the profile of WAN5 by clicking the ID.

Channel	Enable	WAN Type	VLAN Tag	Port-based Bridge
1	Yes	Ethernet(WAN1)	None	
2	Yes	Ethernet(WAN2)	None	
3	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
4	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
5. WAN5	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
6. WAN6	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
7. WAN7	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
8	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4

Multi-VLAN Channel 5: Enable Disable

WAN Type: Ethernet(WAN1)

General Settings

VLAN Header

VLAN Tag:

Priority:

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

P1 P2 P3 P4 P5

Note: 3. P1 is reserved for NAT use, and cannot be configured for bridge mode.

Open Port-based Bridge Connection for this Channel

Physical Members

P1 P2 P3 P4 P5

Note: 3. P1 is reserved for NAT use, and cannot be configured for bridge mode.

3. Setup connection of WAN 5 and bind the service onto it.

NO need to enable Port-based Bridge.

P1 P2 P3 P4 P5

Note: 3. P1 is reserved for NAT use, and cannot be configured for bridge mode.

Open WAN interface for this Channel

WAN for Router-borne Application: IPTV

WAN Setup: Static or Dynamic IP

ISP Access Setup

ISP Name:

Username:

Password:

PPP Authentication: PAP or CHAP

Always On

Idle Timeout: second(s)

IP Address From ISP

Fixed IP (Dynamic IP): Yes No

Fixed IP Address:

WAN IP Network Settings

Obtain an IP address automatically

Router Name: Vigor

Domain Name:

*: Required for some ISPs

Specify an IP address

IP Address:

Subnet:

Mask:

Gateway IP Address:

DNS Server IP Address

Primary IP Address: 8.8.8.8

Secondary IP Address: 8.8.4.4

4. Go to Application >> IGMP to bind it on PVC WAN.

IGMP

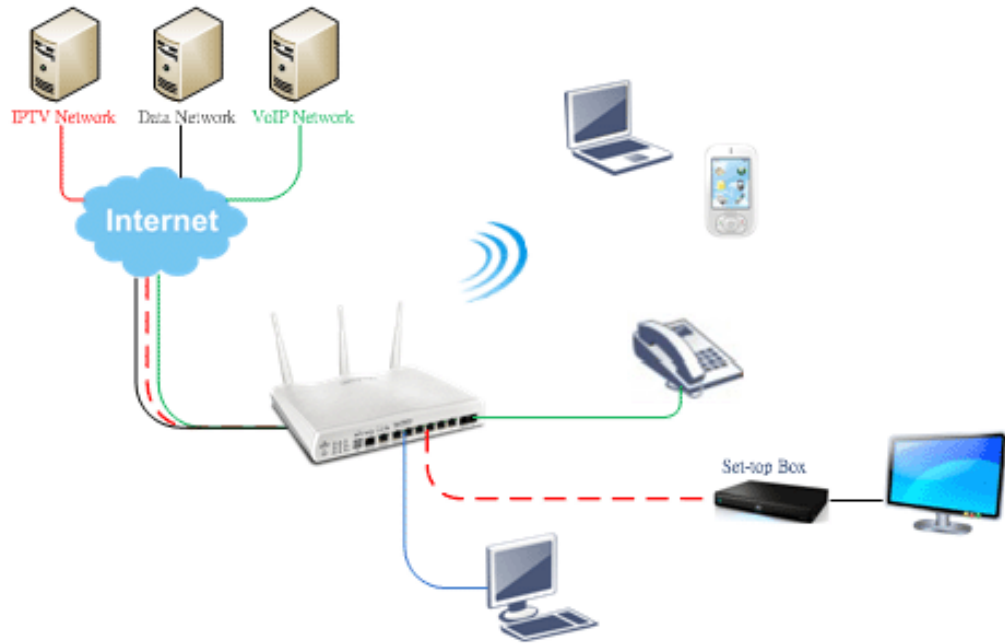
Enable IGMP Proxy PVC

IGMP Proxy is to act as a multicast proxy for will access any multicast group. But this function take no effect when bridge mode is enable.

Enable IGMP Snooping

Enable IGMP Snooping, multicast traffic is only forwarded to ports that have members of that group. Disable IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic.

Bridge mode with VLAN



Multi-VLAN

General				
Channel	Enable	WAN Type	VLAN Tag	Port-based Bridge
1	Yes	Ethernet(WAN1)	None	
2	Yes	Ethernet(WAN2)	None	
3	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
4	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
5	No			
6	No			
7	No			
8	No			

Multi-VLAN Channel 3: Enable Disable

WAN Type :

General Settings

VLAN Header

VLAN Tag:

Priority:

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

Bridge mode

Enable

Physical Members

P1 P2 P3 P4 P5

Note:3.P1 is reserved for NAT use,and cannot be configured for bridge mode.

Set-top box (STB) or the other kinds of media devices are able to attach with Port4 or Port5 of LAN. Those devices that attached with Port4 or Port5 are able to access the services network directly which your ISP provided.

This page is left blank.

Part IX Telnet Commands

Accessing Telnet of Vigor2133

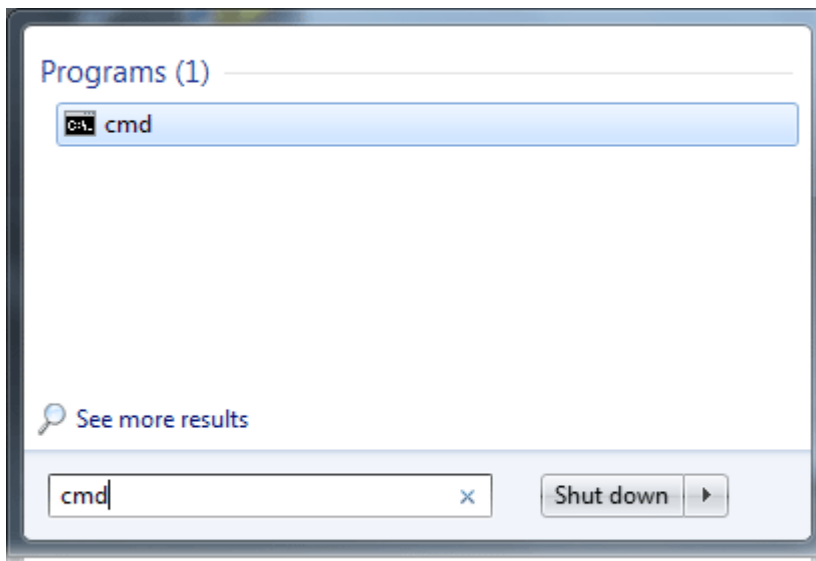
This chapter also gives you a general description for accessing telnet and describes the firmware versions for the routers explained in this manual.



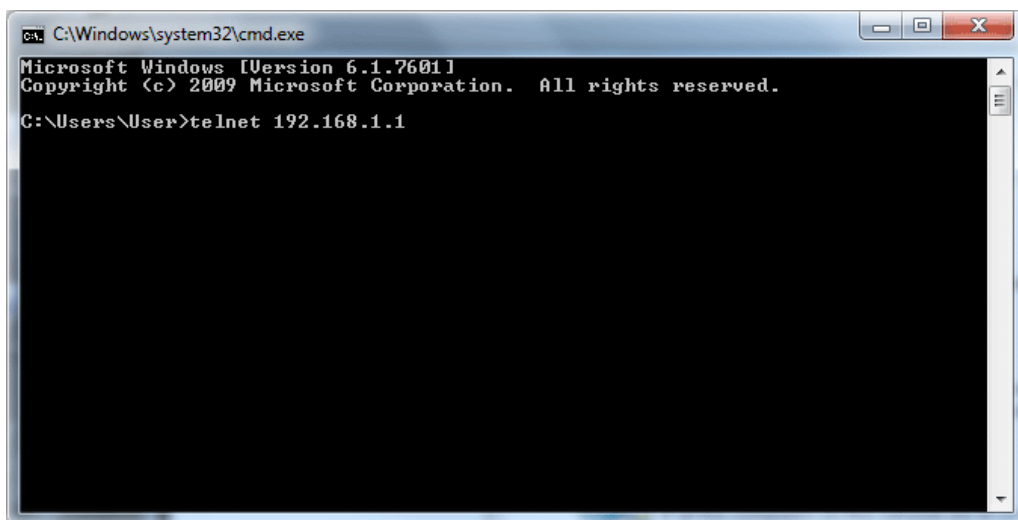
Info

For Windows 7 user, please make sure the Windows Features of Telnet Client has been turned on under Control Panel>>Programs.

Type cmd and press Enter. The Telnet terminal will be open later.

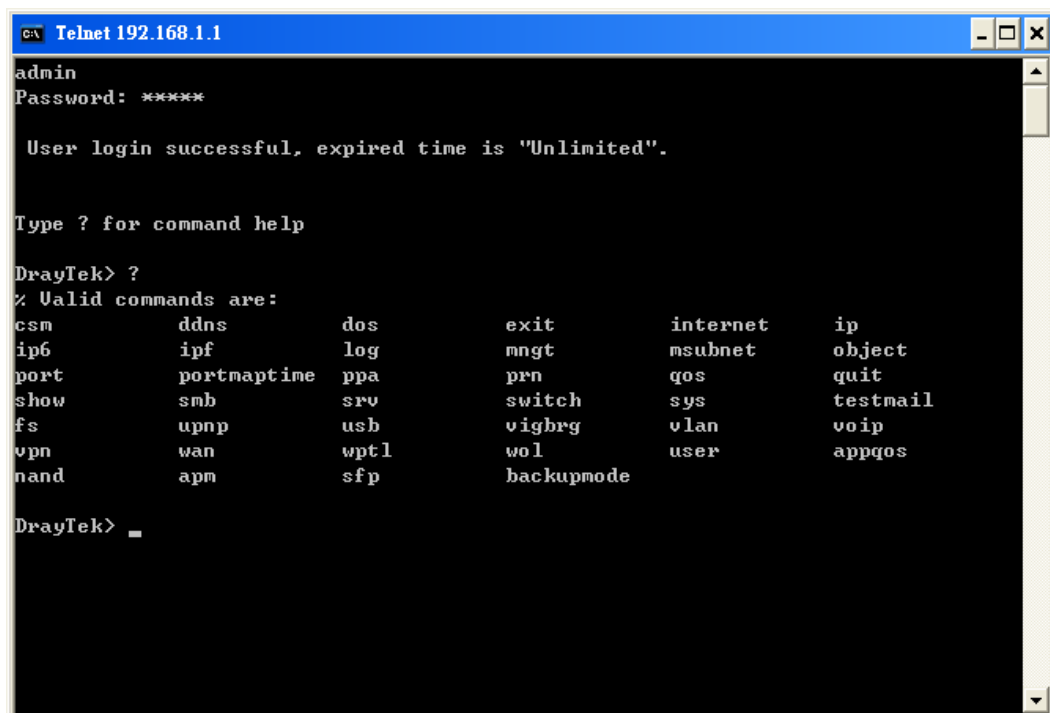
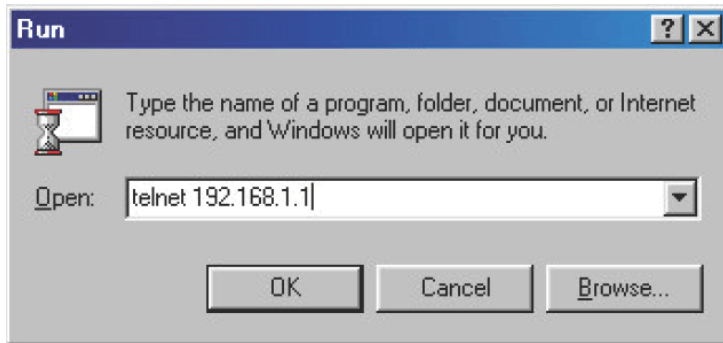


In the following window, type Telnet 192.168.1.1 as below and press Enter. Note that the IP address in the example is the default address of the router. If you have changed the default, enter the current IP address of the router.



Next, type admin/admin for Account/Password. Then, type ?. You will see a list of valid/common commands depending on the router that your use.

For users using previous Windows system (e.g., 2000/XP), simply click **Start >> Run** and type **Telnet 192.168.1.1** in the Open box as below. Next, type **admin/admin** for Account/Password. And, type **?** to get a list of valid/common commands.



Telnet Command: csm appe prof

Commands under CSM allow you to set CSM profile to define policy profiles for different policy of IM (Instant Messenger)/P2P (Peer to Peer) application.

“csm appe prof “ is used to configure the APP Enforcement Profile name. Such profile will be applied in Default Rule of Firewall>>General Setup for filtering.

Syntax

```
csm appe prof -i INDEX [-v | -n NAME|setdefault]
```

Syntax Description

Parameter	Description
<i>INDEX</i>	It means to specify the index number of CSM profile, from 1 to 32.
-v	It means to view the configuration of the CSM profile.
-n	It means to set a name for the CSM profile.
<i>NAME</i>	It means to specify a name for the CSM profile, less than 15 characters.
<i>setdefault</i>	Reset to default settings.

Example

```
> csm appe prof -i 1 -n games
The name of APPE Profile 1 was setted.
```

Telnet Command: csm appe set

It is used to configure group settings for IM/P2P/Protocol and Others in APP Enforcement Profile.

```
csm appe set -i INDEX [-v GROUP| -e AP_IDX | -d AP_IDX]
```

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.
<i>GROUP</i>	Specify the category of the application. Available options are: IM, P2P, Protocol and Others.
<i>AP_IDX</i>	Each application has independent index number for identification in CLI command. Specify the index number of the application here. If you have no idea of the index number, do the following (Take IM as an example): Type “csm appe set -i 1 -v IM”, the system will list all of the index numbers of the applications categorized under IM.

Example

```
> csm appe set -i 1 -e 1
Profile 1 - : AIM is enabled.
```

Telnet Command: csm appe show

It is used to display group (IM/P2P/Protocol and Others) information APP Enforcement Profile.
 csm appe show [-a/-i/-p/-t/-m]

Syntax Description

Parameter	Description
-a	View the configuration status for All groups.
-i	View the configuration status of IM group.
-p	View the configuration status of P2P group.
-t	View the configuration status of protocol group.
-m	View the configuration status of Others group.

Example

```
>csm appe show -t

      Type      Index      Name      Version  Advance
Advanced Option: (M)essage, (F)ile Transfer, (G)ame, (C)onference, and (O)ther
Activities
-----
      PROTOCOL   52      DB2
      PROTOCOL   53      DNS
      PROTOCOL   54      FTP
      PROTOCOL   55      HTTP      1.1
      PROTOCOL   56      IMAP      4.1
      PROTOCOL   57      IMAP STARTTLS 4.1
      PROTOCOL   58      IRC      2.4.0      .....
```

Telnet Command: csm appe config

It is used to display the configuration status (enabled or disabled) for IM/P2P/Protocol/Other applications.

csm appe config -v INDEX [-i/-p/-t/-m]

Syntax Description

Parameter	Description
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.

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).

csm appe email [-e/-d/-s]

Syntax Description

Parameter	Description
-e	Enable notification e-mail mechanism.
-d	Disable notification e-mail mechanism.
-s	Send an example e-mail.

Example

```
> csm appe email -e
Enable APPE email.
```

Telnet Command: csm ucf

It is used to configure settings for URL control filter profile.

Syntax

csm ucf show

csm ucf setdefault

csm ucf msg *MSG*

csm ucf obj *INDEX* [-n *PROFILE_NAME* | -I [*P|B|A|N*] | *uac* | *wf*]

csm ucf obj *INDEX* -n *PROFILE_NAME*

csm ucf obj *INDEX* -p *VALUE*

csm ucf obj *INDEX* -I *P|B|A|N*

csm ucf obj *INDEX* *uac*

csm ucf obj *INDEX* *wf*

Syntax Description

Parameter	Description
<i>show</i>	It means to display all of the profiles.
<i>setdefault</i>	It means to return to default settings for all of the profile.
<i>msg MSG</i>	It means de set the administration message. MSG means the content (less than 255 characters) of the message itself.
<i>obj</i>	It means to specify the object for the profile.
<i>INDEX</i>	It means to specify the index number of CSM profile, from 1 to 8.
-n	It means to set the profile name.
<i>PROFILE_NAME</i>	It means to specify the name of the profile (less than 16 characters)
-p	Set the priority (defined by the number specified in VALUE) for the profile.

<i>VALUE</i>	Number 0 to 3 represent different conditions. 0: It means Bundle: Pass. 1: It means Bundle: Block. 2: It means Either: URL Access Control First. 3: It means Either: Web Feature First.
<i>-l</i>	It means the log type of the profile. They are: P: Pass, B: Block, A: All, N: None
<i>uac</i>	It means to set URL Access Control part.
<i>wf</i>	It means to set Web Feature part.

Example

```
> csm ucf obj 1 -n game -l B
Profile Index: 1   Profile Name:[game]
```

Telnet Command: csm ucf obj INDEX uac

It means to configure the settings regarding to URL Access Control (uac).

Syntax

`csm ucf obj INDEX uac -v`

`csm ucf obj INDEX uac -e`

`csm ucf obj INDEX uac -d`

`csm ucf obj INDEX uac -a P/B`

`csm ucf obj INDEX uac -i E/D`

`csm ucf obj INDEX uac -o KEY_WORD_Object_Index`

`csm ucf obj INDEX uac -g KEY_WORD_Group_Index`

Syntax Description

Parameter	Description
<i>INDEX</i>	It means to specify the index number of CSM profile, from 1 to 8.
<i>-v</i>	It means to view the protocol configuration of the CSM profile.
<i>-e</i>	It means to enable the function of URL Access Control.
<i>-d</i>	It means to disable the function of URL Access Control.
<i>-a</i>	Set the action of specific application, P or B. B: Block. The web access meets the URL Access Control will be blocked. P: Pass. The web access meets the URL Access Control will be passed.
<i>-i</i>	Prevent the web access from any IP address. E: Enable the function. The Internet access from any IP address will be blocked. D: Disable the function.
<i>-o</i>	Set the keyword object.

<i>KEY_WORD_Object_Index</i>	Specify the index number of the object profile.
<i>-g</i>	Set the keyword group.
<i>KEY_WORD_Group_Index</i>	Specify the index number of the group profile.

Example

```

> csm ucf obj 1 uac -i E
Log:[none]
Priority Select : [Bundle : Pass]
-----
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:[none]
Priority Select : [Bundle : Pass]
-----
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: csm ucf obj INDEX wf

It means to configure the settings regarding to Web Feature (wf).

Syntax

csm ucf obj *INDEX wf -v*

csm ucf obj *INDEX wf -e*

csm ucf obj *INDEX wf -d*

csm ucf obj *INDEX wf -a P/B*

csm ucf obj *INDEX wf -s WEB_FEATURE*

csm ucf obj *INDEX wf -u WEB_FEATURE*

csm ucf obj *INDEX wf -f File_Extension_Object_index*

Syntax Description

Parameter	Description
<i>INDEX</i>	It means to specify the index number of CSM profile, from 1 to 8.
<i>-v</i>	It means to view the protocol configuration of the CSM profile.
<i>-e</i>	It means to enable the restriction of web feature.
<i>-d</i>	It means to disable the restriction of web feature.
<i>-a</i>	Set the action of web feature, P or B. B: Block. The web access meets the web feature will be blocked. P: Pass. The web access meets the web feature will be passed.
<i>-s</i>	It means to enable the the Web Feature configuration. Features available for configuration are: c: Cookie p: Proxy u: Upload
<i>-u</i>	It means to cancel the web feature configuration.
<i>-f</i>	It means to set the file extension object index number.
<i>File_Extension_Object_index</i>	Type the index number (1 to 8) for the file extension object.

Example

```
> csm ucf obj 1 wf -s c
-----
Web Feature
[ ]Enable Restrict Web Feature   Action:[pass]

File Extension Object Index : [0] Profile Name : []

[V] Cookie [ ] Proxy [ ] Upload
```

Telnet Command: csm wcf

It means to configure the settings regarding to web control filter (wcf).

Syntax

csm wcf show

csm wcf look

csm wcf cache
 csm wcf server WCF_SERVER
 csm wcf msg MSG
 csm wcf setdefault
 csm wcf obj *INDEX* -v
 csm wcf obj *INDEX* -a P/B
 csm wcf obj *INDEX* -n PROFILE_NAME
 csm wcf obj *INDEX* -I N/P/B/A
 csm wcf obj *INDEX* -o KEY_WORD Object Index
 csm wcf obj *INDEX* -g KEY_WORD Group Index
 csm wcf obj *INDEX* -w E/D/P/B
 csm wcf obj *INDEX* -s CATEGORY|WEB_GROUP
 csm wcf obj *INDEX* -u CATEGORY|WEB_GROUP

Syntax Description

Parameter	Description
<i>show</i>	It means to display the web content filter profiles.
<i>Look</i>	It means to display the license information of WCF.
<i>Cache</i>	It means to set the cache level for the profile.
<i>Server WCF_SERVER</i>	It means to set web content filter server.
<i>Msg MSG</i>	It means de set the administration message. MSG means the content (less than 255 characters) of the message itself.
<i>setdefault</i>	It means to return to default settings for all of the profile.
<i>obj</i>	It means to specify the object profile.
<i>INDEX</i>	It means to specify the index number of web content filter profile, from 1 to 8.
- v	It means to view the web content filter profile.
-a	Set the action of web content filter profile, P or B. B: Block. The web access meets the web feature will be blocked. P: Pass. The web access meets the web feature will be passed.
-n	It means to set the profile name.
<i>PROFILE_NAME</i>	It means to specify the name of the profile (less than 16 characters)
-I	It means the log type of the profile. They are: P: Pass, B: Block, A: All, N: None
-o	Set the keyword object.
<i>KEY_WORD_Object_Index</i>	Specify the index number of the object profile.
-g	Set the keyword group.
<i>KEY_WORD_Group_Index</i>	Specify the index number of the group profile.
-w	It means to set the action for the black and white list. E: Enable, D: Disable,

	P:Pass, B:Block
-s	It means to choose the items under CATEGORY or WEB_GROUP.
-u	It means to discard items under CATEGORY or WEB_GROUP.
WEB_GROUP	Child_Protection, Leisure, Business, Chating, Computer Internet, Other
CATEGORY	Includes: Alcohol & Tobacco, Criminal Activity, Gambling, Hate & Intoleranc, Illegal Drug, Nudity, Pornography/Sexually Explicit, Weapons, Violence, School Cheating,Sex Education, Tasteless, Child Abuse Imges, Entertainment, Games, Sports, Travel, Leisure & Recreation, Fashin & Beauty, Business, Job Search, Web-based Emai, Chat, Instant Messaging, Anonymizers, Forums & Newsgroups, Computers & Technology, Download Sites, Streaming Media & Downloads, Phishing & Fraud, Search Engines & Portals, Social Networking, Spam Sites,Malware, Botnets, Hacking, Illegal Software, Information Security,Peer-to-eer, Advertisements & Pop-Ups, Arts, Transportation, Compromised, Dating & Personals, , Education, Finance, Government,Health & Medcine, News, Non-profits & NGOs, Personal Sites,Politics, Real Estate, Rligion, Restaurants & Dining,Shopping, Translators, General, Cults,Greetig cards, Image Sharing, Network Errors, Parked Domains, Private IP Addresses)

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 -I 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 [value]
```

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>	set WCF for DNS Filter Local Setting
<i>ucf [INDEX]</i>	set UCF for DNS Filter Local Setting
<i>service WCF_PROFILE</i>	WCF_PROFILE: Specify a WCF profile as the base of DNS filtering. Type a number to indicate the index number of WCF profile (1 is first profile, 2 is second profile, and so on ...).
<i>cachetime [CACHE_TIME]</i>	CACHE_TIME: It means to set the time for cache to live (available values are 1 to 24; 1 is one hour, 2 is two hours, and so on ...) for DNS filter.
<i>blockpage</i>	DNS sends block page for redirect port. When a web page is blocked by DNS filter, the router system will send a message page to describe that the page is not allowed to be visited. ON: Enable the function of displaying message page. OFF: Disable the function of displaying message page. SHOW: Display the function of displaying message page is ON or OFF.
<i>profile_show</i>	Display the table of the DNS filter profile.
<i>profile_edit</i>	Modify the content of the DNS filter profile.
<i>-n PROFILE_NAME</i>	PROFILE_NAME: Type the name of the DNS filter profile that you want to modify.
<i>-I N P B A</i>	Specify the log type of the profile. P: Pass. B: Block. A: All. N: None.
<i>-w WCF_PROFILE</i>	WCF_PROFILE: Type the index number of the WCF profile.
<i>-u UCF_PROFILE</i>	UCF_PROFILE: Type the index number of the UCF profile.
<i>-c CACHE_TIME</i>	-c means to set the cache time for DNS filter. CACHE_TIME: It means to set the time for cache to live (available values are 1 to 24; 1 is one hour, 2 is two hours, and so on ...) for DNS filter.
<i>local_bw [value]</i>	Enable /disable the Black/White List. e: Enable Black/White List. d: Disable Black/White List. p: Pass action. b: Block action. a [type index][START_IP][END/MASK_IP]: Set address type (0=mask, 1=single, 2=any, 3=range, 4=group). g [item number][group index]: select group index (1 ~ 192) for group and objects type. o [item number][object index]: select object index (1~ 32) for group and objects type. s: show config setting

c: clear config and reset to default setting

Example

```
> csm dnsf enable ON
DNS Filter enable!
> csm dns profile_edit 1 -n Plant_1
Profile Index: 1
Profile Name:[Plant_1]

Log:[none]

WCF Profile Index: 0

UCF Profile Index: 0
```

Telnet Command: ddns log

Displays the DDNS log.

Example

```
>ddns log
>
```

Telnet Command: ddns time

Sets and displays the DDNS time.

Syntax

`ddns time <update in minutes>`

Syntax Description

Parameter	Description
<i>Update in minutes</i>	Type the value as DDNS time. The range is from 1 to 14400.

Example

```
> ddns time
ddns time <update in minutes>
Valid: 1 ~ 1440
%Now: 1440
> ddns time 1000
ddns time <update in minutes>
Valid: 1 ~ 1440
%Now: 1000
```

Telnet Command: dos

This command allows users to configure the settings for DoS defense system.

Syntax

`dos [-V | D | A]`

`dos [-s ATTACK_F [THRESHOLD][TIMEOUT]]`

dos [-a | e [ATTACK_F][ATTACK_0] | d [ATTACK_F][ATTACK_0]]

Syntax Description

Parameter	Description
-V	It means to view the configuration of DoS defense system.
-D	It means to deactivate the DoS defense system.
-A	It means to activate the DoS defense system.
-s	It means to enable the defense function for a specific attack and set its parameter(s).
ATTACK_F	It means to specify the name of flooding attack(s) or portscan, e.g., synflood, udpflood, icmpflood, or postscan.
THRESHOLD	It means the packet rate (packet/second) that a flooding attack will be detected. Set a value larger than 20.
TIMEOUT	It means the time (seconds) that a flooding attack will be blocked. Set a value larger than 5.
-a	It means to enable the defense function for all attacks listed in ATTACK_0.
-e	It means to enable defense function for a specific attack(s).
ATTACK_0	It means to specify a name of the following attacks: ip_option, tcp_flag, land, teardrop, smurf, pingofdeath, traceroute, icmp_frag, syn_frag, unknow_proto, fraggle.
-d	It means to disable the defense function for a specific attack(s).

Example

```
>dos -A
The Dos Defense system is Activated
>dos -s synflood 50 10
Synflood is enabled! Threshold=50 <pke/sec> timeout=10 <pke/sec>
```

Telnet Command: exit

Type this command will leave telnet window.

Telnet Command: Internet

This command allows you to configure detailed settings for WAN connection.

Syntax

internet [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
<command><parameter>[...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-M 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)
-S <isp name>	It means to set ISP Name (max. 23 characters).
-P <on/off>	It means to enable PPPoE Service.
-u <username>	It means to set username (max. 49 characters) for Internet accessing.
-p <password>	It means to set password (max. 49 characters) for Internet accessing.
-a n	It means to set PPP Authentication Type and n means different types (represented by 0-1). n=0: PAP/CHAP (this is default setting) n=1: PAP Only
-t n	It means to set connection duration and n means different conditions. n=-1: Always-on n=1 ~ 999: Idle time for offline (default 180 seconds)
-i <ip address>	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>	It means to assign gateway IP for such WAN connection.
-s <server ip>	Set PPTP/L2TP Server IP. <server ip>= ppp.qqq.rrr.sss: PPTP/L2TP server IP
-A <idx>	Set to Always On mode, and <idx> as backup WAN#.
-B <mode>	Set to Backup mode; <mode> 0: When any WAN disconnect; 1: When all WAN disconnect.
-V	It means to view Internet Access profile.
-C <sim pin code>	Set SIM PIN code (max. 15 characters) for USB PPP mode.
-O <init string>	Set Modem Initial String (max. 47 characters) for USB PPP mode.
-T <init string2>	Set Modem Initial String2 (max. 47 characters) for USB PPP mode.
-D <dial string>	Set Modem Dial String (max. 31 characters) for USB PPP mode.
-v <service name>	Set Service Name (max. 23 characters) for USB PPP mode.
-m <ppp username>	Set PPP Username (max. 63 characters) for USB PPP mode.
-o <ppp password>	Set PPP Password (max. 62 characters) for USB PPP mode.
-e n	Set PPP Authentication Type for USB PPP mode. n= 0: PAP/CHAP (default), 1: PAP Only
-q n	Set the first schedule for USB PPP mode.

<code>-x n</code>	Set the second schedule for USB PPP mode.
<code>-y n</code>	Set the third schedule for USB PPP mode.
<code>-z n</code>	Set the fourth schedule for USB PPP mode.
<code>-Q <mode></code>	Set (PPP mode or DHCP mode) WAN Connection Detection Mode. <mode> 0: ARP Detect; 1: Ping Detect
<code>-I <ping ip></code>	Set (PPP mode or DHCP mode) WAN Connection Detection Ping IP for USB DHCP or PPP mode. <ping ip>= ppp.qqq.rrr.sss: WAN Connection Detection Ping IP
<code>-L n</code>	Set WAN Connection Detection TTL (1-255) value for USB PPP mode.
<code>-E <sim pin code></code>	Set SIM PIN code (max. 19 characters) for USB DHCP mode.
<code>-G <mode></code>	Set Network Mode for USB DHCP mode. <mode> 0: 4G/3G/2G; 1: 4G Only; 2: 3G Only; 3: 2G Only
<code>-N <apn name></code>	Set APN Name (max. 47 characters) for USB DHCP mode.
<code>-U n</code>	Set MTU(1000-1440) for USB DHCP mode.

