

DrayTek

Vigor160 Series

35b/G.Fast Modem



USER'S GUIDE

V1.0

Vigor160 Series 35b/G.Fast Modem User's Guide (Applicable for Vigor165)

Version: 1.0

Firmware Version: **V4.0.2**

(For future update, please visit DrayTek web site)

Date: January 23, 2019

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	3
I-2-1 Installing Vigor Router	3
I-2-2 Wall-Mounted Installation	4
I-3 Accessing Web Page	5
I-4 Changing Password.....	7
I-5 Dashboard.....	8
I-5-1 Virtual Panel	8
I-5-2 Name with a Link.....	9
I-5-3 Quick Access for Common Used Menu	9
I-5-4 GUI Map	10
I-5-5 Web Console	10
I-5-6 Config Backup	11
I-5-7 Logout.....	11
I-5-8 Online Status	11
I-5-8-1 Physical Connection	11
I-5-8-2 Virtual WAN	13
I-6 Quick Start Wizard	14
I-7 Registering Vigor Device.....	19
Part II Connectivity	21
II-1 Internet Access.....	22
Web User Interface	23
II-1-1 General Setup	23
II-1-2 PPPoE/PPPoA	25
II-1-3 MPoA /Static or dynamic IP.....	27
II-1-4 IPv6.....	31
II-1-4-1 Details Page for IPv6 - Offline	31
II-1-4-2 Details Page for IPv6 - PPP	31
II-1-4-3 Details Page for IPv6 - TSPC.....	32
II-1-4-4 Details Page for IPv6 - AICCU	34
II-1-4-5 Details Page for IPv6 - DHCPv6 Client	35
II-1-4-6 Details Page for IPv6 - Static IPv6.....	36
II-1-4-7 Details Page for IPv6 - 6in4 Static Tunnel	37
II-1-4-8 Details Page for IPv6 - 6rd.....	39
II-1-3 Multi-PVC/VLAN	41
II-2 LAN	48
Web User Interface	50
II-2-1 General Setup	50
II-2-1-1 Details Page for LAN1 - Ethernet TCP/IP and DHCP Setup	51
II-2-1-2 Details Page for LAN1 - IPv6 Setup.....	54

II-2-2 Bind IP to MAC	59
II-3 