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 -M 1 -u link1 -p link1 -a 0
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 public 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 pubsubnet enable
public subnet enabled!
```

Telnet Command: ip pubaddr

This command allows to set the IP routed subnet for the router.

Syntax

ip pubaddr ?

ip pubaddr <public subnet IP address>

Syntax Description

Parameter	Description
<i>?</i>	Display an IP address which allows users set as the public subnet IP address.
<i>public subnet IP address</i>	Specify an IP address. The system will set the one that you specified as the public subnet IP address.

Example

```
> ip pubaddr ?
% ip addr <public subnet IP address>
% Now: 192.168.0.1

> ip pubaddr 192.168.2.5
% Set public subnet IP address done !!!
```

Telnet Command: ip pubmask

This command allows users to set the mask for IP routed subnet of your router.

Syntax

ip pubmask ?

ip pubmask <public subnet mask>

Syntax Description

Parameter	Description
<i>?</i>	Display an IP address which allows users set as the public subnet mask.
<i>public subnet IP address</i>	Specify a subnet mask. The system will set the one that you specified as the public subnet mask.

Example

```
> ip pubmask ?
```

```

% ip pubmask <public subnet mask>
% Now: 255.255.255.0

> ip pubmask 255.255.0.0
% Set public subnet mask done !!!

```

Telnet Command: ip aux

This command is used for configuring WAN IP Alias.

Syntax

```
ip aux add [IP] [Join to NAT Pool]
```

```
ip aux remove [index]
```

Syntax Description

Parameter	Description
<i>add</i>	It means to create a new WAN IP address.
<i>remove</i>	It means to delete an existed WAN IP address.
<i>IP</i>	It means the auxiliary WAN IP address.
<i>Join to NAT Pool</i>	0 (disable) or 1 (enable).
<i>index</i>	Type the index number of the table displayed on your screen.

Example

```

> ip aux add 192.168.1.65 1
% 192.168.1.65 has added in index 2.

DrayTek> ip aux ?
%% ip aux add [IP] [Join to NAT Pool]
%% ip aux remove [Index]

%%      Where IP = Auxiliary WAN IP Address.
%%      Join to NAT Pool = 0 or 1.
%%      Index = The Index number of table.

Now auxiliary WAN1 IP Address table:
Index no.      Status  IP address      NAT IP pool
-----
  1           Disable 0.0.0.0 Yes
  2           Enable 192.168.1.65   Yes

```


Telnet Command: ip addr

This command allows users to set/add a specified LAN IP your router.

Syntax

`ip addr [IP address]`

Syntax Description

Parameter	Description
<i>IP address</i>	It means the LAN IP address.

Example

```
>ip addr 192.168.50.1
% Set IP address OK !!!
```



Info

When the LAN IP address is changed, the start IP address of DHCP server are still the same. To make the IP assignment of the DHCP server being consistent with this new IP address (they should be in the same network segment), the IP address of the PC must be fixed with the same LAN IP address (network segment) set by this command for accessing into the web user interface of the router. Later, modify the start addresses for the DHCP server.

Telnet Command: ip nmask

This command allows users to set/add a specified netmask for your router.

Syntax

`ip nmask [IP netmask]`

Syntax Description

Parameter	Description
<i>IP netmask</i>	It means the netmask of LAN IP.

Example

```
> ip nmask 255.255.0.0
% Set IP netmask OK !!!
```

Telnet Command: ip arp

ARP displays the matching condition for IP and MAC address.

Syntax

`ip arp add [IP address] [MAC address] [LAN or WAN]`

`ip arp del [IP address] [LAN or WAN]`

`ip arp flush`

`ip arp status`

`ip arp accept [0/1/2/3/4/5/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</i>	0: disable to accept illegal source mac address 1: enable to accept illegal source mac address 2: disable to accept illegal dest mac address 3: enable to accept illegal dest mac address 4: Decline VRRP mac into arp table 5: Accept VRRP mac into arp table status: display the setting status.
<i>Time</i>	Available settings will be 10, 20, 30,...2550 seconds.

Example

```
> ip arp accept status
Accept illegal source mac arp: disable

Accept illegal dest mac arp: disable

Accept VRRP mac into arp table: disable
> ip arp status
[ARP Table]
  Index IP Address      MAC Address      Netbios Name
  1    192.168.1.113    00-05-5D-E4-D8-EE  A1000351
```

Telnet Command: ip dhcpc

This command is available for WAN DHCP.

Syntax

ip dhcpc option

ip dhcpc option -h/l

ip dhcpc option -d [idx]

ip dhcpc option -e [1 or 0] -w [wan unumber] -c [option number] -v [option value]

ip dhcpc option -e [1 or 0] -w [wan unumber] -c [option number] -x [option value]

ip dhcpc option -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 option -e 1 -w 1/2 -c 18 -v /path1  
>
```

Telnet Command: ip ping

This command allows users to ping IP address of WAN1/WAN2/PVC3/PVC4/PVC5 for verifying if the WAN connection is OK or not.

Syntax

`ip ping [IP address] [AUTO/WAN1/PVC3/PVC4/PVC5] [Source IP address]`

Syntax Description

Parameter	Description
<i>IP address</i>	It means the WAN IP address.
<i>AUTO/WAN1/PVC3/PVC4/PVC5</i>	It means the WAN port /PVC that the above IP address passes through.

Example

```
> ip ping 192.168.1.1 AUTO  
  
Pinging 192.168.1.1 with 64 bytes of Data through LAN  
  
Receive reply from 192.168.1.1, time<lms  
Receive reply from 192.168.1.1, time<lms  
Receive reply from 192.168.1.1, time<lms  
Receive reply from 192.168.1.1, time<lmsReceive reply from 192.168.1.1,  
time<lms  
  
Packets: Sent = 5, Received = 5, Lost = 0 (0% loss)
```

Telnet Command: ip tracert

This command allows users to trace the routes from the router to the host.

Syntax

`ip tracert [Host/IP address] [WAN1/WAN2/WAN3] [Udp/Icmp]`

Syntax Description

Parameter	Description
<i>IP address</i>	It means 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>	It means the UDP or ICMP.

Example

```
>ip tracert 22.128.2.62 WAN1
Traceroute to 22.128.2.62, 30 hops max
 1  172.16.3.7  10ms
 2  172.16.1.2  10ms
 3  Request Time out.
 4  168.95.90.66 50ms
 5  211.22.38.134 50ms
 6  220.128.2.62 50ms
Trace complete
```

Telnet Command: ip telnet

This command allows users to access specified device by telnet.

Syntax

`ip telnet [IP address][Port]`

Syntax Description

Parameter	Description
<i>IP address</i>	Type the WAN or LAN IP address of the remote device.
<i>Port</i>	Type a port number (e.g., 23). Available settings: 0 ~65535.

Example

```
> ip telnet 172.17.3.252 23
>
```

Telnet Command: ip rip

This command allows users to set the RIP (routing information protocol) of IP.

Syntax

`ip rip [0/1/2]`

Syntax Description

Parameter	Description
-----------	-------------

0/1/2

0 means disable; 1 means first subnet and 2 means second subnet.

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, 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
       3: PVC3,4: PVC4,5: PVC5
-e <0/1> 0: disable, 1: enable
Now status:
WAN[1] Rip Protocol disable
WAN[3] Rip Protocol disable
WAN[4] Rip Protocol disable
WAN[5] Rip Protocol disable
WAN[6] Rip Protocol enable
> ip wanrip 5 -e 1
> ip wanrip ?
Valid ex:ip wanrip <ifno> -e <0/1>
<ifno> 1: WAN1
       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 enable
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 [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>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
<i>rtype</i>	It means the type of the route. default : default route; static: static route. Rip: rip.
<i>status</i>	It means current status of static route.
<i>cnc</i>	It means current IP range for CNC Network.
<i>default</i>	Set WAN1/WAN2/off as current default route.
<i>clean</i>	Clean all of the route settings. 1: Enable the function. 0: Disable the function.

Example

```
> ip route add 172.16.2.0 255.255.255.0 172.16.2.4 3 static
> ip route status

Codes: C - connected, S - static, R - RIP, * - default, ~ - private
C~      192.168.1.0/    255.255.255.0 is directly connected, LAN1
S       172.16.2.0/    255.255.255.0 via 172.16.2.4, WAN1
```

Telnet Command: ip igmp_proxy

This command allows users to enable/disable igmp proxy server.

Syntax

```
ip igmp_proxy set
ip igmp_proxy reset
ip igmp_proxy wan
ip igmp_proxy query
ip igmp_proxy ppp [0/1]
ip igmp_proxy status
```

Syntax Description

Parameter	Description
<i>set</i>	It means to enable proxy server.
<i>reset</i>	It means to disable proxy server.
<i>wan</i>	It means to specify WAN interface for IGMP service.
<i>t_home</i>	It means to specify t_home proxy server for using.
<i>On/off/show/help</i>	It means to turn on/off/display or get more information of the T_home service.
<i>query</i>	It means to set IGMP general query interval. The default value is 125000 ms.
<i>ppp</i>	0 - No need to set IGMP with PPP header. 1 - Set IGMP with PPP header.
<i>status</i>	It means to display current status for proxy server.

Example

```
> ip igmp_proxy query 130000
This command is for setting IGMP General Query Interval
The default value is 125000 ms
Current Setting is:130000 ms
>
```

Telnet Command: ip igmp_snoop

This command allows users to enable or disable IGMP snoop function.

Syntax

```
ip igmp_snoop enable
ip igmp_snoop disable
ip igmp_snoop status
ip igmp_snoop txquery
ip igmp_snoop chkleave
ip igmp_snoop separate
```

Syntax Description

Parameter	Description
-----------	-------------

<i>enable</i>	It means to enable igmp snoop function
<i>disable</i>	It means to disable igmp snoop function.
<i>status</i>	It means to display current igmp configuration.
<i>txquery</i>	It means to send out IGMP QUERY to LAN periodically.
<i>chkleave</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</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.

Example

```

> ip igmp_snoop enable
%% ip igmp snooping [enable|disable|status], IGMP Snooping is Enabled.
> ip igmp_snoop disable
%% ip igmp snooping [enable|disable|status], IGMP Snooping is Disabled.
> ip igmp_snoop separate ?
% ip igmp separate [on/off]
  igmp snoop seprate is ON now.
  igmp packets will be separated by NAT/Bridge.

```

Telnet Command: ip dmz

Specify MAC address of certain device as the DMZ host.

Syntax

`ip dmz [mac]`

Syntax Description

Parameter	Description
<i>mac</i>	It means the MAC address of the device that you want to specify

Example

```
>ip dmz ?
% ip dmz <mac>, now : 00-00-00-00-00-00
> ip dmz 11-22-33-44-55-66
> ip dmz ?
% ip dmz <mac>, now : 11-22-33-44-55-66
>
```

Telnet Command: ip dmzswitch

This command allows users to set DMZ mode.

`ip dmzswitch off`

`ip dmzswitch private`

`ip dmzswitch active_trueip`

Syntax Description

Parameter	Description
<i>off</i>	It means to turn off DMZ function.
<i>private</i>	It means to set DMZ with private IP.
<i>active_trueip</i>	It means to set the DMZ with active true IP.

Example

```
>ip ip dmzswitch off
>
```

Telnet Command: ip session

This command allows users to set maximum session limit number for the specified IP; set message for exceeding session limit and set how many seconds the IP session block works.

Syntax

`ip session on`

`ip session off`

`ip session default [num]`

`ip session defaulttp2p [num]`

`ip session status`

`ip session show`

ip session timer [num]
 ip session [block/unblock][IP]
 ip session [add/del][IP1-IP2][num][p2pnum]

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on session limit for each IP.
<i>off</i>	It means to turn off session limit for each IP.
<i>default [num]</i>	It means to set the default number of session num limit.
<i>DefaultIp2p [num]</i>	It means to set the default number of session num limit for p2p.
<i>status</i>	It means to display the current settings.
<i>show</i>	It means to display all session limit settings in the IP range.
<i>timer [num]</i>	It means to set when the IP session block works. The unit is second.
<i>[block/unblock][IP]</i>	It means to block/unblock the specified IP address. Block: The IP cannot access Internet through the router. Unblock: The specified IP can access Internet through the router.
<i>add</i>	It means to add the session limits in an IP range.
<i>del</i>	It means to delete the session limits in an IP range.
<i>IP1-IP2</i>	It means the range of IP address specified for this command.
<i>num</i>	It means the number of the session limits, e.g., 100.
<i>p2pnum</i>	It means the number of the session limits, e.g., 50 for P2P.

Example

```
> ip session default 100
> ip session add 192.168.1.5-192.168.1.100 100 50
> ip session on
> ip session status

IP range:
  192.168.1.5 - 192.168.1.100 : 100

Current ip session limit is turn on

Current default session number is 100
```

Telnet Command: ip bandwidth

This command allows users to set maximum bandwidth limit number for the specified IP.

Syntax

ip bandwidth *on*
 ip bandwidth *off*
 ip bandwidth *default [tx_rate][rx_rate]*
 ip bandwidth *status*
 ip bandwidth *show*

`ip bandwidth [add/del] [IP1-IP2][tx][rx][shared]`

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on the IP bandwidth limit.
<i>off</i>	It means to turn off the IP bandwidth limit.
<i>default [tx_rate][rx_rate]</i>	It means to set default tx and rx rate of bandwidth limit. The range is from 0 - 65535 Kpbs.
<i>status</i>	It means to display the current settings.
<i>show</i>	It means to display all the bandwidth limits settings within the IP range.
<i>add</i>	It means to add the bandwidth within the IP range.
<i>del</i>	It means to delete the bandwidth within the IP range.
<i>IP1-IP2</i>	It means the range of IP address specified for this command.
<i>tx</i>	It means to set transmission rate for bandwidth limit.
<i>rx</i>	It means to set receiving rate for bandwidth limit.
<i>shared</i>	It means that the bandwidth will be shared for the IP range.

Example

```
> ip bandwidth default 200 800
> ip bandwidth add 192.168.1.50-192.168.1.100 10 60
> ip bandwidth status

IP range:
  192.168.1.50 - 192.168.1.100 : Tx:10K Rx:60K

Current ip Bandwidth limit is turn off

Auto adjustment is off
```

Telnet Command: ip bindmac

This command allows users to set IP-MAC binding for LAN host.

Syntax

`ip bindmac on`

`ip bindmac off`

`ip bindmac [strict_on][strict_off]`

`ip bindmac subnet [all/set LAN_Index/unset LAN_Index/clear/show]`

`ip bindmac show`

`ip bindmac add [IP][MAC][Comment]`

`ip bindmac del [IP]/all`

Syntax Description

Parameter	Description
-----------	-------------

<i>on</i>	It means to turn on IP bandmac 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 / strict_off</i>	It means that only those IP address in IP bindmac policy table can / can not access into network.
<i>subnet</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 type the IP address for binding with specified MAC address.
<i>MAC</i>	It means to type the MAC address for binding with the IP address specified.
<i>Comment</i>	It means to type words as a brief description.
<i>All</i>	It means to delete all the IP bindmac settings.

Example

```

> ip bindmac add 192.168.1.46 00:50:7f:22:33:55 just for test
> ip bindmac show
ip bind mac function is turned OFF
ip bind mac function is STRICT OFF
Show all IP Bind MAC entries.
IP : 192.168.1.46 bind MAC : 00-50-7f-22-33-55 HOST ID : (null)
Comment : just

```

Telnet Command: ip maxnatuser

This command is used to set the maximum number of NAT users.

Syntax

ip maxnatuser *user no*

Syntax Description

Parameter	Description
<i>User no</i>	A number specified here means the total NAT users that Vigor router supports. 0 - It means no limitation.

Example

```
> ip maxnatuser 100
% Max NAT user = 100
```

Telnet Command: ip policy_rt

This command is used to set the IP policy route profile.

Syntax

ip policy_rt [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
<command><parameter>[...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
General Setup for Policy Route	
-i [value]	Specify an index number for setting policy route profile. Value: 1 to 60. "-1" means to get a free policy index automatically.
-e [0/1]	0: Disable the selected policy route profile. 1: Enable the selected policy route profile.
-o [value]	Determine the operation of the policy route. Value: add - Create a new policy route profile. del - Remove an existed policy route profile. edit - Modify an existed policy route profile. flush - Reset policy route to default setting.
-1 [any/range]	Specify the source IP mode. Range: Indicate a range of IP addresses. Any: It means any IP address will be treated as source IP address.
-2 [any/ip_range/ip_subnet/do main]	Specify the destination IP mode. Any: No need to specify an IP address for any IP address will be treated as destination IP address. ip_range: Indicates a range of IP addresses. ip_subnet: Indicates the IP subnet. domain: Indicates the domain name.
-3 [any/range]	Specify the destination port mode. Range: Indicate a range of port number.

	Any: It means any port number can be used as destination port.
<i>-G [default/specific]</i>	Specify the gateway mode.
<i>-L [default/specific]</i>	Specify the failover gateway mode.
<i>-s [value]</i>	Indicate the source IP start. Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.1.0)
<i>-S [value]</i>	Indicate the source IP end. Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.1.100)
<i>-d [value]</i>	Indicate the destination IP start. Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.2.0)
<i>-D [value]</i>	Indicate the destination IP end. Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.2.100)
<i>-p [value]</i>	Indicate the destination port start. Value: Type a number (1 ~ 65535) as the port start (e.g., 1000).
<i>-P [value]</i>	Indicate the destination port end. Value: Type a number (1 ~ 65535) as the port end (e.g., 2000).
<i>-y [value]</i>	Indicate the priority of the policy route profile. Value: Type a number (0 ~ 250). The default value is "150".
<i>-I [value]</i>	Indicate the interface specified for the policy route profile. Value: Available interfaces include, LAN1 ~ LAN4, IP_Routed_Subnet, DMZ_Subnet, WAN1 ~ WAN3, VPN_PROFILE_1 ~ VPN_PROFILE_32, WAN_1_IP_ALIAS_1 ~ WAN_2_IP_ALIAS_32
<i>-g [value]</i>	Indicate the gateway IP address. Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.3.1)
<i>-I [value]</i>	Indicate the failover IP address. Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.4.1)
<i>-t [value]</i>	It means "protocol". Value: Available settings include "TCP", "UDP", "TCP/UDP", "ICMP" and "Any".
<i>-n [0/1]</i>	Indicates the function of "Force NAT". 0: Disable the function. 1: Enable the function.
<i>-a [0/1]</i>	Indicates to enable the function of failover. 0: Disable the function. 1: Enable the function.
<i>-f [value]</i>	It means to specify the interface for failover. Value: Available interfaces include, NO_FAILOVER, Default_WAN, Policy1 ~ Policy10 LAN1 ~ LAN4 IP_Routed_Subnet, VPN_PROFILE_1 ~ VPN_PROFILE_32, WAN_1_IP_ALIAS_1 ~ WAN_2_IP_ALIAS_32
<i>-b [value]</i>	It means "failback". Value: Available settings include, 0: Disable the function of "failback". 1: Enable the function of "failback".

	-v: View current fallback setting.
Diagnose for Policy Route	
-s <i>[value]</i>	It means "source IP". Value: Available settings include: Any: It indicates any IP address can be used as source IP address. "xxx.xxx.xxx.xxx": The type format (e.g, 192.168.1.0).
-d <i>[value]</i>	It means "destination IP". Value : Available settings include: Any: It indicates any IP address can be used as destination IP address. "xxx.xxx.xxx.xxx": Specify an IP address.
-p <i>[value]</i>	It means "destination port". Value: Specify a number or type Any (indicating any number).
-t <i>[value]</i>	It means "protocol". Value: Available settings include "ICMP", "TCP", "UDP" and "Any".

Example

```
> ip policy_rt diagnose -s 192.168.1.100 -d any -p any -t ICMP

-----
      Matched Route (Priority)
-----
* No_Match

-----
      Matched Policy (Priority)
-----
* Policy_1 (200)

* Conclusion:The packet was dropped because the send-to interface of the
matched
> 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 WAN1
```

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> | ...]

Parameter	Description
-a <IP Address>	It is used to configure IP address mapping (IPv4/IPv6 Address or multiple subnet addresses). <i>IP Address</i> : type the IP address (e.g., 192.168.1.56).
-c <CNAME>	It is used to set CNAME for such profile.
-d <address mapping index number>	It means to delete index number with address mapping configured. <i>address mapping index number</i> : 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>-i <profile setting index number></i>	It means to create LAN DNS profile with specified domain name. <i>profile setting index number</i> : type the index number which represents the profile with domain name configured.
<i>-l</i>	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
<i>-n<domain name></i>	It means to specify a domain name to be accessed.
<i>-p<profile name></i>	It means to set name of the LAN DNS profile.
<i>-r</i>	It means to clear specified domain name profile and the address mapping setting.
<i>-s<0/1></i>	It means to determine all subnet packets or only the packets with the same subnet will be replied for address mapping profile. 0: reply all subnet packets. 1: reply only same subnet packet.
<i>-z</i>	It means to update LAN DNS configuration to DNS cache.

Example

```
> ip lanDNSRes -i 1 -n ftp.drayTek.com
% Configure Set1's DomainName:ftp.drayTek.com
> ip lanDNSRes -i 1 -n ftp.drayTek.com
> ip lanDNSRes -i 1 -a 172.16.2.10 -s 1
> ip lanDNSRes -i 1 -a 172.16.3.10 -s 1
> ip lanDNSRes -i 1 -a 172.16.4.10 -s 1
>
```

Telnet Command: ip dnsforward

This command is used to set LAN DNS profile for conditional DNS forwarding.

ip dnsforward [*-<command>* *<parameter>* | ...]

Syntax Description

Parameter	Description
<i>[<command> <parameter> ...]</i>	The available commands with parameters are listed below. [...] <i>]</i> means that you can type in several commands in one line.
<i>-a <IP Address></i>	Set forwarded DNS server IP Address.
<i>-d <DNS server mapping index number></i>	Delete the selected LAN DNS profile.
<i>-e <0/1></i>	0: disable such function. 1: enable such function.
<i>-i <profile setting index number></i>	Type the index number of the profile.
<i>-l</i>	List the content of LAN DNS profile (including domain name, IP address and message).
<i>-n <domain name></i>	Set domain name.

<code>-p <profile name></code>	Set profile name for LAN DNS.
<code>-r</code>	Reset the settings for selected profile.

Example

```
> ip dnsforward -i 1 -n ftp.drayTek.com
% Configure Set1's DomainName:ftp.drayTek.com
> ip dnsforward -i 1 -a 172.16.1.1
% Configure Set1's IP:172.16.1.1
> ip dnsforward -i 1 -l
% Idx: 1
% State: Disable
% Profile: test
% Domain Name: ftp.drayTek.com
% DNS Server IP: 172.16.1.1
>
```

Telnet Command: ip6 addr

This command allows users to set the IPv6 address for your router.

Syntax

```
ip6 addr -s [prefix] [prefix-length] [LAN1|LAN2|...|LAN4|WAN1|WAN2|USB|VPN1|..VPN32]
ip6 addr -d [prefix] [prefix-length] [LAN1|LAN2|...|LAN4|WAN1|WAN2|USB|VPN1|..VPN32]
ip6 addr -a [LAN1|LAN2|...|LAN4|WAN1|WAN2|USB|VPN1|...|VPN32#]
ip6 addr -v [LAN1|LAN2|...|LAN4|WAN1|WAN2|USB]
ip6 addr -o [prefix] [prefix-length][WAN1|WAN2|USB]
ip6 addr -l [prefix] [prefix-length] [LAN1|LAN2|...|LAN4]
ip6 addr - [p/b] [prefix] [prefix-length] [WAN1|WAN2|USB]
ip6 addr -x [LAN1|LAN2|...|LAN4]
ip6 addr -c [LAN1|LAN2|...|LAN4]
ip6 addr -e [0/1/2] [LAN1|LAN2|...|LAN4]
```

Syntax Description

Parameter	Description
<code>-s</code>	It means to add a static ipv6 address.
<code>-d</code>	It means to delete an ipv6 address.
<code>-a</code>	It means to show current address(es) status.
<code>-u</code>	It means to show only unicast addresses.
<code>prefix</code>	It means to type the prefix number of IPv6 address.
<code>prefix-length</code>	It means to type a fixed value as the length of the prefix.
<code>LAN WAN1 WAN2 iface#</code>	It means to specify LAN or WAN interface for such address.

Example

```
> ip6 addr -a
LAN
Unicast Address:
```

```
FE80::250:7FFF:FE00:0/64 (Link)
Multicast Address:
FF02::2
FF02::1:FF00:0
FF02::1
```

Telnet Command: ip6 dhcp req_opt

This command is used to configure option-request settings for DHCPv6 client.

Syntax

```
ip6 dhcp req_opt [LAN1 ~LAN4|WAN1|WAN2|USB] [-<command> <parameter>| ... ]
```

Syntax Description

Parameter	Description
<i>req_opt</i>	It means option-request.
<i>LAN1-4 WAN1 WAN2 USB</i>	It means to specify LAN or WAN interface for such address.
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-a	It means to show current DHCPv6 status.
-s	It means to ask the SIP.
-S	It means to ask the SIP name.
-d	It means to ask the DNS setting.
-D	It means to ask the DNS name.
-n	It means to ask NTP.
-i	It means to ask NIS.
-I	It means to ask NIS name.
-p	It means to ask NISP.
-P	It means to ask NISP name.
-b	It means to ask BCMCS.
-B	It means to ask BCMCS name.
-r	It means to ask refresh time.
<i>Parameter</i>	1: the parameter related to the request will be displayed. 0: the parameter related to the request will not be displayed.

Example

```
> ip6 dhcp req_opt WAN2 -S 1
> ip6 dhcp req_opt WAN2 -r 1
> ip6 dhcp req_opt WAN2 -a
% Interface WAN2 is set to request following DHCPv6 options:
%   sip name
>
```

Telnet Command: ip6 dhcp client

This command allows you to use DHCPv6 protocol to obtain IPv6 address from server.

Syntax

`ip6 dhcp client [WAN1|WAN2|USB] [-<command> <parameter>| ...]`

Syntax Description

Parameter	Description
<code>client</code>	It means the dhcp client 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>-p [IAID]</code>	It means to request identity association ID for Prefix Delegation.
<code>-n [IAID]</code>	It means to request identity association ID for Non-temporary Address.
<code>-t [time]</code>	It means to set solicit interval. Time: 0 ~ seconds (default value is 0).
<code>-c [parameter]</code>	It means to send rapid commit to server.
<code>-l [parameter]</code>	It means to send information request to server.
<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.
<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.
<code>-S [parameter]</code>	It means to set shared secret (max: 31 characters) in delayed protocol.
<code>-K [parameter]</code>	It means to set key ID (1~65535) in delayed protocol.

Example

```
> ip6 dhcp client WAN2 -p 2008::1
> ip6 dhcp client WAN2 -a
  Interface WAN2 has following DHCPv6 client settings:
    DHCPv6 client enabled
    request IA_PD whose IAID equals to 2008
> ip6 dhcp client WAN2 -n 1023456
> ip6 dhcp client WAN2 -a
  Interface WAN2 has following DHCPv6 client settings:
    DHCPv6 client enabled
    request IA_NA whose IAID equals to 2008
> system reboot
```

Telnet Command : ip6 dhcp server

This command allows you to configure DHCPv6 server.

Syntax

`ip6 dhcp server [-<command> <parameter>| ...]`

Syntax Description

Parameter	Description
<i>server</i>	It means the dhcp server settings.
[<command> <parameter>[...]]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-a	It means to show current DHCPv6 status.
-b	It means to show current DHCPv6 IP Assignment Table.
-n <name>	It means to set a profile name.
-c<parameter>	It means to send rapid commit to server. 1: Enable 0: Disable
-e<parameter>	It means to enable or disable the DHCPv6 server. 1: Enable 0: Disable
-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 <1/0>	It means to enable (1) or disable (0) auto_range.
-d<addr>	It means to set the first DNS IPv6 address.
-D<addr>	It means to set the second DNS IPv6 address.
-m<1/0>	It means to enable(1) or disable (0) the server DUID set by Link Layer and Time.
-q	It means to set DNS domain search list.
-z<1/0>	It means enable (1) or disable (0) the DHCP PD.
<i>pdadd</i> <suffix><prefix_len><client linklocal><client DUID>	It means to add PD node.
<i>pddel</i> <PD index>	It means to delete PD node.
-A <parameter>	It means to set authentication protocol. 0: Undefine 2: delayed protocol 3: Reconfigure key
-M <parameter>	It means to set realm value (max: 31 characters) in delayed protocol.
-S <parameter>	It means to set shared secret (max: 31 characters) in delayed protocol.
-K <parameter>	It means to set key ID (1~65535) in delayed protocol.

Example

```

> ip6 dhcp server -d FF02::1
> ip6 dhcp server -i ff02::1
> ip6 dhcp server -x ff02::3
> ip6 dhcp server -a
% Interface LAN has following DHCPv6 server settings:

```

```

%   DHCPv6 server disabled
%   maximum address of the pool: FF02::3
%   minimum address of the pool: FF02::1
%   1st DNS IPv6 Addr: FF02::1

```

Telnet Command: ip6 internet

This command allows you to configure settings for accessing Internet.

Syntax

`ip6 internet [-<command> <parameter> | ...]`

Syntax Description

Parameter	Description
<code>[<command> <parameter> ...]</code>	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
<code>-W n</code>	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
<code>-M n</code>	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
<code>-m n</code>	It means to set IPv6 MTU. N = any value (0 means "unspecified").
<code>6rd</code>	
<code>-C n</code>	It means to set 6rd connection mode. n=0: Auto n=1: Static
<code>-s <server></code>	It means to set 6rd IPv4 Border Relay.
<code>-m n</code>	It means to set 6rd IPv4 address mask length.
<code>-p <prefix></code>	It means to set IPv6 prefix for 6rd connection.
<code>-l n</code>	It means to set the prefix length for 6rd connection.
<code>6in4</code>	
<code>-s <server></code>	It means to set 6in4 remote endpoint IPv4 address.
<code>-l <IPv6 Addr></code>	It means to set the IPv6 address for 6in4 connection.
<code>-P n</code>	It means to set IPv6 WAN prefix length for 6in4 connection.

<i>-p <prefix></i>	It means to set 6in4 LAN Routed Prefix.
<i>-l n</i>	It means to set 6in4 LAN Routed Prefix length.
<i>-T n</i>	It means to set 6in4 Tunnel TTL.
<i>TSPC/AICCU</i>	
<i>-u <username></i>	It means to set Username (max. 63 characters).
<i>-P <password></i>	It means to set Password (max. 63 characters).
<i>-s <server></i>	It means to set Tunnel Server IP. <server>= IPv4 Addr or URL (max. 63 characters)
<i>AICCU</i>	
<i>-p <prefix></i>	It means to set Subnet Prefix (AICCU).
<i>-l n</i>	It means to set Subnet Prefix length (AICCU).
<i>-o</i>	It means to set AICCU always on. On = 1, Off = 0.
<i>-f</i>	It means to set AICCU tunnel ID.
<i>Static</i>	
<i>-w <addr></i>	It means to set Default Gateway.
<i>Others</i>	
<i>-d <server></i>	It means to set 1st DNS Server IP. <server>= IPv6 Addr
<i>-D <server></i>	It means to set 2nd DNS Server IP. <server>= IPv6 Addr
<i>-t <dhcp/ra/none></i>	It means to set ipv6 PPP WAN test mode for DHCP or RA.
<i>-V</i>	It means to view IPv6 Internet Access Profile.
<i>-k</i>	It means to dial the Tunnel on the WAN.
<i>-j</i>	It means to drop the Tunnel on the WAN.
<i>-r n</i>	It means to set Prefix State Machine RA timeout.
<i>-c n</i>	It means to set Prefix State Machine DHCPv6 Client timeout.
<i>-q</i>	It means to set WAN detection mode (0:NS Detect, 1:Ping Detect, 2:Always On).
<i>-z</i>	It means to set Ping Detect TTL (0-255).
<i>-x</i>	It means to set Ping Detect Host (hostname or IPv6 address).
<i>-i</i>	It means to set ipv6 connection interval (1500-60000 (unit:10ms)).
<i>-b</i>	It means to enable DNSv6 based on DHCPv6. On = 1, Off = 0
<i>-R</i>	It means to Enable RIPng. On = 1, Off = 0

Example

```
> ip6 internet -W 2 -M 2 -u 88886666 -p draytek123456 -s amsterdam.freenet6.net
This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
> system reboot
```

Telnet Command: ip6 neigh

This command allows you to display IPv6 neighbour table.

Syntax

```
ip6 neigh -s [inet6_addr] [eth_addr] [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	It means to add a neighbour.
-d	It means to delete a neighbour.
-a	It means to show neighbour status.
inet6_addr	Type an IPv6 address
eth_addr	Type submask address.
LAN1/LAN2/.../LAN4/WAN1/WAN2/USB	Specify an interface for the neighbor.

Example

```
> ip6 neigh -s 2001:2222:3333::1111 00:50:7F:11:ac:22:WAN1
      Neighbour 2001:2222:3333::1111 successfully added!
> ip6 neigh -a

I/F  ADDR                               MAC                               STATE
-----
LAN1  2001:2222:3333::1111              IN_TIMER
LAN4  ::                                  NONE
LAN3  ::                                  NONE
LAN1  ::                                  NONE
LAN2  ::                                  NONE
DMZ   ::                                  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	It means to add a proxy neighbour.
-d	It means to delete a proxy neighbour.
-a	It means to show proxy neighbour status.
inet6_addr	Type an IPv6 address
LAN1/WAN1/WAN2	Specify an interface for the proxy neighbor.

Example

```
> ip6 pneighbor -s FE80::250:7FFF:FE12:300 LAN1
%      Neighbour FE80::250:7FFF:FE12:300 successfully added!
```

Telnet Command: ip6 route

This command allows you to set route for IPv6 connection.

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	It means to add a route.
-d	It means to delete a route.
-a	It means to show the route status.
-D	It means that such route will be treated as the default route.
prefix	It means to type the prefix number of IPv6 address.
prefix-length	It means to type a fixed value as the length of the prefix.
gateway	It means the gateway of the router.
LAN1/LAN2/.../LAN4/WAN1/ WAN2/ USB/VPN1/.../VPN32	It means to specify LAN or WAN interface for such address.

Example

```
> ip6 route -s FE80::250:7FFF:FE12:500 16 FE80::250:7FFF:FE12:100 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:FE00:0/128	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 WAN1

Pinging 2001:4860:4860::8888 with 64 bytes of Data:

Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms

Packets: Sent = 5, Received = 5, Lost = 0 <% loss>
>
```

Telnet Command: ip6 tracert

This command allows you to trace the routes from the router to the host.

Syntax

`ip6 tracert [IPv6 address/Host] [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 tpsc

This command allows you to display TSPC status.

Syntax

`ip6 tpsc [ifno]`

Syntax Description

Parameter	Description
<i>ifno</i>	It means the connection interface. Ifno=1 (means WAN1)

Example

```
> ip6 tpsc 1
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 -V
```

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.
-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 <0/1/2>	It means to set RDNSS Disable/Enable/Deploy when WAN is up.
-d <lifetime>	It means to set RA default lifetime.
-i <lifetime>	It means to set RA min interval time(sec).
-l <lifetime>	It means to set RA MAX interval time(sec).
-h <hoplimit>	It means to set RA hop limit.
-m <mtu/auto>	It means to set RA MTU, 1280-1500. mtu: auto - auto select MTU from WAN,
-e <time>	It means to set reachable time.
-a <time/infinity>	It means to set retransmit timer /infinity.
-p <0/1/2>	It means to set radvd default preference Low/Medium/High. 0-low 1-medium 2-high
-v	It means to view radvd configuration.
-V	It means to view setting in RA.
-L <time/infinity>	It means to set prefix valid lifetime.
-P <time/infinity>	set prefix preferred lifetime.
-r [num]	It means to to set RA test for item. 0-default, 121:logo 121, 124:logo 124..
-R	It means to reload Config and send RA for subnets.
-u	It means to view MTU on all interfaces.

Example

```
> ip6 radvd LAN1 -V
% [LAN1] setting !
% Default Lifetime : 0 seconds
```

% min interval time	: 200 seconds
% MAX interval time	: 600 seconds
% Hop limit	: 64
% MTU	: 0
% Reachable time	: 0
% Retransmit time	: 0
% Preference	: Medium

Telnet Command: ip6 mngt

This command allows you to manage the settings for access list.

Syntax

ip6 mngt list

ip6 mngt list [*add* <Index> <IPv6 Object Index> |*remove* <Index>|*flush*]

ip6 mngt status

ip6 mngt [*http*|*telnet*|*ping*|*https*|*ssh*] [*on*|*off*]

Syntax Description

Parameter	Description
<i>list</i>	It means to show the setting information of the access list.
<i>status</i>	It means to show the status of IPv6 management.
<i>add</i>	It means to add an IPv6 address which can be used to execute management through Internet.
<i>index</i>	It means the number (1, 2 and 3) allowed to be configured for IPv6 management.
<i>remove</i>	It means to remove (delete) the specified index number with IPv6 settings.
<i>flush</i>	It means to clear the IPv6 access table.
<i>http</i> <i>telnet</i> <i>ping</i> <i>https</i> <i>ssh</i>	These protocols are used for accessing Internet.
<i>on</i> <i>off</i>	It means to enable (on) or disable (off) the Internet accessing through http/telnet/ping.

Example

```
> ip6 mngt list add 1 1
%% Set OK.
> ip6 mngt status
% IPv6 Remote Management :
telnet : off, http : off, https : off, ssh : off, ping : off
> ip6 mngt http on
> ip6 mngt status
% IPv6 Remote Management :
telnet : off, http : on, https : off, ssh : off, ping : off
```

Telnet Command: ip6 online

This command allows you to check the online status of IPv6 LAN /WAN.

Syntax

ip6 online [*WAN1*|*WAN2*|*USB*]

Syntax Description

Parameter	Description
<i>[WAN1/WAN2/USB]</i>	It means the connection interface. 0=LAN1 1=WAN1 2=WAN2

Example

```
> ip6 online WAN1
% WAN1 online status :
% IPv6 WAN1 TSPC
% 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 set 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
<i>ifno</i>	It means the connection interface. 1=WAN1 2=WAN2
<i>-r</i>	It means to remove (delete) the specified index number with IPv6 settings.
<i>-s</i>	It means to display the AICCU status.

Example

```
> ip6 aiccu -i 1 -s
Status: Idle
```

Telnet Command: ip6 ntp

This command allows you to set IPv6 settings for NTP (Network Time Protocols) server.

Syntax

```
ip6 ntp -h
```

```
ip6 ntp -v
```

```
ip6 ntp -p [0/1]
```

Syntax Description

Parameter	Description
-h	It is used to display the usage of such command.
-v	It is used to show the NTP state.
-p <0/1>	It is used to specify NTP server for IPv6. 0 - Auto 1 - First Query IPv6 NTP Server.

Example

```
> ip6 ntp -p 1
% Set NTP Priority: IPv6 First
```

Telnet Command: ip6 lan

This command allows you to set IPv6 settings for LAN interface.

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 n	It means to selete LAN interface to be set. n= 1: LAN1 n= 2: LAN2, ... x: LANx. Default is LAN1
-w n	It means to selete WAN interface to be primary interface. n= 0: None, n=1: WAN1 , n=2: WAN2, ... x: WANx.
-d <server>	It means to set 1st DNS Server IP. <server>= IPv6 Address
-D <server>	It means to set 2nd DNS Server IP. <server>= IPv6 Address
-m n	It means to set ipv6 LAN management. n=0:OFF n=1:SLAAC. Default is SLAAC n=2:DHCPv6
-o n	It means to enable Other option(O-bit) flag. (O-bit is redundant when management is DHCPv6) n=0: Disable n=1: Enable.
-e n	It means to add an extension WAN. n: 1: WAN1, 2: WAN2, ... x: WANx.

-E n	It means to delete an extension WAN. n: 1: WAN1 ,2: WAN2, ... x: WANx.
-b map	It means to set bit map(decimal) for extension WAN. map: bit 0: WAN1 bit 1: WAN2, ... bit n: WAN(n+1).
-f n	It means to 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	It means to show IPv6 LAN setting. n=0:show all. Default is show all. n=1: LAN1 n=2: LAN2, ... 4: LAN4, n=5: DMZ.

Example

```
> ip6 lan -l 1 -w 1 -d 2001:4860:4860::8888 -o 1 -f 0 -s 2
% 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/off/default num/status/show]`

`ip6 session [add/del] [IP1-IP2] [num]`

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on session limit for each IP.
<i>off</i>	It means to turn off session limit for each IP.
<i>default <num></i>	It means to set the default number of session num limit.
<i>status</i>	It means to display the current settings.
<i>show</i>	It means to display all IP range session limit settings.
<i>add</i>	It means to add the session limit for an IPv6 range. <IP1-IP2> - Specify a range for IPv6 addresses.
<i>del</i>	It means to delete the session limit for an IPv6 range by first IP (IP1) or 'del all'.

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

Syntax

`ip6 Bandwidth [on/off/default tx_rate rx_rate/status/show]`

`ip6 Bandwidth [add/del] [IP1-IP2] [tx][rx][shared]`

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.

<code>default <tx> <rx></code>	It means to set the default transmission (tx), receiving (rx) rate of bandwidth limit (0-30000 Kbps/Mbps).
<code>status</code>	It means to display the current settings.
<code>show</code>	It means to display all IP range bandwidth limit settings.
<code>add</code>	It means to add the bandwidth limit for an IPv6 range. <IP1-IP2> - Specify a range for IPv6 addresses.
<code>del</code>	It means to delete the bandwidth limit for an IPv6 range by first IP (IP1) or 'del all'.

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

```

Telnet Command: ipf view

IPF users to view the version of the IP filter, to view/set the log flag, to view the running IP filter rules.

Syntax

`ipf view [-VcdhrtzZ]`

Syntax Description

Parameter	Description
<code>-V</code>	It means to show the version of this IP filter.
<code>-c</code>	It means to show the running call filter rules.
<code>-d</code>	It means to show the running data filter rules.
<code>-h</code>	It means to show the hit-number of the filter rules.
<code>-r</code>	It means to show the running call and data filter rules.
<code>-t</code>	It means to display all the information at one time.
<code>-z</code>	It means to clear a filter rule's statistics.
<code>-Z</code>	It means to clear IP filter's gross statistics.

Example

```

> ipf view -V -c -d
ipf: IP Filter: v3.3.1 (1824)
Kernel: IP Filter: v3.3.1
Running: yes
Log Flags: 0x80947278 = nonip
Default: pass all, Logging: available

```

Telnet Command: ipf set

This command is used to set general rule for firewall.

Syntax

ipf set *[Options]*

ipf set *[SET_NO] rule [RULE_NO] [Options]*

Syntax Description

Parameter	Description
<i>Options</i>	There are several options provided here, such as <i>-v</i> , <i>-c [SET_NO]</i> , <i>-d [SET_NO]</i> ,... and etc.
<i>SET_NO</i>	It means to specify the index number (from 1 to 12) of filter set.
<i>RULE_NO</i>	It means to specify the index number (from 1 to 7) of filter rule set.
<i>-v</i>	Type <i>"-v"</i> to view the configuration of general set.
<i>-c [SET_NO]</i>	It means to setup Call Filter, e.g., <i>-c 2</i> . The range for the index number you can type is <i>"0"</i> to <i>"12"</i> (0 means "disable").
<i>-d [SET_NO]</i>	It means to setup Data Filter, e.g., <i>-d 3</i> . The range for the index number you can type is <i>"0"</i> to <i>"12"</i> (0 means "disable").
<i>-l [VALUE]</i>	It means to setup Log Flag, e.g., <i>-l 2</i> Type <i>"0"</i> to disable the log flag. Type <i>"1"</i> to display the log of passed packet. Type <i>"2"</i> to display the log of blocked packet. Type <i>"3"</i> to display the log of non-matching packet.
<i>-p [VALUE]</i>	It means to setup actions for packet not matching any rule, e.g., <i>-p 1</i> Type <i>"0"</i> to let all the packets pass; Type <i>"1"</i> to block all the packets.
<i>-R [v4/v6][Enable/Disable]</i>	: Accept routing packet from WAN
<i>-L [VALUE]</i>	It means to enable/disable Strict Security Firewall. 0:Disable, 1:Enable
<i>-C [VALUE]</i>	It means to set code page. code page number (? for more information).
<i>-M [APPE_NO]</i>	It means to set APPE for packets not matching any rule.
<i>-U [URL_NO]</i>	It means to set URL Content Filter for packets not matching any rule.
<i>-W [WEB_NO]</i>	It means to set WEB Content Filter for packets not matching any rule.
<i>-D [DNS_NO]</i>	It means to set DNS Filter for packet not matching any rule.
<i>-g [VALUE]</i>	It means to set DNS Filter syslog. 0:Disable 1:Enable
<i>-a [AD_SET]</i>	It means to configure the advanced settings.
<i>-f [VALUE]</i>	It means to accept large incoming fragmented UDP or ICMP packets. 0:Disable, 1:Enable
<i>-t [VALUE]</i>	It means to enable Transparent Mode.
<i>-E [VALUE]</i>	It means to set the session limitation max count. VALUE : 0-32000
<i>-Q [VALUE]</i>	It means to set the QoS class.

The value from 0 to 4. 0:None, 1:Class 1, 2:Class 2, 3:Class 3, 4:Default Class
--

Example

```

> ipf set -c 1 #set call filter start from set 1
Setting saved.

> ipf set -d 2 #set data filter start from set 2
Setting saved.
> ipf set -v

Call Filter: Enable (Start Filter Set = 1)
Data Filter: Enable (Start Filter Set = 2)
Log Flag   : Disable

Actions for packet not matching any rule:
Pass or Block      : Pass
CodePage           : ANSI(1252)-Latin I
Max Sessions Limit: 32000
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    : 1440
DrayTek Banner     : Enable
-----
Accept large incoming fragmented UDP or ICMP packets: Enable
Transparent Mode   : Disable
-----
Block routing packet from WAN:
[ ] IPv4
[v] IPv6
-----
[v] Enable Strict Security Firewall
>

```

Telnet Command: ipf rule

This command is used to set filter rule for firewall.

Syntax

```
ipf rule s r [-<command> <parameter> / ...
```

```
ipf rule s r -v
```

Syntax Description

Parameter	Description
s	Such word means Filter Set, range form 1-12.

<i>r</i>	Such word means Filter Rule, range from 1-7.
<i><Command><parameter></i>	The following lists all of the available commands with parameters.
<i>-e</i>	It means to enable or disable the rule setting. 0- disable 1- enable
<i>-D [value]</i>	It means to set direction. 0, LAN//DMZ/RT/VPN -> WAN 1, WAN -> LAN/DMZ/RT/VPN 2, LAN/DMZ/RT/VPN -> LAN/DMZ/RT/VPN
<i>-s o:g <obj></i>	It means to specify source IP object and IP group. o - indicates "object". g - indicates "group". obj - indicates index number of object or index number of group. Available settings range from 1-192. For example, "-s g 3" means the third source IP group profile.
<i>-s u <Address Type> <Start IP Address> <End IP Address> / <Address Mask></i>	It means to configure source IP address including address type, start IP address, end IP address and address mask. u - It means "user defined". <i>Address Type</i> - Type the number (representing different address type). 0 - Subnet Address 1 - Single Address 2 - Any Address 3 - Range Address Example: Set Subnet Address => -s u 0 192.168.1.10 255.255.255.0 Set Single Address => -s u 1 192.168.1.10 Set Any Address => -s u 2 Set Range Address => -s u 3 192.168.1.10 192.168.1.15
<i>-d o:g <obj></i>	It means to specify destination IP object and IP group. o - indicates "object". g - indicates "group" <obj>- indicates index number of object or index number of group. Available settings range from 1-192. For example, "-d g 1" means the first destination IP group profile.
<i>-d u <Address Type> <Start IP Address> <End IP Address> / <Address Mask></i>	It means to configure destination IP address including address type, start IP address, end IP address and address mask. u - It means "user defined". <i>Address Type</i> - 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"

	<p><obj> - indicates index number of object or index number of group. Available settings range from 1-96. For example, "-S 0 1" means the first service type object profile.</p>
<p>-S u <protocol> <source_port__value> <destination_port_vale></p>	<p>It means to configure advanced settings for Service Type, such as protocol and port range. u - it means "user defined". <protocol> - It means TCP(6),UDP(17), TCP/UDP(255). <source_port__value> - 1 - Port OP, range is 0-3. 0:=, 1:!=, 2:>, 3:< 3 - Port range of the Start Port Number, range is 1-65535. 5 - Port range of the End Port Number, range is 1-65535. <destination_port_value>: 2 - Port OP, range is 0-3, 0:=, 1:!=, 2:>, 3:< 4 - Port range of the Start Port Number, range is 1-65535. 6 - Port range of the End Port Number, range is 1-65535.</p>
<p>-f <value></p>	<p>It means to set the fragment type. 0 - Don't care 1 - Unfragmented 2 - Fragmented 3 - Too Short</p>
<p>-F</p>	<p>It means the Filter action you can specify. 0 -Pass Immediately, 1 - Block Immediately, 2 - Pass if no further match, 3 - Block if no further match.</p>
<p>-m <value></p>	<p>It means to set the MAC Bind IP type. 0 - Non-Strict 1 - Strict</p>
<p>-L <value></p>	<p>It means to set number of sessions control. 0 ~ 30000</p>
<p>-q <value></p>	<p>It means the classification for QoS. 1- Class 1, 2 - Class 2, 3 - Class 3, 4 - Other</p>
<p>-l <wan><log flag></p>	<p>It means load balance policy. Such function is used for "debug" only.</p>
<p>-E <value></p>	<p>It means to enable APP Enforcement. 1 - Enable 0 - Disable</p>
<p>-a<index><log flag></p>	<p>It means to specify which APP Enforcement profile will be applied. <index> - Available settings range from 0 ~ 32. "0" means no profile will be applied. <log flag> - Enable (1) the syslog; disable (0) the syslog.</p>
<p>-u<index><log flag></p>	<p>It means to specify which URL Content Filter profile will be applied. <index> - Available settings range from 0 ~ 8. "0" means no profile will be applied. <log flag> - Enable (1) the log; disable (0) the log</p>
<p>-w<index><log flag></p>	<p>It means to specify which web content filter profile will be applied.</p>

	<p><index> - Available settings range from 0 ~ 8. "0" means no profile will be applied.</p> <p><log flag> - Enable (1) the log; disable (0) the log</p>
-n<index><log flag>	<p>It means to specify which DNS filter profile will be applied.</p> <p><index> - Available settings range from 0 ~ 8. "0" means no profile will be applied.</p> <p><log flag> - Enable (1) the log; disable (0) the log</p>
-N <value>	<p>It means to set number of the next filter set.</p> <p>0 - 12</p>
-c <0-20>	<p>It means to set code page. Different number represents different code page.</p> <p>0. None</p> <p>1. ANSI(1250)-Central Europe</p> <p>2. ANSI(1251)-Cyrillic</p> <p>3. ANSI(1252)-Latin I</p> <p>4. ANSI(1253)-Greek</p> <p>5. ANSI(1254)-Turkish</p> <p>6. ANSI(1255)-Hebrew</p> <p>7. ANSI(1256)-Arabic</p> <p>8. ANSI(1257)-Baltic</p> <p>9. ANSI(1258)-Viet Nam</p> <p>10. OEM(437)-United States</p> <p>11. OEM(850)-Multilingual Latin I</p> <p>12. OEM(860)-Portuguese</p> <p>13. OEM(861)-Icelandic</p> <p>14. OEM(863)-Canadian French</p> <p>15. OEM(865)-Nordic</p> <p>16. ANSI/OEM(874)-Thai</p> <p>17. ANSI/OEM(932)-Japanese Shift-JIS</p> <p>18. ANSI/OEM(936)-Simplified Chinese GBK</p> <p>19. ANSI/OEM(949)-Korean</p> <p>20. ANSI/OEM(950)-Traditional Chinese Big5</p>
-C <Windows Size> <Session_Timeout>	<p>It means to set Window size and Session timeout (Minute).</p> <p><Windows Size> - Available settings range from 0 ~ 65535.</p> <p><Session_Timeout> - Make the best utilization of network resources.</p>
-v	It is used to show current filter/rule settings.
-M <Your Comments>	It means to set comment for the set rule.
-U <up or down>	<p>It means to move Up or Down the order of a rule in the filter set.</p> <p>0 - up</p> <p>1 - down</p>

Example

```

> ipf rule 2 1 -e 1 -M "Your Comments" -s "o 1" -d "o 2" -S "o 1" -F "1 1"
> ipf rule 2 1 -v

Filter Set 2 Rule 1:

Status : Enable
Comments: Your Comments
Index(1-15) in Schedule Setup: <null>, <null>, <null>, <null>

```

```

Direction      : LAN/DMZ/RT/VPN -> 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 : 32000
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.

Syntax

```

ipf flowtrack set [-re]
ipf flowtrack view [-f]
ipf flowtrack [-i][/-p][/-t]

```

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.
- i [IP address]	It means to specify IP address (e.g., -i 192.168.2.55).
-p[value]	It means to type a port number (e.g., -p 1024). Available settings are 0 ~ 65535.
-t [value]	It means to specify a protocol (e.g., -t tcp).

Available settings include: <i>tcp</i> <i>udp</i> <i>icmp</i>
--

Example

```
>ipf flowtrack set -r
Refresh the flowstate ok
> ipf flowtrack view -f
Start to show the flowtrack sessions state:

ORIGIN>> 192.168.1.11:59939 ->      8.8.8.8: 53 ,ifno=0
REPLY >>      8.8.8.8: 53 -> 192.168.1.11:59939 ,ifno=3
          proto=17, age=93023180(3920), flag=203
ORIGIN>> 192.168.1.11:15073 ->      8.8.8.8: 53 ,ifno=0
REPLY >>      8.8.8.8: 53 -> 192.168.1.11:15073 ,ifno=3
          proto=17, age=93025100(2000), flag=203
ORIGIN>> 192.168.1.11: 7247 ->      8.8.8.8: 53 ,ifno=0
REPLY >>      8.8.8.8: 53 -> 192.168.1.11: 7247 ,ifno=3
          proto=17, age=93020100(7000), flag=203

End to show the flowtrack sessions state
> ipf flowtrack set -e
Current flow_enable=0
> ipf flowtrack set -e
Curretn flow_enable=1
```

Telnet Command: Log

This command allows users to view log for WAN interface such as call log, IP filter log, flush log buffer, etc.

Syntax

`log [-cfhiptwx?] [-F a | c | f | w]`

Syntax Description

Parameter	Description
<i>-c</i>	It means to show the latest call log.
<i>-f</i>	It means to show the IP filter log.
<i>-F</i>	It means to show the flush log buffer. a: flush all logs c: flush the call log f: flush the IP filter log w: flush the WAN log
<i>-h</i>	It means to show this usage help.
<i>-p</i>	It means to show PPP/MP log.
<i>-t</i>	It means to show all logs saved in the log buffer.
<i>-w</i>	It means to show WAN log.
<i>-x</i>	It means to show packet body hex dump.

Example

```

> log -w
25:36:25.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
    Client IP      = 0.0.0.0
    Your IP        = 0.0.0.0
    Next server IP = 0.0.0.0
    Relay agent IP = 0.0.0.0
25:36:33.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
    Client IP      = 0.0.0.0
    Your IP        = 0.0.0.0
    Next server IP = 0.0.0.0
    Relay agent IP = 0.0.0.0
25:36:41.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
    Client IP      = 0.0.0.0
    Your IP        = 0.0.0.0
    Next server IP = 0.0.0.0
    Relay agent IP = 0.0.0.0
25:36:49.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
    Client IP      = 0.0.0.0
    Your IP        = 0.0.0.0
    Next server IP = 0.0.0.0
    Relay agent IP = 0.0.0.0
25:36:57.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
    Client IP      = 0.0.0.0
    Your IP        = 0.0.0.0
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---

```

Telnet Command: mngt ftpport

This command allows users to set FTP port for management.

Syntax

mngt ftpport [*FTP port*]

Syntax Description

Parameter	Description
<i>FTP port</i>	It means to type the number for FTP port. The default setting is 21.

Example

```

> mngt ftpport 21
% Set FTP server port to 21 done.

```

Telnet Command: mngt httpport

This command allows users to set HTTP port for management.

Syntax

mngt httpport [*Http port*]

Syntax Description

Parameter	Description
<i>Http port</i>	It means to enter the number for HTTP port. The default setting is 80.

Example

```
> mngt httpport 80
% Set web server port to 80 done.
```

Telnet Command: mngt httpsport

This command allows users to set HTTPS port for management.

Syntax

```
mngt httpsport [Https port]
```

Syntax Description

Parameter	Description
<i>Https port</i>	It means to type the number for HTTPS port. The default setting is 443.

Example

```
> mngt httpsport 443
% Set web server port to 443 done.
```

Telnet Command: mngt telnetport

This command allows users to set telnet port for management.

Syntax

```
mngt telnetport [Telnet port]
```

Syntax Description

Parameter	Description
<i>Telnet port</i>	It means to type the number for telnet port. The default setting is 23.

Example

```
> mngt telnetport 23
% Set Telnet server port to 23 done.
```

Telnet Command: mngt sshport

This command allows users to set SSH port for management.

Syntax

```
mngt sshport [ssh port]
```

Syntax Description

Parameter	Description
<i>ssh port</i>	It means to type the number for SSH port. The default setting is 22.

Example

```
> mngt sshport 23
```

```
% Set ssh port to 23 done.
```

Telnet Command: mngt noping

This command is used to pass or block Ping from LAN PC to the internet.

Syntax

mngt noping *[on]*

mngt noping *[off]*

mngt noping *[viewlog]*

mngt noping *[clearlog]*

Syntax Description

Parameter	Description
<i>on</i>	All PING packets will be forwarded from LAN PC to Internet.
<i>off</i>	All PING packets will be blocked from LAN PC to Internet.
<i>viewlog</i>	It means to display a log of ping action, including source MAC and source IP.
<i>clearlog</i>	It means to clear the log of ping action.

Example

```
> mngt noping off  
No Ping Packet Out is OFF!!
```

Telnet Command: mngt defenseworm

This command can block specified port for passing through the router.

Syntax

mngt defenseworm *[on]*

mngt defenseworm *[off]*

mngt defenseworm *[add port]*

mngt defenseworm *[del port]*

mngt defenseworm *[viewlog]*

mngt defenseworm *[clearlog]*

Syntax Description

Parameter	Description
<i>on</i>	It means to activate the function of defense worm packet out.
<i>off</i>	It means to inactivate the function of defense worm packet out.
<i>add port</i>	It means to add a new TCP port for block.
<i>del port</i>	It means to delete a TCP port for block.
<i>viewlog</i>	It means to display a log of defense worm packet, including source MAC and source IP.
<i>clearlog</i>	It means to remove the log of defense worm packet.

Example

```
> mngt defenseworm add 21
Add TCP port 21
Block TCP port list: 135, 137, 138, 139, 445, 21
> mngt defenseworm del 21
Delete TCP port 21
Block TCP port list: 135, 137, 138, 139, 445
```

Telnet Command: mngt rmtcfg

This command can allow the system administrators to login from the Internet. By default, it is not allowed.

Syntax

`mngt rmtcfg [status]`

`mngt rmtcfg [enable]`

`mngt rmtcfg [disable]`

`mngt rmtcfg [http/https/ftp/telnet/ssh/tr069] [on/off]`

Syntax Description

Parameter	Description
<i>status</i>	It means to display current setting for your reference.
<i>enable</i>	It means to allow the system administrators to login from the Internet.
<i>disable</i>	It means to deny the system administrators to login from the Internet.
<i>http/https/ftp/telnet/ssh/tr069</i>	It means to specify one of the servers/protocols for enabling or disabling.
<i>on/off</i>	on - enable the function. off - disable the function.

Example

```
> mngt rmtcfg ftp on
Enable server fail
Remote configure function has been disabled
please enable by enter mngt rmtcfg enable

> mngt rmtcfg enable
%% Remote configure function has been enabled.
> mngt rmtcfg ftp on
%% FTP server has been enabled.
```

Telnet Command: mngt lanaccess

This command allows users to manage accessing into Vigor router through LAN port.

Syntax

`mngt lanaccess -e [0/1] -s [value] -i [value]`

`mngt lanaccess -l`

`mngt lanaccess -E`

`mngt lanaccess -f`

mngt lanaccess -d
 mngt lanaccess -v
 mngt lanaccess -h

Syntax Description

Parameter	Description
-e[0/1]	It means to enable/disable the function. 0-disable the function. 1-enable the function.
-s[value]	It means to specify service offered. Available values include: FTP, HTTP, HTTPS, TELNET, SSH, None, All
-i[value]	It means the interface which is allowed to access. Available values include: LAN2~LAN4, IP Routed Subnet, None, All Note: LAN1 is always allowed for accessing into the router.
-l	It means to indicate the index number (1 ~ 192) of IP object which is allowed to access vigor router.
-E	It means to enable (1) / disable (0) a specific IP to access vigor router.
-f	It means to flush all of the settings.
-d	It means to restore the factory default settings.
-v	It means to view current settings.
-h	It means to get the usage of such command.

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
  - TR069:No
* Subnet:
  - LAN 1: disabled
    - Specific IP(IP object:0) is disabled
  - LAN 2: disabled
    - Specific IP(IP object:0) is disabled
  - LAN 3: enabled
    - Specific IP(IP object:0) is disabled
  - LAN 4: disabled
    - Specific IP(IP object:0) is disabled
  - IP Routed Subnet: disabled
    - Specific IP(IP object:0) is disabled
```

Telnet Command: mngt echoicmp

This command allows users to reject or accept PING packets from the Internet.

Syntax

mngt echoicmp *[enable]*

mngt echoicmp *[disable]*

Syntax Description

Parameter	Description
<i>enable</i>	It means to accept the echo ICMP packet.
<i>disable</i>	It means to drop the echo ICMP packet.

Example

```
> mngt echoicmp enable
%% Echo ICMP packet enabled.
```

Telnet Command: mngt accesslist

This command allows you to specify that the system administrator can login from a specific host or network. A maximum of three IPs/subnet masks is allowed.

Syntax

mngt accesslist *list*

mngt accesslist *add [index][IP Object Index]*

mngt accesslist *remove [index]*

mngt accesslist *flush*

Syntax Description

Parameter	Description
<i>list</i>	It can display current setting for your reference.
<i>add</i>	It means adding a new entry.
<i>index</i>	It means to specify the number of the entry.
<i>ip object index</i>	It means to specify an IP address.
<i>remove</i>	It means to delete the selected item.
<i>flush</i>	It means to remove all the settings in the access list.

Example

```
> mngt accesslist add 1 1
%% Set OK.
> mngt accesslist list
%% Access list :
  [Index]      [IP Object Index]      [IP/CIDR or StartIP ~ EndIP]
=====
  1           1                    Please setting index=1 for IP Object
```

Telnet Command: mngt snmp

This command allows you to configure SNMP for management.

Syntax

`mngt snmp [-<command> <parameter> | ...]`

Syntax Description

Parameter	Description
<code>[<command> <parameter> ...]</code>	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
<code>-e <1/2></code>	1: Enable the SNMP function. 2: Disable the SNMP function.
<code>-g<Community name></code>	It means to set the name for getting community by typing a proper character. (max. 23 characters)
<code>-s <Community name></code>	It means to set community by typing a proper name. (max. 23 characters)
<code>-m <IP address></code>	It means to set one host as the manager to execute SNMP function. Please type in IPv4 address to specify certain host.
<code>-t <Community name></code>	It means to set trap community by typing a proper name. (max. 23 characters)
<code>-n <IP address></code>	It means to set the IPv4 address of the host that will receive the trap community.
<code>-T <seconds></code>	It means to set the trap timeout <0-999>.
<code>-V</code>	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: msubnet switch

This command is used to configure multi-subnet.

Syntax

`msubnet switch [2/3/4][On/Off]`

Syntax Description

Parameter	Description
<code>2/3/4</code>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<code>On/Off</code>	On means turning on the subnet for the specified LAN interface.

Off means turning off the subnet.

Example

```
> msubnet switch 2 On
% LAN2      Subnet On!
```

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.

Telnet Command: msubnet addr

This command is used to configure IP address for the specified LAN interface.

Syntax

`msubnet addr [2/3/4][IP address]`

Syntax Description

Parameter	Description
<i>2/3/4</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<i>IP address</i>	Type the private IP address for the specified LAN interface.

Example

```
> msubnet addr 2 192.168.5.1
% Set LAN2 subnet IP address done !!!
```

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.

Telnet Command: msubnet nmask

This command is used to configure net mask address for the specified LAN interface.

Syntax

`msubnet nmask [2/3/4][IP address]`

Syntax Description

Parameter	Description
<i>2/3/4</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<i>IP address</i>	Type the subnet mask address for the specified LAN interface.

Example

```
> msubnet nmask 2 255.255.0.0
% Set LAN2 subnet mask done !!!
```

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.

Telnet Command: msubnet status

This command is used to display current status of subnet.

Syntax

msubnet status [2/3/4]

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.

Syntax

msubnet dhcps [2/3/4][On/Off]

Syntax Description

Parameter	Description
2/3/4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
On/Off	On means enabling the DHCP server for the specified LAN interface. Off means disabling the DHCP server.

Example

```
> msubnet dhcps 3 off
% LAN3      Subnet DHCP Server disabled!

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet nat

This command is used to configure the subnet for NAT or Routing usage.

Syntax

`msubnet nat [2/3/4] [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.

Syntax

`msubnet gateway [2/3/4] [Gateway IP]`

Syntax Description

Parameter	Description
<i>2/3/4</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<i>Gateway IP</i>	Specify an IP address as the gateway IP.

Example

```
> msubnet gateway 2 192.168.1.13
% Set LAN2 Dhcp Gateway IP done !!!

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet ipcnt

This command is used to defined the total number allowed for each LAN interface.

Syntax

`msubnet ipcnt [2/3/4] [IP counts]`

Syntax Description

Parameter	Description
<i>2/3/4/5</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<i>IP counts</i>	Specify a total number of IP address allowed for each LAN interface. The available range is from 0 to 220.

Example

```
> msubnet ipcnt 2 15
This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet talk

This command is used to establish a route between two LAN interfaces.

Syntax

`msubnet talk [1/2/3/4] [1/2/3/4] [On/Off]`

Syntax Description

Parameter	Description
<i>1/2/3/4</i>	It means LAN interface. 1=LAN1 2=LAN2 3=LAN3 4=LAN4
<i>On/Off</i>	On - It means Off - It means

Example

```
> msubnet talk 1 2 on
% Enable routing between LAN1          and LAN2          !

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
> msubnet talk ?
% msubnet talk <1/2/3/4> <1/2/3/4> <On/Off>
% where 1:LAN1, 2:LAN2, 3:LAN3, 4:LAN4
% Now:
%           LAN1  LAN2  LAN3  LAN4
% LAN1           V
% LAN2           V
% LAN3           V
% LAN4           V
>
```

Telnet Command: msubnet startip

This command is used to configure a starting IP address for DCHP.

Syntax

`msubnet startip [2/3/4] [Gateway IP]`

Syntax Description

Parameter	Description
<i>2/3/4</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<i>Gateway IP</i>	Type an IP address as the starting IP address for a subnet.

Example

```
> ms subnet startip 2 192.168.2.90
%Set LAN2 Dhcp Start IP done !!!

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
> ms subnet startip ?
% ms subnet startip <2/3/4> <Gateway IP>
% Now: LAN2 192.168.2.90; LAN3 192.168.3.10; LAN4 192.168.4.10; LAN5
192.168.5.1
0; LAN6 192.168.6.10
```

Telnet Command: ms subnet pppip

This command is used to configure a starting IP address for PPP connection.

Syntax

`msubnet pppip [2/3/4] [Start IP]`

Syntax Description

Parameter	Description
<i>2/3/4/5</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

```
> ms subnet pppip 2 192.168.2.250
% Set LAN2 PPP(IPCP) Start IP done !!!

This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
> ms subnet pppip ?
% ms subnet pppip <2/3/4> <Start IP>
% Now: LAN2 192.168.2.250; LAN3 192.168.3.200; LAN4 192.168.4.200
```

Telnet Command: ms subnet nodetype

This command is used to specify the type for node which is required by DHCP option.

Syntax

`msubnet nodetype [2/3/4/5][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

```
> ms subnet nodetype ?
% ms subnet 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

> ms subnet nodetype 2 1
% Set LAN2 Dhcp Node Type done !!!

> ms subnet nodetype ?
% ms subnet 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: ms subnet primWINS

This command is used to configure primary WINS server.

Syntax

`msubnet primWINS [2/3/4] [WINS IP]`

Syntax Description

Parameter	Description
<i>2/3/4</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<i>WINS IP</i>	Type the IP address as the WINS IP.

Example

```
> ms subnet primWINS ?
% ms subnet 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.

Syntax

`msubnet secWINS [2/3/4] [WINS IP]`

Syntax Description

Parameter	Description
<i>2/3/4</i>	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
<i>WINS IP</i>	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.

Syntax

`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/DMZ/IP Routed Subnet.

Syntax

```
msubnet mtu [interface][value]
```

Syntax Description

Parameter	Description
<i>interface</i>	Available settings include LAN1~LAN4, IP_Routed_Subnet.
<i>value</i>	1000 ~ 1492(Bytes)

Example

```

> msubnet mtu LAN1 1492%
  Set LAN1 subnet mtu as 1492
> msubnet mtu ?
Usage:

>msubnet mtu <interface> <value>

<interface>: LAN1~LAN4,IP_Routed_Subnet, <value>:    1000 ~ 1496 (Bytes),
de
fault: 1500 (Bytes)

  e.x: >msubnet mtu LAN1 1492

Current Settings:

LAN1 MTU:                1492 (Bytes)
LAN2 MTU:                1500 (Bytes)
LAN3 MTU:                1500 (Bytes)
LAN4 MTU:                1500 (Bytes)
IP Routed Subnet MTU:   1500 (Bytes)

```

Telnet Command: object ip obj

This command is used to create an IP object profile.

Syntax

object ip obj setdefault
 object ip obj *INDEX* -v
 object ip obj *INDEX* -n *NAME*
 object ip obj *INDEX* -i *INTERFACE*
 object ip obj *INDEX* -s *INVERT*
 object ip obj *INDEX* -a *TYPE* [*START_IP*] [*END/MASK_IP*]

Syntax Description

Parameter	Description
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number of the specified object profile.
-v	It means to view the information of the specified object profile. Example: <i>object ip obj 1 -v</i>
-n <i>NAME</i>	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: <i>object ip obj 9 -n bruce</i>
-i <i>INTERFACE</i>	It means to define an interface for the IP object. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=3, means WAN Example: <i>object ip obj 8 -i 0</i>
-s <i>INVERT</i>	It means to set invert selection for the object profile. INVERT=0, means disableing the function. INVERT=1, means enabling the function. Example: <i>object ip obj 3 -s 1</i>
-a <i>TYPE</i>	It means to set the address type and IP for the IP object profile. TYPE=0, means Mask TYPE=1, means Single TYPE=2, means Any TYPE=3, means Rang TYPE=4, means Mac Example: <i>object ip obj 3 -a 2</i>
[<i>START_IP</i>]	When the TYPE is set with 2, you have to type an IP address as a starting point and another IP address as end point. Type an IP address.
[<i>END/MASK_IP</i>]	Type an IP address (different with <i>START_IP</i>) as the end IP address.

Example

```
> object ip obj 1 -n marketing
OK.

> object ip obj 1 -a 1 192.168.1.45
OK.

> 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]
MAC Address:[00:00:00:00:00:00]
Invert Selection:[0]

```

Telnet Command: object ip grp

This command is used to integrate several IP objects under an IP group profile.

Syntax

object ip grp setdefault

object ip grp INDEX -v

object ip grp INDEX -n NAME

object ip grp INDEX -i INTERFACE

object ip grp INDEX -a IP_OBJ_INDEX

Syntax Description

Parameter	Description
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number of the specified group profile.
<i>-v</i>	It means to view the information of the specified group profile. Example: <i>object ip grp 1 -v</i>
<i>-n NAME</i>	It means to define a name for the IP group. NAME: Type a name with less than 15 characters. Example: <i>object ip grp 8 -n bruce</i>
<i>-i INTERFACE</i>	It means to define an interface for the IP group. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=3, 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 -a 1 2
IP Group Profile 2
Name   :[First]
Interface:[Lan]
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]

Set ok!
```

Telnet Command: object ipv6 obj

This command is used to create an IPv6 object profile.

Syntax

obj ipv6 obj *setdefault*

obj ipv6 obj *INDEX -v*

obj ipv6 obj *INDEX -n NAME*

obj ipv6 obj *INDEX -s INVERT*

obj ipv6 obj *INDEX -e MATCH_TYPE*

obj 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 IPv6 object. NAME: Type a name with less than 15 characters. Example: <i>object ipv6 obj 9 -n bruce</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 MATCH_TYPE</i>	It means to set the match type of ipv6 object profile. 0:128 Bits, 1:Suffix 64 Bits Interface ID
<i>-a TYPE</i>	It means to set the address type for the IPv6 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>
<i>[START_IP]</i>	When the TYPE is set with 2, you have to type an IPv6 address as a starting point and another IP address as end point. Type an IPv6 address as the starting point.
<i>[END/ Prefix Length]</i>	Type an IPv6 address (different with START_IP) as the end IPv6 address or the prefix length of the IPv6 address.

Example

```
> obj ipv6 obj 9 -n bruce
Setting saved.

> obj ipv6 obj 3 -s 1
Setting saved.
```

```

> obj ipv6 obj 3 -e 1
You can not set 64 bits Interface ID for Subnet type.

Setting saved.

> 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 IPv6 objects under an IPv6 group profile.

Syntax

`ipv6 grp setdefault`

`ipv6 grp INDEX -v`

`ipv6 grp INDEX -n NAME`

`ipv6 grp INDEX -a IP_OBJ_INDEX`

Syntax Description

Parameter	Description
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number of the specified group profile.
-v	It means to view the information of the specified group profile. Example: <code>object ip grp 1 -v</code>
-n <i>NAME</i>	It means to define a name for the IPv6 group. NAME: Type a name with less than 15 characters. Example: <code>object ip grp 8 -n bruce</code>
-a <i>IP_OBJ_INDEX</i>	It means to specify IPv6 object profiles for the group profile. Example: <code>:object ip grp 3 -a 1 2 3 4 5</code> The IP object profiles with index number 1,2,3,4 and 5 will be group under such profile.

Example

```

> object ipv6 grp 8 -n bruce
IPv6 Group Profile 8
Name      :[bruce]
Included ip object index:
[0:][0]
[1:][0]
[2:][0]

```

```

[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]
> object ipv6 grp 8 -a 1 2 3 4 5
IPv6 Group Profile 8
Name    :[bruce]
Included ip object index:
[0:][1]
[1:][2]
[2:][3]
[3:][4]
[4:][5]
[5:][0]
[6:][0]
[7:][0]

```

Telnet Command: **object service obj**

This command is used to create service object profile.

Syntax

object service obj *setdefault*

object service obj *INDEX -v*

object service obj *INDEX -n NAME*

object service obj *INDEX -p PROTOCOL*

object service obj *INDEX -s CHK [START_P] [END_P]*

object service obj *INDEX -d CHK [START_P] [END_P]*

Syntax Description

Parameter	Description
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number of the specified service object profile.
<i>-v</i>	It means to view the information of the specified service object profile. Example: <i>object service obj 1 -v</i>
<i>-n NAME</i>	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: <i>object service obj 9 -n bruce</i>
<i>-p 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 =58, means ICMPv6 PROTOCOL =255, means TCP/UDP Other values mean other protocols. Example: <i>object service obj 8 -p 1</i>
<i>CHK</i>	It means the check action for the port setting.

	<p>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.</p> <p>1=not equal(!=), when the starting port and ending port values are the same, it indicates all the ports except the port defined here; when the starting port and ending port values are different, it indicates that all the ports except the range defined here are available for this service type.</p> <p>2=larger(>), the port number greater than this value is available..</p> <p>3=less(<), the port number less than this value is available for this profile.</p>
<code>-s CHK [START_P] [END_P]</code>	<p>It means to set source port check and configure port range (1~65565) for TCP/UDP.</p> <p>END_P, type a port number to indicate source port.</p> <p>Example: <code>object service obj 3 -s 0 100 200</code></p>
<code>-d CHK [START_P] [END_P]</code>	<p>It means to set destination port check and configure port range (1~65565) for TCP/UDP.</p> <p>END_P, type a port number to indicate destination port.</p> <p>Example: <code>object service obj 3 -d 1 100 200</code></p>

Example

```

> object service obj 1 -n limit
> object service obj 1 -p 255
> object service obj 1 -s 1 120 240
> object service obj 1 -d 1 200 220
> object service obj 1 -v
Service Object Profile 1
Name      :[limit]
Protocol  :[TCP/UDP]
Source port check action:[!=]
Source port range:[120~240]
Destination port check action:[!=]
Destination port range:[200~220]

```

Telnet Command: object service grp

This command is used to integrate several service objects under a service group profile.

Syntax

`object service grp setdefault`

`object service grp INDEX -v`

`object service grp INDEX -n NAME`

`object service grp INDEX -a SER_OBJ_INDEX`

Syntax Description

Parameter	Description
<code>setdefault</code>	It means to return to default settings for all profiles.
<code>INDEX</code>	It means the index number of the specified group profile.
<code>-v</code>	It means to view the information of the specified group profile. Example: <code>object service grp 1 -v</code>
<code>-n NAME</code>	It means to define a name for the service group.

	NAME: Type a name with less than 15 characters. Example: <i>object service grp 8 -n bruce</i>
<i>-a SER_OBJ_INDEX</i>	It means to specify service object profiles for the group profile. Example: <i>:object service grp 3 -a 1 2 3 4 5</i> The service object profiles with index number 1,2,3,4 and 5 will be group under such profile.

Example

```
>object service grp 1 -n Grope_1
Service Group Profile 1
Name   :[Grope_1]
Included service object index:
[0:][0]
[1:][0]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]

>object service grp 1 -a 1 2
Service Group Profile 1
Name   :[Grope_1]
Included service object index:
[0:][1]
[1:][2]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]
```

Telnet Command: object kw

This command is used to create keyword profile.

Syntax

```
object kw obj setdefault
object kw obj show PAGE
object kw obj INDEX -v
object kw obj INDEX -n NAME
object kw obj INDEX -a CONTENTS
object kw obj INDEX -c
```

Syntax Description

Parameter	Description
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>show PAGE</i>	It means to show the contents of the specified profile. PAGE: type the page number.

<i>Show</i>	It means to show the contents for all of the profiles.
<i>INDEX</i>	It means the index number of the specified keyword profile.
<i>-v</i>	It means to view the information of the specified keyword profile.
<i>-n NAME</i>	It means to define a name for the keyword profile. NAME: Type a name with less than 15 characters.
<i>-a CONTENTS</i>	It means to set the contents for the keyword profile. Example: <i>object kw obj 40 -a test</i>
<i>-c</i>	It means to clear the contents of keyword object profile.

Example

```

> object kw obj 1 -n children
Profile 1
Name   :[children]
Content:[ ]
> object kw obj 1 -a gambling
Profile 1
Name   :[children]
Content:[gambling]

> object kw obj 1 -v
Profile 1
Name   :[children]
Content:[gambling]

```

Telnet Command: object fe

This command is used to create File Extension Object profile.

Syntax

`object fe show`

`object fe setdefault`

`object fe obj INDEX -v`

`object fe obj INDEX -n NAME`

`object fe obj INDEX -e CATEGORY/FILE_EXTENSION`

`object fe obj INDEX -d CATEGORY/FILE_EXTENSION`

Syntax Description

Parameter	Description
<i>show</i>	It means to show the contents for all of the profiles.
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number (from 1 to 8) of the specified file extension object profile.
<i>-v</i>	It means to view the information of the specified file extension object profile.
<i>-n NAME</i>	It means to define a name for the file extension object profile. NAME: Type a name with less than 15 characters.
<i>-e</i>	It means to enable the specific CATEGORY or FILE_EXTENSION.
<i>-d</i>	It means to disable the specific CATEGORY or FILE_EXTENSION

CATEGORY/FILE_EXTENSION	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", ".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", ".vrm", ".ace", ".arj", ".bzip2", ".bz2", ".cab", ".gz", ".gzip", ".rar", ".sit", ".zip", ".bas", ".bat", ".com", ".exe", ".inf", ".pif", ".reg", ".scr", ".torrent"
	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
[ ].vrm

-----

Compression category:
[ ].ace [ ].arj [ ].bzip2 [ ].bz2 [ ].cab [ ].gz [ ].gzip [ ].rar
[ ].sit [ ].zip

-----

Execution category:
[ ].bas [ ].bat [ ].com [ ].exe [ ].inf [ ].pif [ ].reg [ ].scr

```

Telnet Command: 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* -I *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 <i>[NAME]</i>	It means to define a name for the SMS object profile. NAME: Type a name with less than 15 characters.
-s <i>[Service Provider]</i>	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 <i>[Username]</i>	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 <i>[Password]</i>	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 <i>[Quota]</i>	Type 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>-I [Interval]</i>	It means to set the sending interval for the SMS to be delivered. Type the shortest time interval for the system to send SMS.
<i>-I [URL]</i>	It means to set the URL of SMS object profile 9 and 10.

Example

```

> object sms obj 1 -n CTC
> 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* -s *SMTP Server*

object mail obj *INDEX* -I *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>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 mail object profile.
<i>-v</i>	It means to view the information of the specified mail object profile.
<i>-n [Profile Name]</i>	It means to define a name for the mail object profile.

	<i>Profile Name</i> : Type a name with less than 15 characters.
<i>-s [SMTP Server]</i>	It means to set the IP address of the mail server.
<i>-l [Use SSL]</i>	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.
<i>-m [SMTP Port]</i>	It means to set the port number for SMTP server.
<i>-a [Sender Address]</i>	It means to set the e-mail address (e.g., johnwash@abc.com.tw) of the sender.
<i>-t Authentication</i>	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.
<i>-u Username</i>	Type a name for authentication. The maximum length of the name you can set is 31 characters.
<i>-p Password</i>	Type a password for authentication. The maximum length of the password you can set is 31 characters.
<i>-I Sending Interval</i>	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 mail obj INDEX -e Category Status

object mail 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 (這個項目應該要取消, 2133 沒有此功能); 5: CVM(這個項目應該要取消, 2133 沒有此功能)
<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 - (這個項目應該要取消, 2133 沒有此功能) 1: Limit Reached. For CVM -(這個項目應該要取消, 2133 網頁上沒有此功能) 1: CPE Offline; 2: Backup Fail; 3: Restore Fail; 4: FW Update Fail; 5: VPN Profile Setup Fail.

Example

```

> object noti obj 1 -n marketing
> object noti obj 1 -e 1 1
> object noti obj 1 -e 2 1
> object noti obj 1 -e 5 3
> object noti obj 1 -v
Profile Index: 1
Profile Name:[marketing]
      Category                Status
WAN                [v]Disconnected    [ ]Reconnected
VPN Tunnel         [v]Disconnected    [ ]Reconnected
Temperature Alert  [ ]Out of Range
WAN Budget Alert   [ ]Limit Reached ( 這個項目應該要取消, 2133 網頁上沒有此功能)
CVM Alert          [ ]CPE Offline ( 這個項目應該要取消, 2133 網頁上沒有此功能)
                  [ ]CPE Config Backup Fail
                  [v]CPE Config Restore Fail
                  [ ]CPE Firmware Fpgrade Fail
                  [ ]CPE VPN Profile Setup Fail

```

Telnet Command: object schedule

This command is used to create schedule object profile.

Syntax

object schedule set *[INDEX] option*

object schedule view *[INDEX]*

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 includes: -e , -c, -D, -T, -d, -a
<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: 1 ~ 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]</i> <i>[day/date/cycle_days]</i>	Set how often the schedule will be applied. [option] - 0: Once, 1: Weekdays, 2:Monthly, 3:Cycle days [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 [date] : 1-28 [cycle_days] : 1-30 If the [option] set cycle days, then must select which days to do cycle schedule example: To select cycle 10 days:

	> <i>object schedule set 1 -h 3 10</i> "
<i>view [INDEX]</i>	It means to show the content of the profile.
<i>setdefault</i>	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 "2017 4 18"
> 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) [ 2017 ]-[ 4 ]-[ 18 ]
    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
    [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, 100F, 100H, 10F, 10H, status]`

`port [wan1] [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 8021x [enable,disable,status,addport,delport]`

`port jumbo`

`port wanfc`

`port spoof [on, off, stat]`

`port mac_flush`

Syntax Description

Parameter	Description
<i>1, 2, 3, 4, all</i>	It means the number of LAN port.

<i>wan1</i>	It means the WAN1 interface.
<i>AN... 10H</i>	It means the physical type for the specific port. AN: auto-negotiate. 1000F: 1000M Full Duplex. 100F: 100M Full Duplex. 100H: 100M Half Duplex. 10F: 10M Full Duplex. 10H: 10M Half Duplex.
<i>status</i>	It means to view the Ethernet port status.
<i>wanfc</i>	It means to set WAN flow control.

Example

```
> port 1 100F
%Set Port 1 Force speed 100 Full duplex OK !!!
```

Telnet Command: portmuptime

This command allows you to set a time of keeping the session connection for specified protocol.

Syntax

portmuptime [*-<command>* *<parameter>* | ...]

Syntax Description

Parameter	Description
<i>[<command></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>-t <sec></i>	It means "TCP" protocol. <i><sec></i> : Type a number to set the TCP session timeout.
<i>-u <sec></i>	It means "UDP" protocol. <i><sec></i> : Type a number to set the UDP session timeout.
<i>-i <sec></i>	It means "IGMP" protocol. <i><sec></i> : Type a number to set the IGMP session timeout.
<i>-w <sec></i>	It means "TCP WWW" protocol. <i><sec></i> : Type a number to set the TCP WWW session timeout.
<i>-s <sec></i>	It means "TCP SYN" protocol. <i><sec></i> : Type a number to set the TCP SYN session timeout.
<i>-f</i>	It means to flush all portmaps (useful for diagnostics).
<i>-l <List></i>	List all settings.

Example

```
> portmuptime -t 86400 -u 300 -i 10
> portmuptime -l
----- Current setting -----
TCP Timeout   : 86400 sec.
UDP Timeout   : 300 sec.
IGMP Timeout  : 10 sec.
```

```
TCP WWW Timeout: 60 sec.
TCP SYN Timeout: 60 sec.
```

Telnet Command: ppa

This command allows you to configure PPA mode.

```
ppa [-<command> <parameter> | ... ]
```

```
ppa n [-<command> <parameter> | ... ]
```

Syntax Description

Parameter	Description
<i>[<command> <parameter> ...]</i>	The available commands with parameters are listed below. <i>[...]</i> means that you can type in several commands in one line.
<i>-m <mode></i>	Specify a mode. 1=auto 2=manual(traffic) 3=manual(qos) 4=manual(specific hosts) 0=disable
<i>-p <proto></i>	Specify a protocol. proto - 1-TCP; 2-UDP; 3-Both.
<i>-b 1/0</i>	Enable/disable TWO-way hardware acceleration.
<i>-M enable/disable</i>	Enable/disable the multicast hardware acceleration.
<i>-S</i>	Show multicast table in hardware acceleration.
<i>-v <view></i>	Show PPA_WAN_Table and PPA_LAN_Table for reference.
<i>-c</i>	Clean all settings.
ppa n - used in QoS or specific host	
<i>-l <rule></i>	Specify an index number of rule profile for QoS mode.
<i>-h <host></i>	Type an IP address for Specific Host mode.
<i>-s <start port></i>	Specify a starting port number for Specific Host mode.
<i>-e <end port></i>	Specify an ending port number for Specific Host mode
<i>-x</i>	Show hardware acceleration information.
<i>-k</i>	Clean the PPA table.

Example

```
> ppa -m 1 -p 1 -b 0
Set ok! The PPA mode is Auto

% You need to set the Manual mode first !

%TWO way accleration is disable

> ppa -v
% PPA mode is Auto
%PPA Protocol TCP 1, UDP 0
%PPA two way disable
%PPA time is 10
%PPA range is 192
%PPA LAN entries 0
```

Telnet Command: prn

This command allows you to view current status (interface and driver) of USB printer.

Syntax

prn status

prn debug

Example

```
> prn status
Interface: USB bus 2.0
Printer: NotReady

> prn debug
conn[0] :
none
conn[1] :
none
conn[2] :
none
conn[3] :
none
LPD_data_total=0

usbplp_ptr=0
UsbPrintReady=0, UsbIsPrinting=0
```

Telnet Command: qos setup

This command allows user to set general settings for QoS.

Syntax

qos setup [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-h	Type it to display the usage of this command.
-m <mode>	It means to define which traffic the QoS control settings will apply to and enable QoS control. 0: disable. 1: in, apply to incoming traffic only. 2: out, apply to outgoing traffic only. 3: both, apply to both incoming and outgoing traffic. Default is enable (for outgoing traffic).
-i <bandwidth>	It means to set inbound bandwidth in kbps (Ethernet WAN only). The available setting is from 1 to 100000.
-o <bandwidth>	It means to set outbound bandwidth in kbps (Ethernet WAN only). The available setting is from 1 to 100000.
-r <index:ratio>	It means to set ratio for class index, in %.

<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>	Minimum available non-VoIP Inbound Bandwidth when VoIP is detected (Kbps). Default value: half of WAN inbound bandwidth.
<code>-O <bandwidth></code>	Minimum available non-VoIP Outbound Bandwidth when VoIP is detected (Kbps). Default value: half of WAN outbound bandwidth.
<code>-v 0</code>	It means Auto bandwidth adjustment. Adjust to minimum In/Out bandwidth setting (or half QoS bandwidth).
<code>-v 1</code>	When VoIP detected, QoS In/Out bandwidth 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 -m 3 -i 9500 -o 8500 -r 3:20 -u 1 -p 50 -t 1

WAN1 QoS mode is both
Wan 1 is XDSL model ,don,t need to set up
Wan 1 is XDSL model ,don,t need to set up
WAN1 class 3 ratio set to 20
WAN1 udp bandwidth control set to enable
WAN1 udp bandwidth limit ratio set to 50
WAN1 Outbound TCP ACK Prioritizel set to enable
QoS WAN1 set complete; restart QoS
>
```

Telnet Command: qos class

This command allows user to set QoS class.

Syntax

```
qos class -c [no] -[a|e|d] [no][-<command> <parameter> | ... ]
```

Syntax Description

Parameter	Description
<code>[<command> <parameter> ...]</code>	The available commands with parameters are listed below. <code>[...]</code> means that you can type in several commands in one line.
<code>-h</code>	Type it to display the usage of this command.
<code>-c <no></code>	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, " <i>-l 172.16.3.9</i> ". <i>addr1:addr2</i> - It means Range address. Please specify the IP addresses, for example, " <i>-l 172.16.3.9: 172.16.3.50</i> ". <i>addr1:subnet</i> - It means the subnet address with start IP address. Please type the subnet and the IP address, for example, " <i>-l 172.16.3.9:255.255.0.0</i> ". <i>any</i> - It means Any address. Simple type " <i>-l</i> " 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, " <i>-l 172.16.3.9</i> ". <i>addr1:addr2</i> - It means Range address. Please specify the IP addresses, for example, " <i>-l 172.16.3.9: 172.16.3.50</i> ". <i>addr1:subnet</i> - It means the subnet address with start IP address. Please type the subnet and the IP address, for example, " <i>-l 172.16.3.9:255.255.0.0</i> ". <i>any</i> - It means Any address. Simple type " <i>-l</i> " to specify any address for this command.
-p <DSCP id>	Specify the ID.
-s <Service type>	Specify the service type by typing the number. The available types are listed as below: 1:ANY 2:DNS 3:FTP 4:GRE 5:H.323 6:HTTP 7:HTTPS 8:IKE 9:IPSEC-AH 10:IPSEC-ESP 11:IRC 12:L2TP 13:NEWS 14:NFS 15:NNTP 16:PING 17:POP3 18:PPTP 19:REAL-AUDIO 20:RTSP 21:SFTP 22:SIP 23:SMTP 24:SNMP 25:SNMP-TRAPS 26:SQL-NET 27:SSH 28:SYSLOG 29:TELNET 30:TFTP
-S <d/s>	Show the content for specified DSCP ID/Service type.
-V <1/2/3>	Show the rule in the specified class.
[...]	It means that you can type in several commands in one line.

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 192.168.2.10   100 192.168.2.1
[X]LAN3 192.168.3.1  255.255.255.0 V 192.168.3.10   100 192.168.3.1
[X]LAN4 192.168.4.1  255.255.255.0 V 192.168.4.10   100 192.168.4.1
[X]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
  2   Disable 192.168.1.56

%      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
```

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
Index  Status  Comment          Local IP Address
*****
  1.   Enable TEST          192.168.1.110
Total 1 items listed.
```


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: 30000
% Maximum Session Usage: 0
% Current Session Usage: 0
% Current Session Used(include waiting for free): 0
% WAN1 Current Session Usage: 0
% WAN3 Current Session Usage: 0
```

Telnet Command: show status

This command displays current status of LAN and WAN connections.

Example

```
> show status
System Uptime:25:40:53
LAN Status
Primary DNS:8.8.8.8      Secondary DNS:8.8.4.4
IP Address:192.168.1.1   Tx Rate:21417   Rx Rate:15413

WAN 1 Status: Disconnected
Enable:Yes      Line:Fiber      Name:
Mode:PPPoE      Up Time:0:00:00   IP:---      GW IP:---
TX Packets:0      TX Rate(bps):0   RX Packets:0      RX Rate(bps):0

WAN 2 Status: Disconnected
Enable:Yes      Line:Ethernet     Name:
Mode:DHCP Client Up Time:0:00:00   IP:---      GW IP:---
TX Packets:0      TX Rate(bps):0   RX Packets:0      RX Rate(bps):0
```


Telnet Command: smb setting

This command is used to configure file sharing settings for SMB server.

Syntax

smb setting *[enable/disable]*

smb setting *show status*

smb setting *set workgroup [Workgroup name]*

smb setting *set host [host name]*

smb setting *set access [LAN or LANWAN]*

Syntax Description

Parameter	Description
<i>enable/disable</i>	Enable or disable the SMB service.
<i>show status</i>	Display current status of SMB service.
<i>Set workgroup [Workgroup name]</i>	Set a name of workgroup for SMB service.
<i>set host [host name]</i>	Set a name of the host for SMB service.
<i>set access [LAN or LANWAN]</i>	Allow to access into SMB server by LAN or borth LAN and WAN.

Example

```
> smb setting enable
SMB service is enabled.

> smb setting set access LAN
Allow SMB access from LAN only.
>
```

Telnet Command: `srv dhcp dhcp2`

This command is used to enable DHCP2 server.

Syntax

`srv dhcp dhcp2 [-<command> <parameter> | ...]`

Syntax Description

Parameter	Description
<code>[<command> <parameter> ...]</code>	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
<code>-l<enable></code>	It means to enable the LAN port to public DHCP. 0: Disable 1: Enable
<code>-m<enable></code>	It means to enable MAC address to public DHCP. 0: Disable 1: Enable
<code>-e<id></code>	It means to turn on the flag of LAN port 1/2/3/4.
<code>-d<id></code>	It means to turn off the flag of LAN port 1/2/3/4.
<code>-v</code>	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
  Port 3 flag: OFF
  Port 4 flag: OFF
```

Telnet Command: `srv dhcp public`

This command allows users to configure DHCP server for second subnet.

Syntax

`srv dhcp public start [IP address]`

`srv dhcp public cnt [IP counts]`

`srv dhcp public status`

`srv dhcp public add [MAC Addr XX-XX-XX-XX-XX-XX]`

`srv dhcp public del [MAC Addr XX-XX-XX-XX-XX-XX/all/ALL]`

Syntax Description

Parameter	Description
<code>start</code>	It means the starting point of the IP address pool for the DHCP server.
<code>IP address</code>	It means to specify an IP address as the starting point in the IP address pool.

<i>cnt</i>	It means the IP count number.
<i>IP counts</i>	It means to specify the number of IP addresses in the pool. The maximum is 10.
<i>status</i>	It means the execution result of this command.
<i>add</i>	It means creating a list of hosts to be assigned.
<i>del</i>	It means removing the selected MAC address.
<i>MAC Addr</i>	It means to specify MAC Address of the host.
<i>all/ALL</i>	It means all of the MAC addresses.

Example

```
> 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 [?]`

`srv dhcp dns1 [LAN1/LAN2/LAN3/LAN4][DNS IP address]`

Syntax Description

Parameter	Description
<i>?</i>	It means to display current IP address of DNS 1 for the DHCP server.
<i>LAN1/LAN2/LAN3/LAN4</i>	It means to specify the LAN interface.
<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 168.95.1.1
% srv dhcp dns1 lan1 <DNS IP address>
% Now: 168.95.1.1
```

Telnet Command: `srv dhcp dns2`

This command allows users to set Secondary IP Address for DNS Server in LAN.

Syntax

```
srv dhcp dns2 [?]
```

```
srv dhcp dns2 [LAN1/LAN2/LAN3/LAN4][DNS IP address]
```

Syntax Description

Parameter	Description
<i>?</i>	It means to display current IP address of DNS 2 for the DHCP server.
<i>LAN1/LAN2/LAN3/LAN4</i>	It means to specify the LAN interface.
<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 lan1 168.95.1.1
% srv dhcp dns2 lan1 <DNS IP address>
% Now: 168.95.1.1
```

Telnet Command: `srv dhcp frcdnsmanl`

This command can force the router to invoke DNS Server IP address.

Syntax

```
srv dhcp frcdnsmanl [on]
```

```
srv dhcp frcdnsmanl [off]
```

Syntax Description

Parameter	Description
<i>?</i>	It means to display the current status.
<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.

Syntax

`srv dhcp gateway [?]`

`srv dhcp gateway [Gateway IP]`

Syntax Description

Parameter	Description
<code>?</code>	It means to display current gateway that you can use.
<code>Gateway IP</code>	It means to specify a gateway address used for DHCP server.

Example

```
> srv dhcp gateway 192.168.2.1
This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

Telnet Command: `srv dhcp ipcnt`

This command allows users to specify IP counts for DHCP server.

Syntax

`srv dhcp ipcnt [?]`

`srv dhcp ipcnt [IP counts]`

Syntax Description

Parameter	Description
<code>?</code>	It means to display current used IP count number.
<code>IP counts</code>	It means the number that you have to specify for the DHCP server.

Example

```
> srv dhcp ipcnt ?
% srv dhcp ipcnt <IP counts>
% Now: 150
```

Telnet Command: `srv dhcp off`

This function allows users to turn off DHCP server. It needs rebooting router, please type "sys reboot" command to reboot router.

Telnet Command: `srv dhcp on`

This function allows users to turn on DHCP server. It needs rebooting router, please type "sys reboot" command to reboot router.

Telnet Command: `srv dhcp relay`

This command allows users to set DHCP relay setting.

Syntax

`srv dhcp relay servip [server ip]`

`srv dhcp relay subnet [index]`

Syntax Description

Parameter	Description
<i>server ip</i>	It means the IP address that you want to used as DHCP server.
<i>Index</i>	It means subnet 1 or 2. Please type 1 or 2. The router will invoke this function according to the subnet 1 or 2 specified here.

Example

```
> srv dhcp relay servip 192.168.1.46
> srv dhcp relay subnet 2
> srv dhcp relay servip ?
% srv dhcp relay servip <server ip>
% Now: 192.168.1.46
```

Telnet Command: srv dhcp startip

Syntax

```
srv dhcp startip [?]
```

```
srv dhcp startip [IP address]
```

Syntax Description

Parameter	Description
<i>?</i>	It means to display current used start IP address.
<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.

Example

```
> srv dhcp status
LAN1      : DHCP Server On   IP Pool: 192.168.1.10 ~ 192.168.1.209
           Default Gateway: 192.168.1.1
-----
Index  IP Address      MAC Address      Leased Time      HOST ID
-----
LAN1
```

Telnet Command: `srv dhcp leasetime`

This command can set the lease time for the DHCP server.

Syntax

`srv dhcp leasetime [?]`

`srv dhcp leasetime [Lease Time (sec)]`

Syntax Description

Parameter	Description
<code>?</code>	It means to display current leasetime used for the DHCP server.
<code>Lease Time (sec)</code>	It means the lease time that DHCP server can use. The unit is second.

Example

```
> srv dhcp leasetime ?
% srv dhcp leasetime <Lease Time (sec.)>
% Now: 86400
>
```

Telnet Command: `srv dhcp nodetype`

This command can set the node type for the DHCP server.

Syntax

`srv dhcp nodetype <count>`

Syntax Description

Parameter	Description
<code>count</code>	It means to specify a type for node. 1. B-node 2. P-node 4. M-node 8. H-node

Example

```
> srv dhcp nodetype 1
> srv dhcp nodetype ?
%% srv dhcp nodetype <count>
%% 1. B-node 2. P-node 4. M-node 8. H-node
% Now: 1
```

Telnet Command: `srv dhcp primWINS`

This command can set the primary IP address for the DHCP server.

Syntax

```
srv dhcp primWINS [WINS IP address]
```

```
srv dhcp primWINS clear
```

Syntax Description

Parameter	Description
<i>WINS IP address</i>	It means the IP address of primary WINS server.
<i>clear</i>	It means to remove the IP address settings of primary WINS server.

Example

```
> srv dhcp primWINS 192.168.1.88
> srv dhcp primWINS ?
%% srv dhcp primWINS <WINS IP address>
%% srv dhcp primWINS clear
% Now: 192.168.1.88
```

Telnet Command: `srv dhcp secWINS`

This command can set the secondary IP address for the DHCP server.

Syntax

```
srv dhcp secWINS [WINS IP address]
```

```
srv dhcp secWINS clear
```

Syntax Description

Parameter	Description
<i>WINS IP address</i>	It means the IP address of secondary WINS server.
<i>clear</i>	It means to remove the IP address settings of second WINS server.

Example

```
> srv dhcp secWINS 192.168.1.180
> srv dhcp secWINS ?
%% srv dhcp secWINS <WINS IP address>
%% srv dhcp secWINS clear
% Now: 192.168.1.180
```

Telnet Command: `srv dhcp expRecycleIP`

This command can set the time to check if the IP address can be assigned again by DHCP server or not.

Syntax

```
srv dhcp expRecycleIP <sec time>
```

Syntax Description

Parameter	Description
<i>sec time</i>	It means to set the time (5-300 seconds) for checking if the IP can be assigned again or not.

Example

```
> srv dhcp expRecycleIP 250
% DHCP expRecycleIP = 250
```

Telnet Command: `srv dhcp tftp`

This command can set the TFTP server as the DHCP server.

Syntax

```
srv dhcp tftp <TFTP server name>
```

Syntax Description

Parameter	Description
<i>TFTP server name</i>	It means to type the name of TFTP server.

Example

```
> srv dhcp tftp TF123
> srv dhcp tftp ?
%% srv dhcp tftp <TFTP server name>
% Now: TF123
```

Telnet Command: `srv dhcp tftpdel`

This command can remove the name defined for the TFTP server.

Syntax

```
srv dhcp tftpdel
```

Example

```
> srv dhcp tftp TF123
> srv dhcp tftp ?
%% srv dhcp tftp <TFTP server name>
% Now: TF123
> srv dhcp tftpdel
% The TFTP Server Name had been deleted !!!
```

Telnet Command: `srv dhcp option`

This command can set the custom option for the DHCP server.

Syntax

```
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
<code>-h</code>	It means to display usage of this command.
<code>-l</code>	It means to display all the user defined DHCP options.
<code>-d</code>	It means to delete the option number by specifying its index number.
<code>-e [1 or 0]</code>	It means to enable/disable custom option feature. 1:enable 0:disable
<code>-i [lan number]</code>	It means to specify the LAN interface. 1: lan1, a: all lan, r: routed subnet
<code>s [Next Server IP Address]</code>	It means to specify the IP address for the server.
<code>option number</code>	It includes <code>-a</code> , <code>-c</code> , <code>-v</code> and <code>-x</code> . <code>-a</code> : It means to set the option value by specifying the IP address. <code>-c</code> : It means to set option number. Available number ranges from 0 to 255. <code>-v</code> : It means to set option number by typing string. <code>-x</code> : It means to set option number with the format of Hexadecimal characters.
<code>-u</code>	It means to update the option value of the sepecified index.
<code>idx number</code>	It means the index number of the option value.

Example

```
> srv dhcp option -e 1 -i 1/2 -s 8.8.8.8
> srv dhcp option -e 1 -i 1/2 -c 18 -x 2f70617468
> srv dhcp option -e 1 -i 2/r -c 44 -a 192.168.1.10,192.168.1.20
> srv dhcp option -u 2 -i 1 -c 60 -v class_id
> srv dhcp option -l
% state  idx interface      opt type  data
% enable 1  LAN1/2          0  SIAddr  8.8.8.8
% enable 2  LAN1            60 ASCII   class_id
% enable 3  LAN2/r          44 Address 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.

Syntax

`srv nat dmz n m [-<command> <parameter> | ...]`

Syntax Description

Parameter	Description
<i>n</i>	It means to map selected WAN IP to certain host. 1: wan1
<i>m [index]</i>	It means the index number (1 ~ 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 in this field. If WAN IP alias has been configured, then the number of DMZ host can be added more.
<i>[<command> <parameter> ...]</i>	The available commands with parameters are listed below. <i>[...]</i> means that you can type in several commands in one line.
<i>-e</i>	It means to enable/disable such feature. 1:enable 0:disable
<i>-i</i>	It means to specify the private IP address of the DMZ host.
<i>-r</i>	It means to remove DMZ host setting.
<i>-v</i>	It means to display current status.

Example

```
> srv nat dmz 1 1 -i 192.168.1.96
> srv nat dmz -v
%      WAN1 DMZ mapping status:
Index  Status  WAN1 aux IP    Private IP
-----
  1    Disable  0.0.0.0 192.168.1.96
  2    Disable  192.168.1.56
```

Telnet Command: `srv nat ipsecpass`

This command allows users to enable or disable IPSec ESP tunnel passthrough and IKE source port (500) preservation.

Syntax

`srv nat ipsecpass [options]`

Syntax Description

Parameter	Description
<i>[options]</i>	The available commands with parameters are listed below.
<i>on</i>	It means to enable IPSec ESP tunnel passthrough and IKE source port (500) preservation.
<i>off</i>	It means to disable IPSec ESP tunnel passthrough and IKE source

	port (500) preservation.
<i>status</i>	It means to display current status for checking.

Example

```
> srv nat ipsecpass status
%% Status: IPsec ESP pass-thru and IKE src_port:500 preservation is OFF.
```

Telnet Command: `srv nat openport`

This command allows users to set open port settings for NAT server.

Syntax

`srv nat openport n m [-<command> <parameter> | ...]`

Syntax Description

Parameter	Description
<i>n</i>	It means the index number for the profiles. The range is from 1 to 40.
<i>m</i>	It means to specify the sub-item number for this profile. The range is from 1 to 10.
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-a <enable>	It means to enable or disable the open port rule profile. 0: disable 1:enable
-c <comment>	It means to type the description (less than 23 characters) for the defined network service.
-i <local ip>	It means to set the IP address for local computer. Local ip: Type an IP address in this field.
-w <widx> <ipidx>	It means to specify the public IP. <i>widx</i> - means the WAN interface. In which, 1: WAN1 Default, 2: WAN1 Alias 1,.... 255: all WANs. <i>ipidx</i> - means the index number (1 ~ 32) for all Alias IPs.
-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 192.168.1.56 -w 1 1 -p TCP -s 23 -e 83
> Set WAN Port ok!!
```

```

> srv nat openport 1 1 -v
%% Status: Enable
%% Comment: games
%% WAN Interface: WAN1
%% Private IP address: 192.168.1.56
Index  Protocol      Start Port    End Port
*****
 1.    TCP          23           83
 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
>

```

Telnet Command: `srv nat portmap`

This command allows users to set port redirection table for NAT server.

Syntax

`srv nat portmap add [idx][serv name][proto][pub port][src ip idx][pri ip][pri port][wan1~wan3][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`

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 or All (tcp/udp/all) as the protocol.
<i>pub port</i>	It means to specify which port (0-65535) can be redirected to the specified Private IP and Port of the internal host.
<i>src ip idx</i>	It means the index number of source IP object.
<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 (0-65535) of the service offered by the internal host.
<i>wan1~wan3</i>	It means to specify WAN interface for the port redirection.
<i>del [idx]</i>	It means to remove the selected port redirection setting.
<i>disable [idx]</i>	It means to inactivate the selected port redirection setting.
<i>enable [idx]</i>	It means to activate the selected port redirection setting.
<i>flush</i>	It means to clear all the port mapping settings.

table

It means to display Port Redirection Configuration Table.

Example

```
> srv nat portmap add 1 name tcp 100 0 192.168.1.10 200 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	192.168.1.10	200	-1
2		0	0		0	-2
3		0	0		0	-2
4		0	0		0	-2
5		0	0		0	-2
6		0	0		0	-2
7		0	0		0	-2
8		0	0		0	-2
9		0	0		0	-2
10		0	0		0	-2
11		0	0		0	-2
12		0	0		0	-2
13		0	0		0	-2
14		0	0		0	-2
15		0	0		0	-2
16		0	0		0	-2
17		0	0		0	-2
18		0	0		0	-2
19		0	0		0	-2
20		0	0		0	-2

Protocol: 0 = Disable, 6 = TCP, 17 = UDP

Telnet Command: `srv nat status`

This command allows users to view NAT Port Redirection Running Table.

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 trigger`

This command allows users to set port setting for triggering or return to factory default settings of port.

Syntax

`srv nat trigger setdefault`

`srv nat trigger view`

`srv nat trigger n [-<command> <parameter> | ...]`

Syntax Description

Parameter	Description
<code>srv nat trigger setdefault</code>	It means to set to factory default.
<code>srv nat trigger view</code>	It will show all port trigger settings.
<code>n</code>	It means the rule number for the profiles.
<code>[<command> <parameter> ...]</code>	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
<code>-c</code>	Type text as a comment.
<code>-e</code>	Enable/disable this emety [1/0].
<code>-P</code>	Specify the protocol [1-TCP, 2-UDP, 3-All] for triggering.
<code>-t</code>	Specify the number of trigger port.
<code>-P</code>	Specify the protocol [1-TCP, 2-UDP, 3-All] for incoming data.
<code>-i</code>	Specify the number of incoming port.
<code>-d</code>	Delete the specified trigger profile.
<code>-v [n]</code>	Show port trigger setting by specifying the rule number.

Example

```
> srv nat trigger 1 -c test -e 1 -s 2 -p 1 -t 85 -P 2 -i 190
> srv nat trigger view
%%      Port Trigger Rule status:
Index  Status  Comment  TProto  TPort   IProto  IPort
-----
  1    Enable  test     TCP     85      UDP     190
  2    Disable
  3    Disable
  4    Disable
  5    Disable
```

```

6   Disable
7   Disable
8   Disable
9   Disable
10  Disable
11  Disable
12  Disable
13  Disable
14  Disable
15  Disable
16  Disable
17  Disable
18  Disable
19  Disable
20  Disable

```

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    0.0.0.0:100        192.168.1.10:200    Y

O01    TCP    0.0.0.0:23~83     192.168.1.56:23~83  Y
O01    ---    0.0.0.0:0~0       192.168.1.56:0~0   Y
O01    ---    0.0.0.0:0~0       192.168.1.56:0~0   Y
O01    ---    0.0.0.0:0~0       192.168.1.56:0~0   Y
O01    ---    0.0.0.0:0~0       192.168.1.56:0~0   Y
O01    ---    0.0.0.0:0~0       192.168.1.56:0~0   Y
O01    ---    0.0.0.0:0~0       192.168.1.56:0~0   Y
O01    ---    0.0.0.0:0~0       192.168.1.56:0~0   Y
O01    ---    0.0.0.0:0~0       192.168.1.56:0~0   Y
O01    ---    0.0.0.0:0~0       192.168.1.56:0~0   Y
O01    ---    0.0.0.0:0~0       192.168.1.56:0~0   Y

D01    All    0.0.0.0            192.168.1.96        Y

R:Port Redirection, O:Open Ports, D:DMZ

```

Telnet Command: `switch -i`

This command is used to obtain the TX (transmitted) or RX (received) data for each connected switch.

Syntax

```
switch -i [switch idx_no] [option]
```

Syntax Description

Parameter	Description
<code>switch idx_no</code>	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 display current status for 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.

Syntax

switch clear *[idx]*

Syntax Description

Parameter	Description
<i>idx</i>	It means the index number of each item shown on the table. The range is from 1 to 8.
<i>-f</i>	It means to clear all of the data.

Example

```
> switch clear 1
Switch Data clear successful

> switch clear -f
Switch Data clear successful
```

Telnet Command: switch query / syslog

This command is used to enable or disable the switch query / syslog.

Example

```
> switch query on
Extern Device status query is Enable
> switch query off
Extern Device status query is Disable
> switch syslog on
External Device syslog is Enable
```

Telnet Command: sys admin

This command is used for RD engineer to access into test mode of Vigor router.

Telnet Command: sys adminuser

This command is used to create user account and specify LDAP server. The server will authenticate the local user who wants to access into the web user interface of Vigor router.

Syntax

`sys adminuser [option]`

`sys adminuser edit [index] username password`

Syntax Description

Parameter	Description
<i>option</i>	Available options includes: Local [0-1] 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 the function of default or wireless LAN button.

Syntax

`sys board button [def/wlan [on/off]]`

Syntax Description

Parameter	Description
<i>def</i>	It is used to disable/enable Bonjour service (0: disable, 1: enable).
<i>wlan</i>	It is used to disable/enable http (web) service (0: disable, 1: enable).
<i>on/off</i>	On - enable the button function. Off - disable the button function.

Example

```
> sys board button def on
> default button is on now.
```

Telnet Command: sys cfg

This command reset the router with factory default settings. When a user types this command, all the configuration will be reset to default setting.

Syntax

sys cfg default

sys cfg status

Syntax Description

Parameter	Description
<i>default</i>	It means to reset current settings with default values.
<i>status</i>	It means to display current profile version and status.

Example

```
> sys cfg status
Profile version: 3.0.0    Status: 1 (0x4845af2c)
> sys cfg default
>
```

Telnet Command: sys cmdlog

This command displays the history of the commands that you have typed.

Example

```
> sys cmdlog
[1] ?
[2] sys ?
[3] sys adminuser ?
[4] sys board ?
[5] sys board button ?
[6] sys board button def on
[7] sys cfg ?
[8] sys cfg status
[9] sys /
[10] sys cmdlog ?
[11] sys cmdlog
```

Telnet Command: sys ftpd

This command displays current status of FTP server.

Syntax

sys ftpd *on*

sys ftpd *off*

Syntax Description

Parameter	Description
-----------	-------------

<i>on</i>	It means to turn on the FTP server of the system.
<i>off</i>	It means to turn off the FTP server of the system.

Example

```
> sys ftpd on
% sys ftpd turn on !!!
```

Telnet Command: sys domainname

This command can set and remove the domain name of the system when DHCP mode is selected for WAN.

Syntax

`sys domainname [wan1] [Domain Name Suffix]`

`sys domainname [wan1] clear`

Syntax Description

Parameter	Description
<i>wan1</i>	It means to specify WAN interface for assigning a name for it.
<i>Domain Name Suffix</i>	It means the name for the domain of the system. The maximum number of characters that you can set is 39.
<i>clear</i>	It means to remove the domain name of the system.

Example

```
> sys domainname wan1 clever
> sys domainname wan2 intellegent
> sys domainname ?
% sys domainname <wan1 > <Domain Name Suffix (max. 39 characters)>
% sys domainname <wan1 > clear
% Now: wan1 == clever
>
```

Telnet Command: sys iface

This command displays the current interface connection status (UP or Down) with IP address, MAC address and Netmask for the router.

Example

```
> sys iface
Interface 0 Ethernet:
Status: UP
IP Address: 192.168.1.1      Netmask: 0xFFFFFFFF00 (Private)
IP Address: 0.0.0.0        Netmask: 0xFFFFFFFF
MAC: 00-50-7F-00-00-00
Interface 4 Ethernet:
Status: DOWN
IP Address: 0.0.0.0        Netmask: 0x00000000
MAC: 00-50-7F-00-00-02
Interface 5 Ethernet:
Status: DOWN
IP Address: 0.0.0.0        Netmask: 0x00000000
```



```

MAC: 00-50-7F-00-00-03
Interface 6 Ethernet:
Status: DOWN
IP Address: 0.0.0.0           Netmask: 0x00000000
MAC: 00-50-7F-00-00-04
Interface 7 Ethernet:
Status: DOWN
IP Address: 0.0.0.0           Netmask: 0x00000000
MAC: 00-50-7F-00-00-05
Interface 8 Ethernet:
Status: DOWN
IP Address: 0.0.0.0           Netmask: 0x00000000
MAC: 00-50-7F-00-00-06

--- 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 39.

Example

```

> sys name wan1 drayrouter
> sys name ?
% sys name <wan1> <ASCII string (max. 39 characters)>
% sys name <wan1 > clear
% Now: wan1 == drayrouter

```

Note: Such name can be used to recognize router's identification in SysLog dialog.

Telnet Command: `sys passwd`

This command allows users to set password for the administrator.

`sys passwd [old password] [new password: ASCII string]`

Syntax Description

Parameter	Description
<i>old password</i>	It means the old password for administrator.
<i>new password: ASCII string</i>	It means the password for administrator. The maximum character that you can set is 83.

Example

```
> sys passwd admin admin123
> Password change successful !!!
> sys passwd admin123 admin
```

Telnet Command: `sys reboot`

This command allows users to restart the router immediately.

Example

```
> sys reboot
>
```

Telnet Command: `sys autoreboot`

This command allows users to restart the router automatically within a certain time.

Syntax

`sys autoreboot [on/off/hour(s)]`

Syntax Description

Parameter	Description
<i>on/off</i>	On - It means to enable the function of auto-reboot. Off - It means to disable the function of auto-reboot.
<i>hours</i>	It means to set the time schedule for router reboot. For example, if you type "2" in this field, the router will reboot with an interval of two hours.

Example

```
> sys autoreboot on
autoreboot is ON
> sys autoreboot 2
autoreboot is ON
autoreboot time is 2 hour(s)
```

Telnet Command: `sys commit`

This command allows users to save current settings to FLASH. Usually, current settings will be saved in SRAM. Yet, this command will save the file to FLASH.

Example

```
> sys commit
>
```

Telnet Command: `sys tftpd`

This command can turn on TFTP server for upgrading the firmware.

Example

```
> sys tftpd
% TFTP server enabled !!!
```

Telnet Command: `sys version`

This command can display current version for the system.

Example

```
> sys version
Router Model: Vigor2133ac   Version: 3.8.5_RC4a English
Profile version: 3.0.0     Status: 1 (0x4845af2c)
Router IP: 192.168.1.1     Netmask: 255.255.255.0
Firmware Build Date/Time: Mar 30 2017 17:42:06
Router Name: DrayTek
Revision: 63880 V385
```

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 ( 224B), used#: 2808, cached#: 27
Buf KMC4088 (4088B), used#: 1155, cached#: 5
Buf KMC2552 (2552B), used#: 1671, cached#: 420
Buf KMC1016 (1016B), used#: 13, cached#: 3
Buf KMC504 ( 504B), used#: 148, cached#: 4
Buf KMC248 ( 248B), used#: 374, cached#: 26
Buf KMC120 ( 120B), used#: 1200, cached#: 80
Buf KMC56 ( 56B), used#: 27, cached#: 37
Buf KMC24 ( 24B), used#: 1061, cached#: 91
Dynamic memory: 26214400B; 10034208B used; 1156064B/0B in level 1/2 cache.

FLOWTRACK Memory Status
# of free = 32000
# of maximum = 0
# of flowstate = 32000
# of lost by siganture = 0
# of lost by list = 0
```

Telnet Command: `sys pollbuf`

This command can turn on or turn off polling buffer for the router.

Syntax

`sys pollbuf [on]`

`sys pollbuf [off]`

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on pulling buffer.
<i>off</i>	It means to turn off pulling buffer.

Example

```
> sys pollbuf on
% Buffer polling is on!

> sys pollbuf off
% Buffer polling is off!
```

Telnet Command: `sys britask`

This command can improve triple play quality.

Syntax

`sys britask [on]`

`sys britask [off]`

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on the bridge task for improving the triple play quality.
<i>off</i>	It means to turn off the bridge task.

Example

```
> sys britask on
% bridge task is ON, now
```

Telnet Command: sys tr069

This command can set CPE settings for applying in VigorACS.

Syntax

```
sys tr069 get [parm] [option]
sys tr069 set [parm] [value]
sys tr069 getnoti [parm]
sys tr069 setnoti [parm] [value]
sys tr069 log
sys tr069 debug [on/off]
sys tr069 save
sys tr069 inform [event code]
sys tr069 port [port num]
sys tr069 cert_auth [on/off]
```

Syntax Description

Parameter	Description
<i>get [parm] [option]</i>	It means to get parameters for tr-069. option=<nextlevel>: only gets nextlevel for GetParameterNames.
<i>set [parm] [value]</i>	It means to set parameters for tr-069.
<i>getnoti [parm]</i>	It means to get parameter notification value.
<i>setnoti [parm] [value]</i>	It means to set parameter notification value.
<i>log</i>	It means to display the TR-069 log.
<i>debug [on/off]</i>	on: turn on the function of sending debug message to syslog. off: turn off the function of sending debug message to syslog.
<i>save</i>	It means to save the parameters to the flash memory of the router.
<i>Inform [event code]</i>	It means to inform parameters for tr069 with different event codes. [event code] includes: 0-"0 BOOTSTRAP", 1-"1 BOOT", 2-"2 PERIODIC", 3-"3 SCHEDULED", 4-"4 VALUE CHANGE", 5-"5 KICKED", 6-"6 CONNECTION REQUEST", 7-"7 TRANSFER COMPLETE", 8-"8 DIAGNOSTICS COMPLETE", 9-"M Reboot"
<i>port [port num]</i>	It means to change tr069 listen port number.
<i>cert_auth [on/off]</i>	on: turn on certificate-based authentication. off: turn off certificate-based authentication.

Example

```
> sys tr069 get Int. nextlevel
Total number of parameter is 24
```

```

Total content length of parameter is 915
InternetGatewayDevice.LANDeviceNumberOfEntries
InternetGatewayDevice.WANDeviceNumberOfEntries
InternetGatewayDevice.DeviceInfo.
InternetGatewayDevice.ManagementServer.
InternetGatewayDevice.Time.
InternetGatewayDevice.Layer3Forwarding.
InternetGatewayDevice.LANDevice.
InternetGatewayDevice.WANDevice.
InternetGatewayDevice.Services.
InternetGatewayDevice.X_00507F_InternetAcc.
InternetGatewayDevice.X_00507F_LAN.
InternetGatewayDevice.X_00507F_NAT.
InternetGatewayDevice.X_00507F_Firewall.
InternetGatewayDevice.X_00507F_Bandwidth.
InternetGatewayDevice.X_00507F_Applications.
InternetGatewayDevice.X_00507F_VPN.
InternetGatewayDevice.X_00507F_VoIP.
InternetGatewayDevice.X_00507F_WirelessLAN.
InternetGatewayDevice.X_00507F_System.
InternetGatewayDevice.X_00507F_Status.

InternetGatewayDevice.X_00507F_Diagnostics.
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---

```

Telnet Command: sys alg

This command can turn on/off ALG (Application Layer Gateway) for traversal.

Syntax

```
sys alg [1]
```

```
sys alg [0]
```

Syntax Description

Parameter	Description
1	It means to turn on ALG.
0	It means to turn off ALG.

Example

```

> sys sip_alg ?
Usage: sys alg <command> <parameter>
-e: enable ALG (0:disable, 1:enable)

Current ALG status
-ALG Master Switch: Disabled

```

Telnet Command: sys sip_alg

This command can turn on/off ALG (Application Layer Gateway) for SIP.

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.
-p 0/1	Set the listening port (1-65535) for SIP ALG.
-u 0/1	Enable (1) or disable (0) the listening along UDP path.
-t 0/1	Enable (1) or disable (0) the listening along TCP path.

Example

```
> sys sip_alg -p 65535
Current listening port: 65535
```

Telnet Command: sys rtsp_alg

This command can turn on/off SIP ALG (Application Layer Gateway) for RTSP

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	Enable (1) or disable (0) the function of RTSP ALG.
-p 0/1	Set the listening port (1-65535) for RTSP ALG.
-u 0/1	Enable (1) or disable (0) the listening along UDP path.
-t 0/1	Enable (1) or disable (0) the listening along TCP path.
-v	Display RTP and RTCP portmap information of RTSP ALG.

Example

```
> sys rtsp_alg -e 1
Auto enable ALG Master Switch

Enable RTSP ALG

> sys rtsp_alg -p 85
Current listening RTSP Port: 85
> 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: 85
```

```
-Max RTSP session num: 256
-Remain RTSP session num: 256
```

Telnet Command: sys license

This command can process the system license.

Syntax

```
sys license licmsg
sys license licauth
sys license regser
sys license licera
sys license licifno
sys license lic_wiz [set/reg/qry]
sys license trigger [-e/-d/-s]
sys license dev_chg
sys license dev_key
```

Syntax Description

Parameter	Description
<i>licmsg</i>	It means to display license message.
<i>licauth</i>	It means the license authentication time setting.
<i>regser</i>	It means the license register server setting.
<i>licera</i>	It means to erase license setting.
<i>licifno</i>	It means license and signature download interface setting.
<i>lic_wiz</i> [<i>set/reg/qry</i>]	It means the license wizard setting. qry: query service support status set [idx] [trial] [service type] [sp_id] [start_date] [License Key] reg: register service in portal
<i>trigger</i> [<i>-e/-d/-s</i>]	It means to trigger the license automatically to update on boot time. -e - Enable the license trigger to update. -d - Disable the license trigger to update. -s - Display license status.
<i>dev_chg</i>	It means to change the device key.
<i>dev_key</i>	It means to show device key.

Example

```
> sys license licifno

License and Signature download interface setting:
licifno [AUTO/WAN#]

Ex: licifno wan1

Download interface is "auto-selected" now.
```



```

> sys license lic_trigger -e
Trigger the license to update, value=1

> sys license lic_trigger -d
Don't trigger the license to update, value=0

> sys license lic_trigger -s
License update state=0 (0:disable, 1:enable)

```

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. <i>[...]</i> means that you can type in several commands in one line.
<i>-l</i>	Display DNS IPv4 entry in the DNS cache table.
<i>-s</i>	Display DNS IPv6 entry in the DNS cache table.
<i>-v</i>	Display the TTL limit value in the DNS cache table.
<i>-t <0/n ></i>	Set the TTL limit value in the DNS cache table. 0- No limit N - Greater than or equal to 5.
<i>-c</i>	Clear the DNS cache table.

Example

```
> sys dnsCacheTbl -l
%DNS Cache Table List
> sys dnsCacheTbl -t 65
% Set TTL limit: 65 seconds.
% When TTL larger than 65s , delete the DNS entry in the router's DNS cache
tabl
e.
>
```

Telnet Command: sys syslog

This command is used to enable / disable syslog.

Syntax

sys syslog *-a <enable> [-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
<i>[<command><parameter>/...]</i>	The available commands with parameters are listed below. <i>[...]</i> means that you can type in several commands in one line.
<i>-a <1/0></i>	Enable (1) or disable (0) Syslog Access Setup.
<i>-s <1/0></i>	Enable (1) or disable (0) Syslog Save to Syslog Server.
<i>-i <IP address></i>	Define the IP address of the Syslog server.
<i>-d <port number></i>	Define the port number (1 ~ 65535) as the destination port.
<i>-u <1/0></i>	Enable (1) or disable (0) Syslog Save to USB Disk.

<code>-m <1/0></code>	Enable (1) or disable (0) Mail Syslog.
<code>-f <1/0></code>	Enable (1) or disable (0) Firewall Log.
<code>-v <1/0></code>	Enable (1) or disable (0) VPN Log.
<code>-e <1/0></code>	Enable (1) or disable (0) User Access Log.
<code>-c <1/0></code>	Enable (1) or disable (0) Call Log.
<code>-w <1/0></code>	Enable (1) or disable (0) WAN Log.
<code>-r <1/0></code>	Enable (1) or disable (0) Router/DSL Information.
<code>-t <1/0></code>	Enable (1) or disable (0) AlertLog Setup.
<code>-o <port number></code>	Define the port number (1 ~ 65535) for AlertLog.
<code>-p</code>	Update the IP address of the server.

Example

```
> sys syslog -a 1 -s 1 -i 192.168.1.25 -d 514
> sys syslog -p
> Updating server IP address..
```

Telnet Command: sys mailalert

This command is used to configure settings for mail alert function.

Syntax

sys mailalert [*<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.
<code>-e <0/1></code>	Enable (1) or disable (0) the mail alert function.
<code>-i <SMTP Server IP></code>	Set the SMTP sever IP address.
<code>-o <SMTP Server Port></code>	Set the port number (1~65535) for SMTP server.
<code>-a <Mail Address></code>	Set Alert Mail Reciver E-maiil Address.
<code>-r <Mail Address></code>	Set Mail Return E-mail Address.
<code>-s <0/1></code>	Enable/Disable Use SSL.
<code>-h <0/1></code>	Enable/Disable SMTP Authentication.
<code>-u <Username></code>	Set Username for SMTP Authentication.
<code>-p <Password></code>	Set Password for SMTP Authentication.
<code>-l <type> <0 /1 ></code>	"0 <0/1>" : Set Enable/Disable Mail Alert of the DoS Attack. "1 <0/1>" : Set Enable/Disable Mail Alert of the APPE. "2 <0/1>" : Set Enable/Disable Mail Alert of the VPN Log. "3 <0/1>" : Set Enable/Disable Mail Alert of the APPE Signature. "6 <0/1>" : Set Enable/Disable Mail Alert of the Reboot Debug Log.
<code>-f</code>	Reset Mail Alert Setting to factory default.
<code>-v</code>	Show Current Mail Alert Setting.
<code>-R <0/1></code>	Set Mail Alert Reboot Debug Log Mode. 0: Limited Mode, 1: Unlimited Mode.

Example

```
> sys mailalert -e 1
> sys mailalert -i 172.16.3.168
> sys mailalert -o 886
> sys mailalert -a john@draytek.com
> sys mailalert -v
----- Current setting for Mail Alert -----
Mail Alert: Enable
SMTP Server IP Address: 172.16.3.168
SMTP Server Port: 886
Alert Mail Reciver E-maiil Address: john@draytek.com
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 wan [option]`

`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>Option [0/1/2/3]</i>	Select WAN interface for applying the time server. 0 - Auto 1 - WAN1 2 - WAN2 3 - WAN3
<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 or hidden the information displayed on the dashboard.

Syntax

sys dashboard show

sys dashboard *-[<command> <value> [-<command> <value> | ...]*

Syntax Description

Parameter	Description
<i>[<command><parameter>/...]</i>	The available commands with parameters are listed below. <i>[...]</i> means that you can type in several commands in one line.
<i>command</i>	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
<i>value</i>	1 : Enable 0 : Disable

Example

```

> sys dashboard -1 1 -2 0
System Information enabled
IPv4 LAN Information disabled

```

Telnet Command: testmail

This command is used to display current settings for sending test mail.

Example

```

> testmail
Send out test mail
Mail Alert:[Disable]
SMTP_Server:[0.0.0.0]
Mail to:[]
Return-Path:[]

```

Telnet Command: upnp off

This command can close UPnP function.

Example

```
>upnp off
UPNP say bye-bye
```

Telnet Command: upnp on

This command can enable UPnP function.

Example

```
>upnp on
UPNP start.
```

Telnet Command: upnp nat

This command can display IGD NAT status.

Example

```
> upnp nat ?
***** IGD NAT Status *****

((0))
InternalClient >>192.168.1.10<<, RemoteHost >>0.0.0.0<<
InternalPort >>21<<, ExternalPort >>21<<
PortMapProtocol >>TCP<<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
Ftp Example [MICROSOFT]
((1))
InternalClient >>0.0.0.0<<, RemoteHost >>0.0.0.0<<
InternalPort >>0<<, ExternalPort >>0<<
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
0<<

--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
```

Telnet Command: upnp service

This command can display the information of the UPnP service. UPnP service must be enabled first.

Example

```
> upnp on
UPNP start.

> upnp service
>>>> SERVICE TABLE1 <<<<<
```

```

serviceType urn:schemas-microsoft-com:service:OSInfo:1
serviceId urn:microsoft-com:serviceId:OSInfo1
SCPDURL /upnp/OSInfo.xml
controlURL /OSInfo1
eventURL /OSInfoEvent1
UDN uuid:774e9bbe-7386-4128-b627-001daa843464

>>>> SERVICE TABLE2 <<<<<
serviceType urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1
serviceId urn:upnp-org:serviceId:WANCommonIFC1
SCPDURL /upnp/WComIFCX.xml
controlURL /upnp?control=WANCommonIFC1
eventURL /upnp?event=WANCommonIFC1
UDN uuid:2608d902-03e2-46a5-9968-4a54ca499148
.
.
.

```

Telnet Command: upnp subscribe

This command can show all UPnP services subscribed.

Example

```

> upnp on
UPNP start.
> upnp subscribe
>>>> (1) serviceType urn:schemas-microsoft-com:service:OSInfo:1

>>>> (2) serviceType
urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1

>>>> (3) serviceType urn:schemas-upnp-org:service:WANPOTSLinkConfig:1

>>>> (4) serviceType urn:schemas-upnp-org:service:WANPPPConnection:1

>>>> (5) serviceType urn:schemas-upnp-org:service:WANIPConnection:1

```

Telnet Command: upnp tmpvs

This command can display current status of temp Virtual Server of your router.

Example

```

Vigor> upnp tmpvs
***** Temp virtual server status *****

((0))
real_addr >>192.168.1.10<<, pseudo_addr >>172.16.3.229<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>TCP<<
time >>0<<

((1))
real_addr >>0.0.0.0<<, pseudo_addr >>0.0.0.0<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<

```



```
The protocol >>0<<
time >>0<<
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
```

Telnet Command: upnp wan

This command is used to specify WAN interface to apply UPnP.

Syntax

```
upnp wan [n]
```

Syntax Description

Parameter	Description
<i>n</i>	It means to specify WAN interface to apply UPnP. n=0, it means to auto-select WAN interface. n=1, WAN1

Example

```
> upnp wan 1
use wan1 now.
```

Telnet Command: usb devstat

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 devstat
USB Port1: No device
USB Port2: No device
```

Telnet Command: usb user

This command is used to set profiles for FTP/SMB users.

Syntax Description

```
usb user add [Index] [Username] [Password] [Permission] [Home path]
```

```
usb user rm [Index]
```

```
usb user enable [Index]
```

```
usb user disable [Index]
```

```
usb user list
```

Syntax Description

Parameter	Description
<i>add</i>	Add a new user profile.
<i>rm</i>	Delete an existed user profile.
<i>enable</i>	Enable a user profile.
<i>disable</i>	Disable a user profile.
<i>list</i>	Display all of the user profile.

<i>index</i>	It means the index number of the user profile. There are 16 profiles allowed to be configured. So the range of such option is 1 ~ 16.
<i>Username</i>	Type a text (maximum 11 characters) as the username for the user profile.
<i>Password</i>	Type a text (maximum 11 characters) as the password for the user profile.
<i>Permission</i>	Specify the action (RWDLCR) permitted. If one of the actions is not allowed, simple type "-" instead. R - Read File. W - Write File. D - Delete File. L - List directory. C - Create directory. R - Remove selected directory.
<i>Home path</i>	Set the path (maximum 159 characters) for the USB user profile.

Example

```
> usb user add 1 root 1234 R-DLCR /usr
```

Telnet Command: vigbrg set

This command is to configure specified WAN as bridge mode.

Syntax Description

```
vigbrg set -v [IP version] -w [WAN_idx] -l [LAN_idx] -e [0/1] -f [0/1]
```

Syntax Description

Parameter	Description
<i>-v [IP version]</i>	Indicate the IP version for the IP address. 4 - IPv4. 6 - IPv6.
<i>-w [WAN_idx]</i>	WAN_idx - Indicate the WAN interface. 1 - WAN1
<i>-l [LAN_idx]</i>	LAN_idx - Indicate the LAN interface. 1 - LAN1 2 - LAN2 3 - LAN3 4 - LAN4
<i>e [0/1]</i>	Enable (1) or disable (0) the Vigor Bridge for WAN or/and LAN.
<i>f [0/1]</i>	Enable (1) or disable (0) the firewall functions.

Example

```
> vigbrg set -v 4 -w 1 -l 1 -e 1
[WAN1] IPv4 bridge is enable. Set subnet[LAN1]
```

Telnet Command: vigbrg status

This command can show whether the Vigor Bridge Function is enabled or disabled.

Example

```
> vigbrg status
Show gConfig setting of bridge mode
[WAN1] IPv4 bridge is enable [LAN1].
```

Telnet Command: vigbrg cfgip

This command allows users to transfer a bridge modem into ADSL router by accessing into and adjusting specified IP address. Users can access into Web UI of the router to manage the router through the IP address configured here.

Syntax

`vigbrg cfgip [IP Address]`

Syntax Description

Parameter	Description
<i>IP Address</i>	It means to type an IP address for users to manage the router.

Example

```
> vigbrg cfgip 192.168.1.15
> vigbrg cfgip ?
% Vigor Bridge Config IP,
% Now: 192.168.1.15
```

Telnet Command: vigbrg wanstatus

This command can display the existed WAN connection status for the modem (change from ADSL router into bridge modem), including index number, MAC address, Stamp Time, PVC, VLAN port for Vigor Bridge Function..

Example

```
> vigbrg wanstatus
Vigor Bridge: Running
WAN mac table:
Index   MAC Address           Stamp Time           PVC   VLan Port
```

Telnet Command: vigbrg wlanstatus

This command can display the existed WLAN connection status for the modem (change from router into bridge modem), including index number, MAC address, Stamp Time, PVC, VLAN port for Vigor Bridge Function.

Example

```
> vigbrg wlanstatus
Vigor Bridge: Running
WAN mac table:
Index   MAC Address           Stamp Time           PVC   VLan Port
```

Telnet Command: vlan group

This command allows you to set VLAN group. You can set four VLAN groups. Please run `vlan restart` command after you change any settings.

Syntax

`vlan group id [set/set_ex] [p1/p2/p3/p4/s1/s2/s3/s4]`

Syntax Description

Parameter	Description
<i>id</i>	It means the group 0 to 7 for VLAN.
<i>set</i>	It indicates each port can join more than one VLAN group.
<i>set_ex</i>	It indicates each port can join one VLAN group at one time.
<i>p1/p2/p3/p4</i>	It indicates LAN port 1 to LAN port 4. To group LAN1, LAN2, LAN3 and/or LAN4 under one VLAN group, please 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 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] [on/off]</i>	unlimited on: It allows the incoming of untagged packets even all VLAN are tagged. unlimited off: It does not allow the incoming of untagged packets.
<i>[p1_untag] [on/off]</i>	P1_untag on: It allows the incoming of untagged packets from LAN port 1.

	P1_untag off: It does not allow the incoming of untagged packets from LAN port 1.
--	---

Example

```
> vlan tagged unlimited on
unlimited mode is ON
```

Telnet Command: vlan vid

This command is used to configure VID number for each VLAN channel.

Syntax

vlan vid *n* *vid_no*

Syntax Description

Parameter	Description
<i>n</i>	It means VLAN channel. The range is from 0 to 7.
<i>vid_no</i>	It means the value of VLAN ID. Type the value as the VLAN ID number. The range is form 0 to 4095.

Example

```
> vlan vid 1 4095
VLAN1, vid=4095
```

Telnet Command: vlan sysvid

This command is used to modify and show the scope (reserved 78) of the VLAN IDs used internally by the system.

Syntax

vlan sysvid [*show* | *n*]

Syntax Description

Parameter	Description
<i>show</i>	It means to show the scope of VLAN ID used internally.
<i>n</i>	It means the value to be set as VLAN ID. The range is from 0 to 4018.

Example

```
> vlan sysvid 100
You have set system VLAN ID to range: 100 ~ 177,
We recommend that you reboot the system now.

> vlan sysvid 200
You have set system VLAN ID to range: 200 ~ 263,
We recommend that you reboot the system now.

> vlan sysvid show
The system VLAN ID is in range: 200 ~ 263
```

Telnet Command: vpn l2lset

This command allows users to set advanced parameters for LAN to LAN function.

Syntax

```
vpn l2lset [list index] peerid [peerid]  
vpn l2lset [list index] localid [localid]  
vpn l2lset [list index]main [auto/proposal index]  
vpn l2lset [list index] aggressive [g1/g2]  
vpn l2lset [list index]pfs [on/off]  
vpn l2lset [list index] phase1[lifetime]  
vpn l2lset [list index] phase2[lifetime]  
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</i>	It means the peer identity for aggressive mode.
<i>localid</i>	It means the local identity for aggressive mode.
<i>main</i>	It means to choose proposal for main mode.
<i>auto index</i>	It means to choose default proposals.
<i>proposal index</i>	It means to choose specified proposal.
<i>aggressive</i>	It means the chosen DH group for aggressive mode
<i>pfs</i>	It means "perfect forward secrete".
<i>on/off</i>	It means to turn on or off the PFS function.
<i>phase1</i>	It means phase 1 of IKE.
<i>lifetime</i>	It means the lifetime value (in second) for phase 1 and phase 2.
<i>phase2</i>	It means phase 2 of IKE.
<i>X509localid</i>	It means the local identity for X509 server.

Example

```
> vpn l2lset 1 peerid test
```

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 <0-4>
 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.
<on/off>	It means to enable or disable the profile. on - Enable. off - Disable.
motp <on/off>	It means to enable or disable the authentication with mOTP function. on - Enable. off - Disable.
pin_secret<pin> <secret>	It means to set PIN code with secret. <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)
timeout <0-9999>	It means to set the time out for dial-in VPN profile. The default is 300 seconds.
username	It means to set a username for dial-in VPN profile.
password	It means to set the password for dial-in VPN profile.
dintype <Type> <on/off>	It means to set dial-in type for creating VPN connection. <Type>- 0:PPTP,1:IPsec Tunnel,2:L2TP with IPsec Policy,3:SSL Tunnel <on/off> - on - Enable; off - Disable
subnet <0-4>	It means to set the LAN subnet for the VPN profile. 0:LAN1 1:LAN2 2:LAN3 3:LAN4 4:DMZ
assignip <on/off>	It means to enable the assignment for static IP address. on: enable off: disable.
smdoe <on/off>	It means to enable the function of Specify Remote Node. on: enable

	off: disable.
<i>remoteip</i> <Remote_Client_IP_Address >	It means to assign the IP address for the remote client.
<i>peer</i> <Peer_ID>	It means to assign the peer ID for such profile.
<i>naming</i> <pass/block>	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, it can block data transmission of Netbios Naming Packet inside the tunnel.
<i>multicastvpn</i> <pass/block>	Pass -Let multicast packets pass through the router. Block - This is default setting. It can let multicast packets be blocked by the router.
<i>prekey</i> <on/off>	It means to enable/disable the pre-shared key for IKE authentication method. on: enable off: disable.
<i>assignkey</i> <Pre_Shared_Key>	Assign the pre-shared key. Pre_Shared_Key - Type a string.
<i>digsig</i> <on/off>	Enable /disable the function of Digital Signature (X.509) for IKE authentication method.
<i>ipsec</i> <Method> <on/off>	Set the IPsec security method for the specified VPN profile. Method - 0:Medium(AH) High(ESP), 1:DES, 2:3DES, 3:AES on / off - enable / disable.
<i>localid</i> <Local_ID>	Assign a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. Local_ID - Type a string.

Example

```

> vpn dinset 1

Dial-in profile index 1

Profile Name: ???
Status: Deactive

Mobile OTP: Disabled

Password:

Idle Timeout: 300 sec

> vpn dinset 1 on
% set profile active

> vpn dinset 1 motp on
% Enable Mobile OTP mode!>
> vpn dinset 1 pin_secret 1234 e759bb6f0e94c7ab4fe6
> vpn dinset 1

Dial-in profile index 1

Profile Name: ???

```

```
Status: Active

Mobile OTP: Enabled

PIN: 1234

Secret: e759bb6f0e94c7ab4fe6

Idle Timeout: 300 sec
```

Telnet Command: vpn subnet

This command allows users to specify a subnet selection for the specified remote dial-in VPN profile.

Syntax

```
vpn subnet [index] [1/2/3/4]
```

Syntax Description

Parameter	Description
<index>	It means the index number of the VPN profile.
<1/2/3/4/5>	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.

Syntax

Command of PPTP Dial-Out

```
vpn setup <index> <name> pptp_out <ip> <usr> <pwd> <nip> <nmask>
```

Command of IPSec Dial-Out

```
vpn setup <index> <name> ipsec_out <ip> <key> <nip> <nmask>
```

Command of L2Tp Dial-Out

```
vpn setup <index> <name> l2tp_out <ip> <usr> <pwd> <nip> <nmask>
```

Command of Dial-In

```
vpn setup <index> <name> dialin <ip> <usr> <pwd> <key> <nip> <nmask>
```

Syntax Description

Parameter	Description
For PPTP Dial-Out	
<index>	It means the index number of the profile.

<name>	It means the name of the profile.
<ip>	It means the IP address to dial to.
<usr> <pwd>	It means the user and the password required for the PPTP connection.
<nip> <nmask>	It means the remote network IP and the mask. e.g., vpn setup 1 name1 pptp_out 1.2.3.4 vigor 1234 192.168.1.0 255.255.255.0
For IPsec Dial-Out	
<index>	It means the index number of the profile.
<name>	It means the name of the profile.
<ip>	It means the IP address to dial to.
<key>	It means the value of IPsec Pre-Shared Key.
<nip> <nmask>	It means the remote network IP and the mask. e.g., vpn setup 1 name1 ipsec_out 1.2.3.4 1234 192.168.1.0 255.255.255.0
For L2TP Dial-Out	
<index>	It means the index number of the profile.
<name>	It means the name of the profile.
<ip>	It means the IP address to dial to.
<usr> <pwd>	It means the user and the password required for the L2TP connection.
<nip> <nmask>	It means the remote network IP and the mask. e.g., vpn setup 1 name1 l2tp_out 1.2.3.4 vigor 1234 192.168.1.0 255.255.255.0
For Dial-In	
<index>	It means the index number of the profile.
<name>	It means the name of the profile.
<ip>	It means the IP address allowed to dial in.
<usr> <pwd>	It means the user and the password required for the PPTP/L2TP connection.
<key>	It means the value of IPsec Pre-Shared Key.
<nip> <nmask>	It means the remote network IP and the mask. e.g., vpn setup 1 name1 dialin 1.2.3.4 vigor 1234 abc 192.168.1.0 255.255.255.0

Example

```
> vpn setup 1 name1 dialin 1.2.3.4 vigor 1234 abc 192.168.1.0 255.255.255.0
% Profile Change Log ...

% Profile Index : 1
% Profile Name : name1
% Username : vigor
% Password : 1234
% Pre-share Key : abc
```

```

% Call Direction : Dial-In
% Type of Server : ISDN PPTP IPsec L2TP
% Dial from : 1.2.3.4
% Remote Network IP : 192.168.1.0
% Remote Network Mask : 255.255.255.0
>

```

Telnet Command: vpn option

This command allows users to configure settings for LAN to LAN profile.

Syntax

vpn option <index> <cmd1>=<param1> [<cmd2>=<para2> | ...]

Syntax Description

Parameter	Description
<index>	It means the index number of the profile. Available index numbers: 1 ~ 32
For Common Settings	
<index>	It means the index number of the profile.
<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>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.

Syntax

vpn mroute <index> list

vpn mroute <index> add <network ip>/<mask>

vpn mroute <index> del <network ip>/<mask>

Syntax Description

Parameter	Description
-----------	-------------

<i>list</i>	It means to display all of the route settings.
<i>add</i>	It means to add a new route.
<i>del</i>	It means to delete specified route.
<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.

Syntax

```
vpn list <index> all
vpn list <index> com
vpn list <index> out
vpn list <index> in
vpn list <index> net
```

Syntax Description

Parameter	Description
<i>all</i>	It means to list configuration of the specified profile.
<i>com</i>	It means to list common settings of the specified profile.
<i>out</i>	It means to list dial-out settings of the specified profile.
<i>in</i>	It means to list dial-in settings of the specified profile.
<i>net</i>	It means to list Network Settings of the specified profile.
<i><index></i>	It means the index number of the profile. Available index numbers: 1 ~ 32

Example

```
> vpn list 32 all
% Common Settings

% Profile Name           : ???
% Profile Status        : Disable
% Netbios Naming Packet : Pass
% Call Direction        : Both
% Idle Timeout          : 300
% PING to keep alive    : off

% Dial-out Settings
```



```

% Type of Server          : PPTP
% Link Type:              : 64k bps
% Username                : ???
% Password                :
% PPP Authentication      : PAP/CHAP
% VJ Compression          : on
% Pre-Shared Key          :
% IPSec Security Method   : AH
% Schedule                : 0,0,0,0
% Remote Callback         : off
% Provide ISDN Number     : off
% IKE phase 1 mode        : Main mode
% IKE Local ID            :

% Dial-In Settings

--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
> vpn list 1 com
% Common Settings

% Profile Name            : ???
% Profile Status          : Disable
% Netbios Naming Packet   : Pass
% Call Direction          : Both
% Idle Timeout            : 300
% PING to keep alive     : off
>

```

Telnet Command: vpn remote

This command allows users to enable or disable *PPTP/IPSec/L2TP* VPN service.

Syntax

vpn remote [*PPTP/IPSec/L2TP/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 2ndsubnet

This command allows users to enable second subnet IP as VPN server IP.

Syntax

vpn 2ndsubnet on

vpn 2ndsubnet off

Syntax Description

Parameter	Description
on/off	It means to enable or disable second subnet.

Example

```
> vpn 2ndsubnet on
%Enable second subnet IP as VPN server IP!
```

Telnet Command: vpn NetBios

This command allows users to enable or disable NetBios for Remote Access User Accounts or LAN-to-LAN Profile.

Syntax

vpn NetBios set <H2I/L2I> <index> <Block/Pass>

Syntax Description

Parameter	Description
<H2I/L2I>	H2I means Remote Access User Accounts. L2I means LAN-to-LAN Profile. Specify which one will be applied by NetBios.
<index>	The index number of the profile.
<Block/Pass>	Pass - Have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. Block - When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, set it block data transmission of Netbios Naming Packet inside the tunnel.

Example

```
> vpn NetBios set H2l 1 Pass
% Remote Dial In Profile Index [1] :
% NetBios Block/Pass: [PASS]
```

Telnet Command: vpn mss

This command allows users to configure the maximum segment size (MSS) for different TCP types.

Syntax

vpn mss show

vpn mss default

vpn mss set <connection type> <TCP maximum segment size range>

Syntax Description

Parameter	Description
<i>show</i>	It means to display current setting status.
<i>default</i>	TCP maximum segment size for all the VPN connection will be set as 1360 bytes.
<i>set</i>	Use it to specify the connection type and value of MSS.
<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
>vpn mss show
VPN TCP maximum segment size (MSS) :
  PPTP = 1400
  L2TP = 1360
  IPSec = 1360
  L2TP over IPSec = 1360

```

Telnet Command: vpn ike

This command is used to display IKE memory status and leakage list.

Syntax

vpn ike -q

Example

```

> vpn ike -q
IKE Memory Status and Leakage List

# of free L-Buffer=95, minimum=94, leak=1
# of free M-Buffer=529, minimum=529 leak=3
# of free S-Buffer=1199, minimum=1198, leak=1
# of free Msgid-Buffer=1024, minimum=1024

```

Telnet Command: vpn Multicast

This command allows users to pass or block the multi-cast packet via VPN.

Syntax

vpn Multicast set <H2I/L2I> <index> <Block/Pass>

Syntax Description

Parameter	Description
<H2I/L2I>	H2I means Host to LAN (Remote Access User Accounts). L2I means LAN-to-LAN Profile.
<index>	The index number of the profile.
<Block/Pass>	Set Block/Pass the Multicast Packets. The default is Block.

Example

```
> vpn Multicast set 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 second subnet is allowed to pass VPN tunnel. off -the second subnet is not allowed to pass VPN tunnel.

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 sameSubnet

This command allows users to build VPN between clients via virtual subnet.

```
Vpn sameS -I [value]
vpn sameS -E [0/1]
vpn sameS -e[value]
vpn sameS -I [xxx.xxx.xxx.xxx]
vpn sameS -o [add/del]
vpn sameS -v
```

Syntax Description

Syntax Description

Parameter	Description
-I [value]	It means to specify the index number of VPN profile.
-E [0/1]	It means to enable / disable the IpsecWithSameSubnet. 0: Disable 1: Enable.
-e [1/2/3/4]	It means to translate LAN subnet to virtual subnet. 1: LAN1 2: LAN2 3: LAN3 4: LAN4
-I [IP address]	Set the IP address as the virtual subnet.
-o [add/del]	Specify the operation to be performed.
-v	View the current settings. However, only the enabled profile will be viewed.

Example

```
> vpn sameS -i 1 -e 1 -E 1 -e 1 -I 10.10.10.0 -o add
> vpn sameS -v
IPsec with the same subnet:
VPN profile 1 enable,
% translated LAN1 to Virtual subnet: 10.10.10.0
```

Telnet Command: wan ppp_mru

This command allows users to adjust the size of PPP LCP MRU. It is used for specific network.

Syntax

```
wan ppp_mru <WAN interface number> <MRU size >
```

Syntax Description

Parameter	Description
<i><WAN interface number></i>	Type a number to represent the physical interface. For Vigor130, the number is 1 (which means WAN1).
<i><MRU size ></i>	It means the number of PPP LCP MRU. The available range is from 1400 to 1600.

Example

```
>wan ppp_mru 1 ?
% Now: 1492

> wan ppp_mru 1 1490
>
> wan ppp_mru 1 ?
% Now: 1490

> wan ppp_mru 1 1492
> wan ppp_mru 1 ?
% Now: 1492
```

Telnet Command: wan mtu

This command allows users to adjust the size of MTU for WAN1.

Syntax

wan mtu *[value]*

Syntax Description

Parameter	Description
<i>value</i>	It means the number of MTU for PPP. The available range is from 1000 to 1500. For Static IP/DHCP, the maximum number will be 1500. For PPPoE, the maximum number will be 1492. For PPTP/L2TP, the maximum number will be 1460.

Example

```
> wan mtu 1100
> wan mtu ?
Static IP/DHCP (Max MSS: 1500)
PPPoE(Max MSS: 1492)
PPTP/L2TP(Max MSS: 1460)
% wan ppp_mss <MSS size: 1000 ~ 1500>
% Now: 1100
```

Telnet Command: wan dns

This command allows you to configure the DNS server.

Syntax

wan dns *<wan_no>* *<dns_select>* *<ipv4_addr>*

Syntax Description

Parameter	Description
<i>wan_no</i>	It means to indicate the WAN interface. 1: WAN1
<i>dns_select</i>	It means to set primary or secondary DNS server.
<i>ipv4_addr</i>	It means to type the IPv4 address for the DNS server.

Example

```
> wan dns 1 pri 192.168.1.126
% Set WAN1 primary DNS done.
% Now: 192.168.1.126
```

Telnet Command: wan DF_check

This command allows you to enable or disable the function of DF (Don't fragment)

Syntax

`wan DF_check [on]`

`wan DF_check [off]`

Syntax Description

Parameter	Description
<i>on/off</i>	It means to enable or disable DF.

Example

```
> wan DF_check on
%DF bit check enable!
> wan DF_check off
%DF bit check disable (reset DF bit)!
```

Telnet Command: wan disable

This command allows you to disable WAN connection.

Example

```
> wan disable WAN
%WAN disabled.
```

Telnet Command: wan enable

This command allows you to disable wan connection.

Example

```
> wan enable WAN
%WAN1 enabled.
```

Telnet Command: wan forward

This command allows you to enable or disable the function of WAN forwarding. The packets are allowed to be transmitted between different WANs.

Syntax

`wan forward [on]`

wan forward *[off]*

Syntax Description

Parameter	Description
<i>on/off</i>	It means to enable or disable WAN forward.

Example

```
> wan forward ?
%WAN forwarding is Disable!

> wan forward on
%WAN forwarding is enable!
```

Telnet Command: wan status

This command allows you to display the status of WAN connection, including connection mode, TX/RX packets, DNS settings and IP address.

Example

```
> wan status
WAN1: Offline, stall=N
Mode: ---, Up Time=00:00:00
IP----, GW IP----
TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0
Primary DNS=0.0.0.0, Secondary DNS=0.0.0.0

PVC_WAN3: Offline, stall=N
Mode: ---, Up Time=00:00:00
IP----, GW IP----
TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0

PVC_WAN4: Offline, stall=N
Mode: ---, Up Time=00:00:00
IP----, GW IP----
TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0

PVC_WAN5: Offline, stall=N
Mode: ---, Up Time=00:00:00
IP----, GW IP----
TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0
```

Telnet Command: wan detect

This command allows you to configure WAN connection detection. When Ping Detection is enabled (for Static IP or DHCP or PPPoE mode), Router pings specified IP addresses to detect the WAN connection.

Syntax

```
wan detect <wan1> <on/off/always_on>
wan detect <wan1> <off> -t <time>
wan detect <wan1> <off> -i <Interval>
wan detect <wan1> target <ip addr>
wan detect <wan1> ttl <1-255>
```


wan detect <wan1> target2 <ip addr>
 wan detect <wan1> target_gw <1/0>
 wan detect <wan1> interval <interval>
 wan detect <wan1> retry <retry>
 wan detect status

Syntax Description

Parameter	Description
<i>on</i>	Enable ping detection. The IP address of the target shall be set.
<i>off</i>	Enable ARP detection (default).
<i>always_on</i>	Disable link detect, always connected(only support static IP)
<i>-t <time></i>	Set the time setting. The default value is "30" and the range shall be 1 to 255.
<i>-i <Interval></i>	Type the interval for the system to execute the PING operation. The default value is "5" and it shall be smaller than time setting.
<i>target <ip addr></i>	Set the IP address for ping target.
<i>target2 <ip addr></i>	Set the secondary ping target.
<i>target_gw <1/0></i>	Set whether to use gateway as ping target. (1: yes 0: no) Note that USB WAN (PPP mode) cannot support PING gateway
<i>tll <1-255></i>	It means to set the ping TTL value (work as trace route) If you do not set any value for ttl here or just type 0 here, the system will use default setting (255) as the ttl value.
<i>interval<Interval></i>	Set the interval between each ping operation. Available setting is between 1 and 3600. The unit is second. <i>interval:</i> Type a value.
<i>retry <retry></i>	Set how many ping operations are retried before the Router judges that the WAN connection is disconnected. Available setting is between 1 and 255. The unit is times. <i>retry :</i> Type a number.
<i>status</i>	It means to show the current status.

Example

```
> DrayTek> wan detect status
WAN1: off, send time=30, Interval = 5
WAN2: off, send time=30, Interval = 5
WAN3: off, send time=30, Interval = 5
WAN4: off, send time=30, Interval = 5
WAN5: off, send time=30, Interval = 5
WAN6: off, send time=30, Interval = 5>
```

Telnet Command: wan mvlan

This command allows you to configure multi-VLAN for WAN and LAN. It supports pure bridge mode (modem mode) between Ethernet WAN and LAN port 2~4.

Syntax

wan mvlan [*pvc_no/status/save/enable/disable*] [*on/off/clear/tag tag_no*] [*service type/vlan priority*] [*px ...*]
 wan mvlan *keeptag*[*pvc_no*][*on/off*]

Syntax Description

Parameter	Description
<i>pvc_no</i>	It means index number of PVC. There are 10 PVC, 0(Channel-1) to 9(Channel-9) allowed to be configured. However, bridge mode can be set on PVC number 2 to 9.
<i>status</i>	It means to display the whole Bridge status.
<i>save</i>	It means to save the configuration into flash of Vigor router.
<i>enable/disable</i>	It means to enable/disable the Multi-VLAN function.
<i>on/off</i>	It means to turn on/off bridge mode for the specific channel.
<i>clear</i>	It means to turn off/clear the port.
<i>tag tag_no</i>	It means to tag a number for the VLAN. -1: No need to add tag number. 1-4095: Available setting numbers used as tagged number.
<i>service type</i>	It means to specify the service type for VLAN. 0: Normal. 1: IGMP.
<i>vlan priority</i>	It means to specify the priority for the VALN setting. Range is from 0 to 7.
<i>px</i>	It means LAN port. Available setting number is from 2 to 4. Port number 1 is locked for NAT usage.
<i>keeptag</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 Service Type Tag Priority Keep Tag
-----
 7 ON 0 0 1 1 Normal 0(OFF) 0 OFF
>
```

Telnet Command: wan multifno

This command allows you to specify a channel (in Multi-PVC/VLAN) to make bridge connection to a specified WAN interface.

Syntax

`wan multifno [channel #] [WAN interface #]`

`wan multifno status`

Syntax Description

Parameter	Description
<i>channel #</i>	There are 4 (?) channels including VLAN and PVC. Available channel range: 4 ~ 10.
<i>WAN interface #</i>	Type a number to indicate the WAN interface. 1=WAN1
<i>status</i>	It means to display current bridge status.

Example

```

> wan multifno 5 1
% Configured channel 5 uplink to WAN1
> wan multifno status
% Channel 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
>

```

Telnet Command: wan vlan

This command allows you to configure the VLAN tag of WAN1.

Syntax

wan vlan wan [#] tag [value]

wan vlan wan [#] [enable/disable]

wan vlan wan [#] pri [value]

wan vlan stat

Syntax Description

Parameter	Description
wan [#]	Specify which WAN interface will be tagged.
tag [value]	Type a number for tagging on WAN interface.
enable/disable	Enable: Specified WAN interface will be tagged. Disable: Disable the function of tagging on WAN interface.
pri [value]	It means the priority for such VLAN. The value shall be 0 ~ 7.
stat	Display current VLAN status.

Example

```

> wan vlan stat

% Interface      Pri      Tag      Enabled
% =====
% WAN1           0        0

```

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 -i <Host/IP address> -s <mtu_size> -d <decrease size> -w <1> -c <1-10>

Syntax Description

Parameter	Description
-I [Host/IP address]	Specify the IPv4 target to detect. It can be an IPv4 address or domain name. Host/IP address: Type the IP address/domain name of the target.
-s [mtu_size]	Set the MTU size base for Discovery.

	base_size: Available setting is 1000 ~ 1500.
-d [<i>decrease size</i>]	Set the MTU size to decrease between detections. decrease size: Available setting is 1 ~ 100.
-w	Specify the WAN interface to be detected.
-c [<i>count</i>]	Set the times that you want to send the ping packets out. count: Available settings are 1 ~ 10. Default value is 3.

Example

```
> wan detect_mtu -w 1 -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 -i <Host/IP address> -s <mtu_size> -w <1>
```

Syntax Description

Parameter	Description
-i [<i>Host/IP address</i>]	Specify the IPv6 target to detect. It can be an IPv4 address or domain name. Host/IP address: Type the IP address/domain name of the target.
-s [<i>mtu_size</i>]	Set the MTU size base for Discovery. base_size: Available setting is 1280 ~ 1500.
-w	Specify the WAN interface to be detected.

Example

```
> wan detect_mtu6 -w 2 -i 2404:6800:4008:c06::5e -s 1500
>
```

Telnet Command: wl acl

This command allows the user to configure wireless access control settings.

Syntax

```
wl acl enable [ssid1 ssid2 ssid3 ssid4]
wl acl disable [ssid1 ssid2 ssid3 ssid4]
wl acl add [MAC] [ssid1 ssid2 ssid3 ssid4] [isolate]
wl acl del [MAC]
wl acl mode [ssid1 ssid2 ssid3 ssid4] [white/black]
wl acl show
wl acl showmode
wl acl clean
```

Syntax Description

Parameter	Description
<i>enable</i> [<i>ssid1 ssid2 ssid3 ssid4</i>]	It means to enable the settings for SSID1, SSID2, SSID3 and SSID4.

<i>disable [ssid1 ssid2 ssid3 ssid4]</i>	It means to disable the settings for SSID1, SSID2, SSID3 and SSID4.
<i>add [MAC] [ssid1 ssid2 ssid3 ssid4] [isolate]</i>	It means to associate a MAC address to certain SSID interfaces' access control settings. The isolate setting will limit the wireless client's network capabilities to accessing the wireless LAN only. [MAC] format: xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx or xx.xx.xx.xx.xx.xx
<i>del [MAC]</i>	It means to delete a MAC address entry defined in the access control list.
<i>mode [ssid1 ssid2 ssid3 ssid4] [white/black]</i>	It means to set white/black list for each SSID.
<i>wl acl show</i>	It means to show access control status.
<i>wl acl showmode</i>	It means to show the mode for each SSID.
<i>wl acl clean</i>	It means to clean all access control setting.

Example

```
> wl acl showmode
ssid1: none
ssid2: none
ssid3: none
ssid4: none
> wl acl add 00-50-70-ff-12-70
Set Done !!
> wl acl add 00-50-70-ff-12-70 ssid1 ssid2 isolate
Set Done !!
> wl acl show
-----Enable Mac Address Filter-----
ssid1: dis  ssid2: dis  ssid3: dis  ssid4: dis
-----MAC Address Filter-----
Index  Attribute      MAC Address      Associated SSIDs
  0                00:50:70:ff:12:70  ssid1 ssid2 ssid3 ssid4
  1                s                00:50:70:ff:12:70  ssid1 ssid2

s: Isolate the station from LAN
>
```

Telnet Command: wl config

This command allows users to configure general settings and security settings for wireless connection.

Syntax

wl config mode [value]

wl config mode show

wl config channel [number]

wl config preamble [enable]

wl config txburst [enable]

wl config ssid [ssid_num enable ssid_name [hidden_ssid]]

wl config security [SSID_NUMBER] [mode]

wl config ratectl [ssid_num enable upload download]

wl config isolate [*ssid_num lan member*]

Syntax Description

Parameter	Description
<i>mode[value]</i>	It means to select connection mode for wireless connection. Available settings are: "11bgn", "11gn", "11n", "11bg", "11g", or "11b".
<i>mode show</i>	It means to display what the current wireless mode is.
<i>channel [number]</i>	It means the channel of frequency of the wireless LAN. The available settings are 0,1,2,3,4,5,6,7,8,9,10,11,12 and 13. number=0, means Auto number=1, means Channel 1 number=13, means Channel 13.
<i>preamble [enable]</i>	It means to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. 0: disable to use long preamble. 1: enable to use long preamble.
<i>txburst [enable]</i>	It means to enhance the performance in data transmission about 40%* more (by enabling Tx Burst). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. 0: disable the function. 1: enable the funciton.
<i>ssid[ssid_num enable ssid_name [hidden_ssid]]</i>	It means to set the name of the SSID, hide the SSID if required. <i>ssid_num</i> : Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. <i>ssid_name</i> : Give a name for the specified SSID. <i>hidden_ssid</i> : Type 0 to hide the SSID or 1 to display the SSID
<i>Security [SSID_NUMBER] [mode][key][index]</i>	It means to configure security settings for the wireless connection. <i>SSID_NUMBER</i> : Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. <i>mode</i> : Available settings are: disable: No security. wpa1x: WPA/802.1x Only wpa21x: WPA2/802.1x Only wpamix1x: Mixed (WPA+WPA2/802.1x only) wep1x: WEP/802.1x Only wpapsk: WPA/PSK wpa2psk: WPA2/PSK wpamixpsk: Mixed (WPA+WPA2)/PSK wep: WEP <i>key, index</i> : Moreover, you have to add keys for <i>wpapsk</i> , <i>wpa2psk</i> , <i>wpamixpsk</i> and <i>wep</i> , and specify index number of schedule profiles to be followed by the wireless connection. WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8-63 ASCII text string or 64 Hexadecimal digit format.
<i>ratectl [ssid_num enable upload download]</i>	It means to set the rate control for the specified SSID. <i>ssid_num</i> : Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. <i>enable</i> : It means to, enable the function of the rate control for the

	<p>specified SSID. 0: disable and 1:enable.</p> <p><i>upload</i>: It means to configure the rate control for data upload. The unit is kbps.</p> <p><i>download</i>: It means to configure the rate control for data download. The unit is kbps.</p>
<i>isolate [ssid_num lan member]</i>	<p>It means to isolate the wireless connection for LAN and/or Member.</p> <p><i>lan</i> - It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other.</p> <p><i>member</i> - It can make the wireless clients (stations) with the same SSID not accessing for each other.</p>

Example

```

> wl config mode 11bgn
Current mode is 11bgn
% <Note> Please restart wireless after you set the channel
> wl config channel 13
Current channel is 13
% <Note> Please restart wireless after you set the channel.
> wl config preamble 1
Long preamble is enabled
% <Note> Please restart wireless after you set the parameters.
> wl config ssid 1 enable dray
SSID Enable Hide_SSID Name
1 1 0 dray
% <Note> Please restart wireless after you set the parameters.
> wl config security 1 wpa1x
%% Configured Wlan Security Setting:
% SSID1
%% Mode: wpa1x
%% Wireless card must be reset for configurations to take effect
%% (Telnet Command: wl restart)

```

Telnet Command: wl set

This command allows users to configure basic wireless settings.

Syntax

`wl set [SSID] [CHAN[En]]`

`wl set txburst [enable]`

Syntax Description

Parameter	Description
<i>SSID</i>	It means to type the SSID for the router. The maximum character that you can use is 32.
<i>CHAN[En]</i>	It means to specify required channel for the router. <i>CHAN</i> : The range for the number is between 1 ~ 13. <i>En</i> : type <i>on</i> to enable the function; type <i>off</i> to disable the function.
<i>txburst [enable]</i>	It means to enhance the performance in data transmission about 40%* more (by enabling Tx Burst). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. 0: disable the function. 1: enable the function.

Example

```
> wl set MKT 2 on
% New Wlan Setting is:
% SSID=MKT
% Chan=2
% Wl is Enable
```

Telnet Command: wl act

This command allows users to activate wireless settings.

Syntax

`wl act [En]`

Syntax Description

Parameter	Description
<i>En</i>	It means to enable or disable the function of VPN isolation. 0: diable 1: enable

Example

```
> wl act on
% Set Wlan to Enable.
```

Telnet Command: wl scan

This command allows users to perform AP scanning.

Syntax

`wl scan [start]`

`wl scan set [wlist/blist/stime][MAC]`

`wl scan del [wlist/blist] [MAC]`

`wl scan filter [ssid/channel/mac]`

`wl scan show [0/1/2/3]`

Syntax Description

Parameter	Description
<i>start</i>	It means to start AP scanning.
<i>set [wlist/blist/stime] [MAC]</i>	Set white list/block list/scan time. <i>wlist</i> - It means to set white list for passing. MAC address must be added in the end. e.g., <code>wl scan set wlist 001122aabbcc</code> <i>blist</i> - It means to set black list for blocking. MAC address must be added in the end. <i>stime</i> - It means to set scanning time. Time value (2-5 second) must be added in the end. e.g., <code>wl scan set time 5</code>
<i>del</i>	Remove white list/block list. e.g., <code>wl scan del wlist 001122aabbcc</code>
<i>filter</i>	Set which filter you want.

	<i>ssid</i> - scanning the AP based on SSID setting. <i>channel</i> - scanning the AP based on channel setting. <i>mac</i> - scanning the AP based on MAC address setting.
<i>show [0/1/2/3]</i>	It is used to show AP list. 0 - display white list 1 - display block list, 2 - display gray/unknown list, 3 - display all list

Example

```
> wl scan set wlist 001122aabbcc
> wl scan start
> wl scan show 3
>
```

Telnet Command: wl stamgt

This command is used to configure connection time and reconnection time for each SSID that wireless client used for accessing into Internet.

Syntax

wl stamgt [enable/disable] [ssid_num].

wl stamgt [show] [ssid_num].

wl stamgt set [ssid_num] [c] [r]

wl stamgt reset [ssid_num].

Syntax Description

Parameter	Description
<i>enable/disable</i>	It means to enable/disable the station management control.
<i>ssid_num</i>	It means channel selection. Available channel for 2.4G: 0/1/2/3 Available channel for 5G: 4/5/6/7.
<i>show</i>	It means to display status or configuration of the selected channel.
<i>c</i>	It means connection time. The unit is minute.
<i>r</i>	It means reconnection time. The unit is minute.

Example

```
> wl stamgt enable 1
% Station Management Status: enabled
> wl stamgt set 1 60 60
> wl stamgt show 1
NO. SSID          BSSID          Connect time  Reconnect time
1. Draytek       00:11:22:aa:bb:cc 0d:0:58:26   0d:0:0
```

Telnet Command: wl iso_vpn

This command allows users to activate the function of VPN isolation.

Syntax

wl iso_vpn [ssid] [En]

Syntax Description

Parameter	Description
<i>ssid</i>	It means the number of SSID. 1: SSID1 2: SSID2 3: SSID3 4: SSID4
<i>En</i>	It means to enable or disable the function of VPN isolation. 0: disable 1: enable

Example

```
> wl iso_vpn 1 on
% ssid: 1 isolate vpn on :1
```

Telnet Command: wl wpa

This command allows you to configure WPA wireless settings.

Syntax

wl wpa 1/2/3

Syntax Description

Parameter	Description
<i>wl wpa</i>	Type 1/2/3 to represent different WPA modes. 1 - means WPA+WPA2 2 - means WPA2 Only 3 - means WPA Only

Example

```
> wl wpa 1
>
```

Telnet Command: wl wmm

This command allows users to set WMM for wireless connection. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs).

Syntax

```
wl wmm ap QueIdx Aifsn Cwmin Cwmax Txop ACM
wl wmm bss QueIdx Aifsn Cwmin Cwmax Txop ACM
wl wmm ack Que0_Ack Que1_Ack Que2_Ack Que3_Ack
wl wmm enable SSID0 SSID1 SSID2 SSID3
wl wmm apsd value
wl wmm show
```

Syntax Description

Parameter	Description
<i>ap</i>	It means to set WMM for access point.
<i>bss</i>	It means to set WMM for wireless clients.
<i>ack</i>	It means to map to the Ack policy settings of AP WMM.
<i>enable</i>	It means to enable the WMM for each SSID. 0: disable 1: enable
<i>Apsd [value]</i>	It means to enable / disable the ASPD(automatic power-save delivery) function. 0: disable 1: enable
<i>show</i>	It displays current status of WMM.
<i>QueIdx</i>	It means the number of the queue which the WMM settings will be applied to. There are four queues, best effort, background, voice, and video.
<i>Aifsn</i>	It controls how long the client waits for each data transmission.
<i>Cwmin/ Cwmax</i>	CWMin means contention Window-Min and CWMax means contention Window-Max. Specify the value ranging from 1 to 15.
<i>Txop</i>	It means transmission opportunity. Specify the value ranging from 0 to 65535.
<i>ACM</i>	It can restrict stations from using specific category class if it is enabled. 0: disable 1: enable

Example

```

> wl wmm ap 0 3 4 6 0 0
  QueIdx=0: APAifsn=3,APCwmin=4,APCwmax=6, APTxop=0,APACM=0
> wl wmm enable 1 0 1 0
  WMM_SSID0 =1, WMM_SSID1 =0,WMM_SSID2 =1,WMM_SSID3 =0
> wl wmm show
  Enable WMM: SSID0 =1, SSID1 =0,SSID2 =1,SSID3 =0
  APSD=0
  QueIdx=0: APAifsn=3,APCwmin=4,APCwmax=6, APTxop=0,APACM=0
  QueIdx=1: APAifsn=7,APCwmin=4,APCwmax=10, APTxop=0,APACM=0
  QueIdx=2: APAifsn=1,APCwmin=3,APCwmax=4, APTxop=94,APACM=0
  QueIdx=3: APAifsn=1,APCwmin=2,APCwmax=3, APTxop=47,APACM=0
  QueIdx=0: BSSAifsn=3,BSSCwmin=4,BSSCwmax=10, BSSTxop=0,BSSACM=0
  QueIdx=1: BSSAifsn=7,BSSCwmin=4,BSSCwmax=10, BSSTxop=0,BSSACM=0
  QueIdx=2: BSSAifsn=2,BSSCwmin=3,BSSCwmax=4, BSSTxop=94,BSSACM=0
  QueIdx=3: BSSAifsn=2,BSSCwmin=2,BSSCwmax=3, BSSTxop=47,BSSACM=0
  AckPolicy[0]=0: AckPolicy[1]=0,AckPolicy[2]=0,AckPolicy[3]=0

```

Telnet Command: *wl ht*

This command allows you to configure wireless settings.

Syntax

wl ht bw value

wl ht gi value

wl ht badecline value

wl ht autoba value

wl ht rdg value

wl ht msdu value

wl ht txpower value

wl ht antenna value

wl ht greenfield value

Syntax Description

Parameter	Description
<i>wl ht bw value</i>	The value you can type is 0 (for BW_20) and 1 (for BW_40).
<i>wl ht gi value</i>	The value you can type is 0 (for GI_800) and 1 (for GI_4001)
<i>wl ht badecline value</i>	The value you can type is 0 (for disabling) and 1 (for enabling).
<i>wl ht autoba value</i>	The value you can type is 0 (for disabling) and 1 (for enabling).
<i>wl ht rdg value</i>	The value you can type is 0 (for disabling) and 1 (for enabling).
<i>wl ht msdu value</i>	The value you can type is 0 (for disabling) and 1 (for enabling).
<i>wl ht txpower value</i>	The value you can type ranges from 1 - 6 (level).
<i>wl ht antenna value</i>	The value you can type ranges from 0-3. 0: 2T3R 1: 2T2R 2: 1T2R 3: 1T1R
<i>wl ht greenfield value</i>	The value you can type is 0 (for mixed mode) and 1 (for green field).

Example

```
> wl ht bw value 1
  BW=0
  <Note> Please restart wireless after you set new parameters.
> wl restart
  Wireless restart.....
```

Telnet Command: wl restart

This command allows you to restart wireless setting.

Example

```
> wl restart
Wireless restart.....
```

Telnet Command: wl wds

This command allows you to configure WDS settings.

Syntax

`wl wds mode [value]`

`wl wds security [value]`

`wl wds ap [value]`

`wl wds hello [value]`

`wl wds status`

`wl wds show`

`wl wds mac [value]`

`wl wds flush`

Syntax Description

Parameter	Description
<code>mode [value]</code>	It means to specify connection mode for WDS. [value]: Available settings are : d: Disable b: Bridge r: Repeater
<code>security [value]</code>	It means to configure security mode with encrypted keys for WDS. <i>mode</i> : Available settings are: disable: No security. wep: WEP wpapsk [key]: WPA/PSK wpa2psk [key]: WPA2/PSK <i>key</i> : Moreover, you have to add keys for <i>wpapsk</i> , <i>wpa2psk</i> , and <i>wep</i> , and specify index number of schedule profiles to be followed by the wireless connection. WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8-63 ASCII text string or 64 Hexadecimal digit format. e.g., <code>wl dual wds security disable</code> <code>wl dual wds security wep 12345</code> <code>wl dual wds security wpa2psk 12345678</code>
<code>ap [value]</code>	It means to enable or disable the AP function. Value: 1 - enable the function. 0 - disable the function.
<code>hello [value]</code>	It means to send hello message to remote end (peer). Value: 1 - enable the function.

	0 - disable the function.
<i>status</i>	It means to display WDS link status for 2.4GHz connection.
<i>show</i>	It means to display current WDS settings.
<i>mac add [index addr]</i>	add <i>[index addr]</i> - Add the peer MAC entry in Repeater/Bridge WDS MAC table.
<i>mac clear/disable/enable [index/all]</i>	clear/disable/enable <i>[index/all]</i> - Clear, disable, enable the specified or all MAC entries in Repeater/Bridge WDS MAC table. e.g, <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.

Syntax

wl btnctl *[value]*

Syntax Description

Parameter	Description
<i>value</i>	0: disable 1: enable

Example

```
> wl btnctl 1
Enable wireless button control
Current wireless button control is on
>
```

Telnet Command: wl iwpriv and wl ce_cert

These commands are reserved for RD debug. Do not use them.

Telnet Command: wl efuse

This command is used to configure parameters related to wireless RF hardware. At present, it is not allowed for end user to operate.

Telnet Command: wl set8021x

This command allows you to configure the external or internal server used by Vigor router for wireless authentication.

Syntax

wl set8021x -t *[0/1]*

wl set8021x -v

Syntax Description

Parameter	Description
-t	Specify the type (external or internal) of wireless authentication server. 0 - Indicate the external RADIUS server. 1 - Indicate the local 802.1x server.
-v	View the settings of 802.1x.

Example

```
> wl set8021x -t 1
% <Note> Please restart wireless after you set the parameters.
> wl set8021x -v
802.1X type is : Local 802.1X
>
```

Telnet Command: wl artfns

This command allows users to configure airtime fairness function for wireless (2.4GHz) connection.

Syntax

wl artfns enable *[value]*

wl artfns trg_num *[value]*

wl artfns show

Syntax Description

Parameter	Description
<i>enable [value]</i>	It means to enable wireless airtime fairness function. 1 - enable 0 - disable
<i>Trg_num [value]</i>	Set a threshold when the active station number achieves this number, the airtime fairness function will be applied. Available values will be 2 to 64.
<i>show</i>	Display current status (enable or disable) and triggering client number for airtime fairness function.

Example

```
> wl artfns enable 1
> wl artfns trg_num 3
> wl artfns show
airtime fairness: enable
trg_num: 3
>
```

Telnet Command: wl_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 cardmac

Example

```
> wl_dual cardmac
Card MAC: 54:2a:a2:37:00:ef
```

Telnet Command: wl_dual config

This command allows users to configure general settings and security settings for wireless connection (5GHz).

wl_dual config enable *[value]*

wl dual config enable show

wl_dual config mode *[value]*

wl_dual config mode show

wl_dual config channel *[number]*

wl_dual config channel show

wl_dual config preamble *[enable]*

wl_dual config preamble show

wl_dual config ssid *[ssid_num enable ssid_name]*

wl_dual config ssid hide *[ssid_num enable]*

wl_dual config ssid show

wl_dual config ratectl *[ssid_num enable upload download]*

`wl_dual config ratectl show`
`wl_dual config isolate lan [ssid_num enable]`
`wl_dual config isolate member [ssid_num enable]`
`wl_dual config isolate vpn [ssid_num enable]`
`wl_dual config isolate show`

Syntax Description

Parameter	Description
<code>enable[value]</code>	It means to enable/disable the 5GHz wireless function. 1: enable 0: disable
<code>show</code>	It means to display if 5G wireless function is enabled or not.
<code>mode[value]</code>	It means to select connection mode for wireless connection. Available settings are: "11a", "11n_5g", "11n" and "11an".
<code>mode show</code>	It means to display what the current wireless mode is.
<code>channel [number]</code>	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.
<code>channel show</code>	It means to display what the current channel is.
<code>preamble [enable]</code>	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.
<code>preamble show</code>	It means to display if preamble is enabled or not.
<code>ssid[ssid_num enable ssid_name]</code>	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.
<code>ssid hide [ssid_num enable]</code>	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. enable: Type 0 to hide the SSID or 1 to display the SSID.
<code>ssid show</code>	It means to display a table of SSID configuration.
<code>ratectl [ssid_num enable upload download]</code>	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: <code>wl_dual config ratectl 1 1 25 25</code>)
<code>ratectl show</code>	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.

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 [SSID_NUMBER] [mode][key][index]</i>	<p><i>SSID_NUMBER</i>: Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4.</p> <p><i>mode</i>: Available settings are:</p> <ul style="list-style-type: none"> 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 <p><i>key, index</i>: Moreover, you have to add keys for <i>wpapsk</i>, <i>wpa2psk</i>, <i>wpamixpsk</i> and <i>wep</i>, and specify index number of schedule profiles to be followed by the wireless connection.</p> <p>WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8-63 ASCII text string or 64 Hexadecimal digit format.</p>
<i>show</i>	It means to display current mode selection for each SSID.

Example

```

> wl_dual security 1 wpa2psk 123456789e
% <Note> Please restart 5G wireless after you set the parameters.

> wl_dual security show
%% 5G Wireless LAN Security Settings:
% SSID1
%% Mode: WPA2/PSK
% SSID2
%% Mode: Disable
% SSID3
%% Mode: Disable
% SSID4
%% Mode: Disable

```

Telnet Command: wl_dual stalist

This command is used to display the wireless station which accessing Internet via Vigor2120.

Syntax

wl dual stalist

Example

```

> wl_dual stalist
5G Wireless Station List :

Index  Status  IP Address          MAC Address          Associated with

Status Codes :

```

C: Connected, No encryption.
E: Connected, WEP.
P: Connected, WPA.
A: Connected, WPA2.
B: Blocked by Access Control.
N: Connecting.
F: Fail to pass WPA/PSK authentication.

Telnet Command: `wl_dual wds`

This command allows users to configure WDS for wireless connection (5GHz).

Syntax

```
wl_dual wds mode [value]
wl_dual wds security [value]
wl_dual wds ap [value]
wl_dual wds hello [value]
wl_dual wds status
wl_dual wds show
wl_dual wds mac add [index addr]
wl_dual wds mac clear/disable/enable [index/all]
wl_dual wds flush
```

Syntax Description

Parameter	Description
<code>mode [value]</code>	It means to specify connection mode for WDS. [value]: Available settings are : d: Disable b: Bridge r: Repeater
<code>security [value]</code>	It means to configure security mode with encrypted keys for WDS. <i>mode</i> : Available settings are: disable: No security. wep: WEP wpapsk [key]: WPA/PSK wpa2psk [key]: WPA2/PSK <i>key</i> : Moreover, you have to add keys for <i>wpapsk</i> , <i>wpa2psk</i> , and <i>wep</i> , and specify index number of schedule profiles to be followed by the wireless connection. WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8-63 ASCII text string or 64 Hexadecimal digit format. e.g., <code>wl_dual wds security disable</code> <code>wl_dual wds security wep 12345</code> <code>wl_dual wds security wpa2psk 12345678</code>
<code>ap [value]</code>	It means to enable or disable the AP function. Value: 1 - enable the function. 0 - disable the function.
<code>hello [value]</code>	It means to send hello message to remote end (peer).

	Value: 1 - enable the function. 0 - disable the function.
status	It means to display WDS link status for 5GHz connection.
show	It means to display current WDS settings.
mac add <i>[index addr]</i>	add <i>[index addr]</i> - Add the peer MAC entry in Repeater/Bridge WDS MAC table.
mac clear/disable/enable <i>[index/all]</i>	clear/disable/enable <i>[index/all]</i> - Clear, disable, enable the specified or all MAC entries in Repeater/Bridge WDS MAC table. e.g, <i>wl_dual wds mac enable 1</i>
flush	It means to reset all WDS setting.

Example

```

> wl_dual wds status
Please enable WDS hello function first.

> wl_dual wds hello 1
% <Note> Please restart router after you set the parameters.
> wl dual wds mode b
> wl dual wds security wep
>
>
> wl_dual wds show
5G Wireless WDS Setting

Mode : Bridge
Security : WEP
AP Function : Enable
Send Hello Function : Enable

Bridge :
Index  Enable  MAC Address
  1      0    00:00:00:00:00:00
  2      0    00:00:00:00:00:00
  3      0    00:00:00:00:00:00
  4      0    00:00:00:00:00:00

Repeater :
Index  Enable  MAC Address
  5      0    00:00:00:00:00:00
  6      0    00:00:00:00:00:00
  7      0    00:00:00:00:00:00
  8      0    00:00:00:00:00:00
> wl_dual wds wep 12345
% <Note> Please restart router after you set the parameters.

```

Telnet Command: wl_dual wps

This command allows users to configure WPS for wireless connection (5GHz).

Syntax

wl_dual wps enable *[value]*

wl dual wps pbc

wl_dual wps pin *[code]*

wl_dual wps show

Syntax Description

Parameter	Description
<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 apcli

This command allows users to configure AP client mode for wireless connection (5GHz).

Syntax

wl_dual apcli show

wl_dual apcli enable *[value]*

wl_dual apcli security *[mode]*

wl_dual apcli ssid *[ssid_name]*

wl_dual apcli bssid

Syntax Description

Parameter	Description
<i>show</i>	Display current status of wireless AP client.
<i>enable [value]</i>	It means to enable wireless 5GHz AP client mode. 1 - enable 0 - disable
<i>Security [mode]</i>	There are several modes to be selected: Disable - disable the security settings. wpapsk [key] - WPA Pre-shared Key will be used. Keys must start with 0x to be identified as a Hexadecimal number key. WPA keys must be in 8-63 ASCII string or 64 Hexadecimal digit format. wpa2psk [key] - WPA2 Pre-shared Key will be used. Keys must start with 0x to be identified as a Hexadecimal number key. WPA keys must be in 8-63 ASCII string or 64 Hexadecimal digit format. wpamixpsk [key] - WPA Mixed Pre-shared Key will be used. Keys must start with 0x to be identified as a Hexadecimal number key. WPA keys must be in 8-63 ASCII string or 64 Hexadecimal digit format.

	wep [key] [index] - WEP key will be used. You need to type the key string and specify the index number of the profile to be applied. WEP keys must be in 5/13 ASCII string or 10/26 Hexadecimal digit format.
<i>ssid [ssid_name]</i>	Specify the SSID for wireless 5GHz AP client.
<i>bssid</i>	Type the MAC address for wireless 5GHz AP client.

Example

```
> wl_dual apcli enable 1
Wireless 5G AP-Clinet is enabled
Vigor> wl_dual apcli show
% Wireless 5G AP-Clinet is enabled
% Current SSID is
%% Security Mode: disable
% Wireless 5G client is disconnected
%% data rate=---, mode=---, signal=0%
> wl_dual apcli ssid carrie
% <Note> Please restart wireless 5g after you set the parameters.
Current SSID is carrie
```

Telnet Command: wl_dual artfns

This command allows users to configure airtime fairness function for wireless (5GHz) connection.

Syntax

`wl_dual artfns enable [value]`

`wl_dual artfns trg_num [value]`

`wl_dual artfns show`

`wl_dual artfns status`

Syntax Description

Parameter	Description
<i>enable [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: radius

This command allows you to configure detailed settings for RADIUS server

Syntax

`radius enable [0/1]`

`radius authport [port number]`

`radius client [add] [idx] -i [address] -m [mask] -p [prefix] -l [length] -s [secret]`

`radius client [del] [idx]`

`radius show`

`radius set_dot1x_phase1 -e [method_idx]`

`radius set_dot1x_phase1 -d [method_idx]`

`radius set_dot1x_phase2 -e [method_idx]`

`radius set_dot1x_phase2 -d [method_idx]`

Syntax Description

Parameter	Description
<code>enable[0/1]</code>	Enable (1) or disable (0) the RADIUS server.
<code>authport [port number]</code>	Configure the port number for authentication. Port number: Available range is from 0 to 65535. Default value is "1812".
<code>set_auth_method [method idx]</code>	Specify which method will be used for authentication. Method idx: "0" is "Only PAP"; "1" is "PAP/CHAP/MS-CHAP/MS-CHAPv2".
<code>client add</code>	Specify a client to be authenticated by RADIUS server by typing required information as follows: -i [address]: client IPv4 address(domain) -m [mask]: client IPv4 mask -p [prefix]: client IPv6 prefix -l [length]: client IPv6 prefix length -s [secret]: shared secret ex: radius client add 1 -i 192.168.1.1 -m 255.255.255.0 -s 123
<code>client [del] [idx]</code>	<code>del</code> - Delete related settings for selected client. <code>idx</code> - Specify the index number of client profiles.
<code>show</code>	Display the status of RADIUS server.
<code>enable_dot1x [0/1]</code>	Enable (1) or disable (0) the 802.1X Authentication function of RADIUS Server. Default is disabled.
<code>set_dot1x_phase1</code>	Set the phase1 method for 802.1X authentication of RADIUS server.

<i>[method_idx]</i>	<i>method_idx</i> - Specify which method will be used. At present, dot1x_phase1 can only support PEAP now. So only "1" can be used for it.
<i>set_dot1x_phase2</i> <i>[method_idx]</i>	Set the phase2 method for 802.1X authentication of RADIUS server. <i>method_idx</i> - Specify which method will be used. Dot1x_phase2 can only support MS-CHAPv2 now. So only "1" can be used for it.
-e	Set method for dot1x_phase1 or dot1x_phase2.
-d	Delete method for dot1x_phase1 or dot1x_phase2.

Example

```
> radius client add 1 -i 192.168.1.1 -m 255.255.255.0 -s 123
This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

Telnet Command: wol

This command allows Administrator to set the white list of WAN IP addresses/Subnets, that the magic packet from these IP addresses/Subnets will be eligible to pass through NAT and wake up the LAN client. You also need to set NAT rule for LAN client.

Syntax

```
wol up [MAC Address]
wol fromWan [on/off/any]
wol fromWan_Setting [idx][ip address][mask]
```

Syntax Description

Parameter	Description
<i>MAC Address</i>	It means the MAC address of the host.
<i>on/off/any</i>	It means to enable or disable the function of WOL from WAN. on: enable off: disable any: It means any source IP address can pass through NAT and wake up the LAN client. This command will allow the user to choose whether WoL packets can be passed from the Internet to the LAN network from a specific WAN interface.
<i>[idx][ip address] [mask]</i>	It means the index number (from 1 to 4). These commands will allow the user to configure the LAN clients that the user may wake up from the Internet through the use of the WoL packet. <i>ip address</i> - It means the WAN IP address. <i>mask</i> - It means the mask of the IP address.

Example

```
> wol fromWan on
> wol fromWan_Setting 1 192.168.1.45 255.255.255.0
>
```

Telnet Command: user

The command is used to create new user account profiles.

Syntax

sser set [-a/-b/-c/-d/-e/-l/-o/-q/-r/-s/-u]

user edit [PROFILE_IDX]

[-a/-d/-e/-f/-i/-m/-n/-p/-q/-r/-s/-t/-u/-v/-w/-x/-A/-H/-T/-P/-I/-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> - type the index number of the selected profile. <i>User name</i> - type the user name that you want it to pass. <i>IP_Address</i> - type the IP address that you want it to pass.
<i>-c[user name]</i> <i>-c all</i>	Clear the user record. <i>user name</i> - type the user name that you want to get clear corresponding record. <i>all</i> - all of the records will be removed.
<i>-d</i>	Set User management function in Rule-Based mode.
<i>-e</i>	Set User management function in User-Based mode.
<i>-l all</i> <i>-l user</i> <i>-l ip</i>	Show online user. <i>all</i> - all of the users will be displayed on the screen. <i>user name</i> - type the user name that you want to view on the screen. <i>ip</i> - type the IP address that you want to view on the screen.
<i>-o</i>	It means to show user account information. e.g., <i>-o</i>
<i>-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> - type the name of the user profile. <i>all</i> - all of the user profile settings will be removed.
<i>-s</i>	It means to set login service. 0:HTTPS 1:HTTP e.g., <i>-s 1</i>
<i>-b user [user name]</i> <i>-b ip [ip address]</i>	Block specifies user or IP address. <i>user name</i> - type the user name that you want to block. <i>ip address</i> -- type the IP address that you want to block.
<i>-u user [user name]</i> <i>-u ip [ip address]</i>	Unblock specifies user or IP address. <i>user name</i> - type the user name that you want to unblock. <i>ip address</i> -- type the IP address that you want to unblock.

<i>User edit</i>	
<i>PROFILE_IDX</i>	Type the index number of the profile that you want to edit.
<i>-a [Param]</i>	Enable / disable the internal RADIUS service. 0:Disable 1:Enable
<i>-e</i>	Enable User profile function.
<i>-d</i>	Disable User profile function.
<i>-f [Param]</i>	Enable / disable local 802.1x user service. 0:Disable 1:Enable
<i>-i [Param]</i>	It means to set idle time. e.g., <i>-i 60</i>
<i>-n [Param]</i>	It means to set a user name for a profile. e.g., <i>-n fortest</i>
<i>-p [Param]</i>	It means to configure user password. e.g., <i>-p 60fortest</i>
<i>-q [Param]</i>	set time quota It means to set time quota of the user profile. e.g., <i>-q 200</i>
<i>-r [Param]</i>	It means to set data quota. e.g., <i>-r 1000</i>
<i>-s [Param]</i>	It means to set schedule index. Available settings are "sch_idx1,sch_idx2,sch_idx3, and sch_idx4".
<i>-t [Param]</i>	It means to enable /disable time quota limitation for user profile 0:Disable 1:Enable
<i>-u [Param]</i>	It means to enable /disable data quota limitation for user profile 0:Disable 1:Enable
<i>-v</i>	It means to view user profile(s).
<i>-w [Param]</i>	It means to specify the data quota unit (MB/GB). e.g., <i>-w MB</i>
<i>-x [Param]</i>	It means to set external server authentication 0: None 1: LDAP 2: Radius 3: TACAS e.g., <i>-x 2</i>
<i>-l [Param]</i>	Set Log Type. 0:None, 1:Login, 2:Event, 3:All
<i>-p [Param]</i>	Set Pop Browser Tracking Window. 0:Disable, 1:Enable
<i>-T [Param]</i>	Set Authentication by Telnet. 0:Disable,

	1:Enable
<i>-H [Param]</i>	Set Authentication by WEB. 0:Disable, 1:Enable
<i>-A [Param]</i>	Set Authentication by Alert Tool. 0:Disable, 1:Enable
<i>-M [Param]</i>	Set the reset default quota type. 0: when login permission schedule expired, 1: at the start time of schedule]
<i>-I [Param]</i>	Set the reset default quota schedule index to do schedule at the start time.
<i>-S</i>	Show the reset default quota type and schedule index.
<i>User account</i>	
<i>USER_NAME</i>	It means to type a name of the user account.
<i>-d</i>	It means to enable /disable data quota limitation for user account. 0:Disable 1:Enable
<i>-q</i>	It means to set account time quota. e.g., <i>-q 200</i>
<i>-r</i>	It means to set account data quota. e.g., <i>-r 1000</i>
<i>-t</i>	It means to enable /disable time quota limitation for user account. 0:Disable 1:Enable
<i>-w</i>	It means to set data quota unit (MB/GB).

Example

```
> user account admin -d 1
Enable the [admin] data quota limited
```

Telnet Command: appqos

The command is used to configure QoS for APP.

Syntax

appqos view

appqos enable *[0/1]*

appqos traceable *[-v | -e AP_INDEX CLASS | -d AP_INDEX]*

appqos untraceable *[-v | -e AP_INDEX CLASS | -d AP_INDEX]*

Syntax Description

Parameter	Description
<i>view</i>	It means to display current status of APP QoS.
<i>enable[0/1]</i>	It means to enable or disable the function of APP QoS. 0:Disable 1:Enable
<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.

Syntax

nand bad

nand usage

Example

```
>nand usage
Show NAND Flash Usage:
Partition      Total          Used           Available      Use%
cfg            4194304        7920           4186384        0%
bin_web       33554432       11869493       21684939       35%
cfg-bak       4194304        7920           4186384        0%
bin_web-bak   33554432       11869493       21684939       35%
> nand bad
Show NAND Flash Bad Blocks:
Block  Address      Partition
1020   0x07f80000   unused
1021   0x07fa0000   unused
1022   0x07fc0000   unused
1023   0x07fe0000   unused
```

Telnet Command: apm enable / disable / show /clear/discover/query

The apm command(s) is use to display, remove, discover or query the information of VigorAP registered to Vigor2133.

Syntax

apm enable
apm disable
apm show
apm clear
apm discover
apm query

Syntax Description

Parameter	Description
<i>enable</i>	Enable the APM function.
<i>disable</i>	Disable the 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 Vigor2133. Information related to the registered AP will be send back to Vigor2133 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 Vigor2133.
<i>clear</i>	It means to remove the information related to VigorAP registered Vigor2133.

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>	<p>You need to type 10 numbers in this field. Each number represents different setting value.</p> <p>[1] - The first number means the load balance function. 1 - enable load balance, 0 - disable load balance.</p> <p>[2] - The second number means the station limit function. 1 -enable station limit, 0 - disable station limit.</p> <p>[3] - The third number means the traffic limit function. 1 - enable traffic limit, 0 - disable traffic limit.</p> <p>[4] - The forth number means the limit num of station. Available range is 3-64.</p> <p>[5] - The fifth number means the upload limit function. 1 - enable upload limit, 0 - disable upload limit.</p> <p>[6] - The sixth number means the download limit function. 1 - enable download limit, 0 - disable download limit.</p> <p>[7] - The seventh number means disassociation by idle time. 1 - enable disassociation, 0 - disable disassociation.</p> <p>[8] - The eighth number means to enable or disable disassociation by signal strength. 1 - enable disassociation, 0 - disable disassociation.</p> <p>[9] - The ninth number means to determine the unit of traffic limit (for upload) 1 - Mbps 0 - kbps</p> <p>[10] - The tenth number means to determine the unit of traffic limit (for download) 1 - Mbps 0 - kbps</p> <p>[11]Enter RSSI threshold (-200 ~ -50 dbm)</p>

Example

```
> apm lbcfg set 1 1 1 32 100 200 1 1 1 0 -200
> apm lbcfg show
apm LoadBalance Config :
1. Enable LoadBalance : 1
```

```

2. Enable station limit : 1
3. Enable traffic limit : 1
4. Limit Number : 32
5. Upload limit : 100
6. Download limit : 200
7. Enable disassociation by idle time : 1
8. Enable disassociation by Signal strength : 1
9. Traffic limit unit (upload) : 1
10. Traffic limit unit (download) : 0
11. RSSI threshold : -200
flag : 31

```

Telnet Command: apm apsyslog

This command is used to display the AP syslog data coming from VigorAP.

Syntax

apm apsyslog [*AP_Index*]

Syntax Description

Parameter	Description
<i>AP_Index</i>	Specify the index number which represents VigorAP.

Example

```

> apm apsyslog 1
8d 02:46:09 syslog: [APM] Send Rogue AP Detection data.
8d 02:53:04 syslog: [APM] Run AP Detection / Discovery.
8d 02:56:09 syslog: [APM] Send Rogue AP Detection data.
8d 03:00:42 kernel: 60:fa:cd:55:f5:ea had disassociated.
8d 03:03:12 syslog: [APM] Run AP Detection / Discovery.
8d 03:06:09 syslog: [APM] Send Rogue AP Detection data.
8d 03:13:21 syslog: [APM] Run AP Detection / Discovery.
8d 03:16:10 syslog: [APM] Send Rogue AP Detection data.
8d 03:16:41 kernel: 60:fa:cd:55:f5:ea had associated successfully
8d 03:16:55 kernel: 60:fa:cd:55:f5:ea had disassociated.

```

Telnet Command: apm syslog

This command is used to display related syslog data from central AP management.

Syntax

apm syslog

Example

```

> apm syslog
"2015-11-04 12:24:21", "[APM] [VigorAP900_01daa902080] Get Rogue AP Detection
Data from AP"
2015-11-04 12:24:56", "[APM] [VigorAP900_01daa902080] Get Rogue AP Detection
Data from AP Success"
2015-11-04 12:34:21", "[APM] [VigorAP900_01daa902080] Get Rogue AP Detection
Data from AP"
2015-11-04 12:34:57", "[APM] [VigorAP900_01daa902080] Get Rogue AP Detection
Data from AP Success"

```

Telnet Command: apm stanum

This command is used to display the total number of the wireless clients, no matter what mode of wireless connection (2.4G WLAN or 5G WLAN) used by wireless clients to access into Internet through VigorAP.

Syntax

apm stanum [AP_Index]

Syntax Description

Parameter	Description
AP_Index	Specify the index number which represents VigorAP.

Example

```
> apm stanum

% Show the APM AP Station Number data.
% apm stanum AP_Index.
%   ex : apm stanum 1
%       Idx  Nearby(2.4/5G)  Conn(2.4/5G)
%       1    2    5           0    0
%       2    2    5           1    0
%       3    2    5           1    0
```

Telnet Command: backupmode

This command is used to backup the firmware to the router. The firmware will be retrieved for rebooting Vigor router after it crashes over three times.

Syntax

backupmode [<command><parameter>|...]

Syntax Description

Parameter	Description
[<command><parameter> ...]]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-t n	Set the backup time. n : 1 ~ 168 hours
-m n	Set the firmware backup mode. 1: Backup after timeout. 0: Backup after upgrade.
-b	Backup the firmware manually and immediately.

Example

```
> backupmode -b
Do Firmware backup now!!!.
```

Index

6

- 6rd Mode, 62
- 6rd Prefix, 63
- 6rd Prefix Length, 63

8

- 802.1x ports, 97

A

- Accelerate heaviest traffic sessions, 102
- Access Control, 167
- Access Mode, 43
- Access Mode - Ethernet, 43
- Activation, 325
- Active Mode, 41
- Address Mapping, 141, 153
- Administrator Password, 301
- Advance Mode, 248
- Advanced Setting, 175
- Aggregation MSDU, 175
- AH, 204
- Airtime Fairness, 179
- Always On, 47, 52, 54, 55, 56, 57, 59, 60, 63
- AP Discovery, 178
- AP Maintenance, 371, 379
- AP Map, 371
- APP Enforcement, 245
- APP Enforcement Filter, 266
- APP Enforcement Profile, 267
- APP QoS, 339
- Applications, 118
- Applied Interfaces, 100
- Apply the Class Rule, 102
- APSD Capable, 176
- ARP Cache Table, 431
- ARP Detect, 45, 47
- ARP Table, 95
- Auth Type, 122

- Authentication Mode, 171
- Auto Logout, 15
- Auto ULA Prefix, 87
- Auto-Update interval, 120
- Aux. WAN IP, 112

B

- Backup, 95
- Backup MX, 122
- Band Steering, 181
- Bandwidth Limit, 327, 331
- Bind IP to MAC, 94
- Bind to WAN, 222
- Bridge mode, 65
- Bridge Mode, 58, 60
- Bridge Subnet, 60

C

- Cache, 276
- Call Direction, 206
- Call Filter, 240
- Certificate Backup, 237
- Certificate Management, 230
- Change the TTL value, 48
- Channel, 64, 160, 163
- Channel Bandwidth, 175
- Choose IP, 110
- Codepage, 245
- Comment, 95, 112
- Config Backup, 21
- Configuration Backup, 308
- Configure via Client PinCode, 171
- Configure via Push Button, 171
- Connection Management, 215
- Connection Type, 122
- Connectivity, 39
- Country Code, 176
- CSM, 266
- CSV file, 388, 390

Current System Time, 127

D

Dashboard, 17
Data Filter, 240
Data Flow Monitor, 437
Data Quota, 352
DataType, 43, 79
Daylight Saving, 315
Days in a week, 128
Default Lifetime, 88
Default MAC Address, 46, 48
Default Preference, 88
Default Rule, 244
Destination IP, 148
Destination Port, 130
Details - PPPoE, 44
Details Page, 43
Details-IP Routed Subnet, 84
Details-IPv6-6in4 Static Tunnel, 60
Details-IPv6-6rd, 62
Details-Ipv6-AICCU, 54
Details-IPv6-DHCPv6 Client, 57
Details-IPv6-Offline, 52
Details-IPv6-PPP, 52
Details-IPv6-Static IPv6, 58
Details-IPv6-TSPC, 53
Details-LAN-DMZ, 82
Details-LAN-Ethernet, 80
Details-PPTP/L2TP, 50
Details-Static IP or Dynamic IP, 46
Determine Real WAN IP, 122
DHCP, 31
DHCP Client Identifier, 48
DHCP Server Configuration, 80, 82, 84
DHCP Server IP Address, 80, 82
DHCP Table, 433
DHCPv6 (Stateful), 86
DHCPv6 Server, 87
Diagnostics, 428, 429
Dial-out Triggering, 429
Digital Signature, 190, 204
Display Name, 42, 43

DMZ Host, 109
DNS Cache Table, 435
DNS Filter, 245
DNS Filter Profile, 279
DNS Server IP Address, 49, 81, 83
DNS Server IPv6 Address, 87
Domain Name, 48
DoS Defense, 241, 258
DoS Flood Table, 443
DrayTek Banner, 256
Dynamic DNS, 118, 120
Dynamic DNS Account, 121

E

Each /Shared, 331
Enable PING to keep alive, 47
End IPv6 Address, 87
End Port, 113
ESP, 204
Event Code, 299
Extension WAN, 88
External Devices, 383

F

Failover to/Failback, 141
File Explorer, 418
File Extension Object, 401
Filter Setup, 247
Firewall, 240
Firmware Upgrade, 324
Fixed IP, 46, 51
Force NAT /Force Routing, 149
Force Update, 120
Function Support List, 382

G

Gateway IP Address, 48, 80, 82
General Mode, 215
General Setup, 41
Get Community, 316
Green Field, 175
Group ID, 133

Guard Interval, 175
GUI Map, 20

H

Hardware Acceleration, 101
Hardware Installation, 5
Hide SSID, 163
Host Name, 32

I

Idle Timeout, 46, 203
IGMP, 132
IGMP Proxy, 132
IGMP Snooping, 132
IKE Authentication Method, 210
IM, 268
Incoming Port, 116
Incoming Protocol, 116
Indicators and Connectors, 2
Installation, i
Inter-LAN Routing, 79
Internet Access, 43
Internet Access - Advanced, 43
IP (Internet Protocol), 40
IP Address, 48, 51, 80, 82
IP Address Assignment Method (IPCP), 46
IP Address Assignment Method(IPCP), 51
IP Address List, 124
IP Bind List, 95
IP Filters, 240
IP Object, 387
IP Pool Counts, 80, 82, 84
IP Routed Subnet, 331
IPsec General Setup, 199
IPsec Tunnel, 203
IPTV, 67
IPv4 Border Relay, 62
IPv4 Mask Length, 63
IPv6 Address, 59
IPv6 Gateway Address, 59
IPv6 Group, 393
IPv6 Neighbour Table, 432

IPv6 Object, 391
IPv6 TSPC Status, 442
Isolate, 163
ISP Access Setup, 45, 50

K

keep alive, 206
Keep Alive Period, 300
Keep WAN Connection, 47
Keyword Group, 400
Keyword Object, 398

L

LAN, 76
LAN DNS / DNS Forwarding, 118, 123
LAN- General Setup, 78
LAN Port Mirror, 96
LAN Routed Prefix, 60
LAN to LAN, 205
Landing Page, 348, 352
Lease Time, 80, 82, 84
Line Speed, 41
Load Balance, 381
Load Balance for AP, 371
Load-Balance /Route Policy, 147
Local Certificate, 190, 231
Local ID, 204
Local IP Address, 112
Log, 273
Login, 37
Login Name, 122
Login Page Greeting, 306
Login Page Logo, 348
Logout, 22

M

Mail Alert, 136
Mail Extender, 122
Mail Service, 136
Main Screen, 15
Management, 295, 318
Manually ULA Prefix, 87

Max User Login, 350
Min/Max Interval Time, 88
Mirror Port, 96
Mode, 159, 166
Modem Code Upgrade, 324
mOTP, 203, 224
MPPE, 197
MTU, 45, 48, 50, 88
Multicast via VPN, 203, 224
Multiple SSID, 156
Multi-VLAN, 64
MyVigor, 34, 275

N

Name Link, 18
NAT, 104
NAT Sessions Table, 434
NAT Traversal, 131
NetBios Name Service, 416
Netbios Naming Packet, 203
Network Configuration, 80, 82, 84
Network Interface, 146
Next Server IP Address/SIAddr, 79
Notification Object, 408
NS Detect, 57

O

Objects Settings, 386
Online Statistics, 334
Open Ports, 112
Operation Mode, 175
Option Number, 43, 79
Override user management, 100

P

P2P, 269
PAP, 197
Password, 45, 48, 50, 54, 55
Password Strength, 166, 303
Path MTU Discovery, 45, 48, 50
Peer ID, 195
Physical Connection, 22

Physical Members, 65
Physical Mode, 41, 42, 43
Physical Type, 41, 42
PIN Code, 224
Ping Detect, 45, 47, 52, 54, 56, 57, 59, 60, 63
Ping Diagnosis, 436
Ping Gateway IP, 45, 47
Ping Interval, 45, 47
PING Interval, 47
Ping IP/Hostname, 52, 54, 56, 57, 59, 60, 63
Ping Retry, 45, 47
Policy, 351
Port Redirection, 105
Port Triggering, 115, 116
Port-based Bridge, 64
Port-Based VLAN, 90
PPP Authentication, 46, 51
PPP General Setup, 197
PPP Setup, 51
PPP/MP Setup, 46
PPPoE, 26
PPTP, 203
PPTP/L2TP, 28
Prefer user management, 100
Prefix Len, 145
Prefix Length, 59
Pre-shared Key, 173
Pre-Shared Key (PSK), 166
Primary DNS Sever, 87
Primary IP Address, 81, 83
Primary/Secondary Ping IP, 45, 47
Printer Server, 416
Priority, 42, 65, 91, 141
Private IP, 107
Private IP Address, 40
Private Port, 107
Production Registration, 37
Protocol, 269
Protocol Processing Engine (PPE), 101
Provider Host, 121
Psec Peer Identity, 200
Public IP Addresss, 40
Public Port, 107

Q

Quality of Service, 327, 333
Quick Access, 19
Quick Start Wizard, 25

R

RADIUS/TACACS+, 118, 129
Rate Control, 77, 161, 164
Reboot System, 323
Recipient, 135
Registering Vigor Router, 37
Relay Agent, 80, 82
Remote Access Control, 196
Remote Dial-in User, 202
Remote Endpoint IPv4 Address, 60
Repeater, 173
Restore, 95
RIP Protocol, 48
RIPng Protocol, 53, 88
Root CA, 235
Route Policy, 141
Router Advertisement Configuration, 88
Router Name, 48, 312
Routing, 141
Routing Information Protocol, 77
Routing Table, 429
RTS Threshold, 176
Rule-Based, 347

S

Scan, 178
Schedule, 118, 127, 164
Secondary DNS Server, 87
Secondary IP Address, 81, 83
Security, 165, 239
Security Key, 160
Self-signed, 222
Self-Signed Certificate, 321
Sensor, 420
Server Address, 50
Server Certificate, 222
Server IP Address, 130

Server Response, 122
Service, 116
Service Activation Wizard, 34
Service API, 121
Service Name, 107
Service Provider, 121, 404
Service Type Group, 396
Service Type Object, 394
Sessions Control, 244
Sessions Limit, 327, 329
Set Community, 316
Set to Factory Default, 120, 127, 142
Setup Query Server, 276
Shared Secret, 130
SLAAC(stateless), 86
Smart Bandwidth Limit, 332
SMB, 416, 417
SMB Client Support List, 422
SMS / Mail Alert Service, 135
SMS Alert, 135
SMS Provider, 135
SMS/Mail Service Object, 403
SNMP, 316
Source IP, 107, 113, 116, 148
Specific Hosts, 102
Specify Remote Node, 203
SPI, 241
SSID, 160
SSL Tunnel, 203
SSL VPN, 221
Start IP Address, 80, 82, 84
Start IPv6 Address, 87
Start Port, 113
Static IP, 30
Static Route, 77, 142
Static Route for IPv6, 145
Station Control, 177
Station List, 157, 182
Stations (STA), 156
Status, 372
Strict Bind, 95
Strict Security Checking, 256
Strict Security Firewall, 243

STUN Settings, 300
Subnet, 91
Subnet Mask, 48, 51, 80, 82
Subnet Prefix, 55
Syslog Alarm, 421
Syslog Explorer, 441
Syslog/Mail Alert, 312
System Maintenance, 296
System Status, 297
System time set, 127

T

Tag value, 42
Tagged VLAN, 90
Temperature Sensor, 420
Time and Date, 315
Time Quota, 352
Time Schedule, 332
Time Server, 315
Time Zone, 315
TR-069, 299
Trace Route, 440
Traceable, 340
Traffic Graph, 380, 439
Trap Community, 317
Triggering Port, 116
Triggering Protocol, 116
Troubleshooting, 427
Trusted CA, 236
Trusted CA Certificate, 235
TSPC, 53
TTL (Time to Live), 45, 47, 52, 54, 56, 57, 59, 60, 63
Tunnel Broker, 54, 55
Tunnel ID, 55
Tunnel TTL, 60
TX Power, 175

U

Unique Local Address (ULA) configuration, 87
UPnP, 118, 131
URL Access Control, 273
URL Content Filter, 245, 266

URL Content Filter Profile, 271
URL Redirect, 99
USB Application, 414
USB Device Status, 419
USB General Settings, 415
USB User Management, 416
User Account, 223
User Group, 227, 354
User Management, 346
User Online Status, 355
User Password, 303
User Profile, 349
User-Based, 347
Username, 45, 48, 50, 54, 55

V

VID, 91
Virtual LAN, 77
Virtual Panel, 18
Virtual WAN, 24
VLAN, 90
VLAN Applications, 456
VLAN Configuration, 92
VLAN Tag, 64, 65, 91
VLAN Tag insertion, 42
VPN, 184
VPN and Remote Access, 185
VPN Client Wizard, 187
VPN Server Wizard, 192

W

Wake by IP Address, 134
Wake on LAN, 118, 134
WAN, 40
WAN Connection Detection, 45, 47, 52, 54, 56, 57, 59, 60, 63
WAN Inbound Bandwidth, 335
WAN Interface, 107, 112
WAN IP Alias, 46, 48, 51
WAN IP Network Settings, 48, 51
WAN Outbound Bandwidth, 335
WAN Setup, 67
WAN Type, 64

WDS, 172
Web Console, 21
Web Content Filter, 245, 266
Web Content Filter Profile, 275
Web Feature, 274
Web Portal Setup, 98, 177
WEP, 157, 166
white/black list, 167
Wildcard, 122
Wired 802.1x, 97
Wireless LAN, 155
Wireless Wizard, 159
Wizard Mode, 248
WLAN Isolation, 157
WLAN Profile, 374
WMM Capable, 175
WPA, 157, 166
WPS, 158, 168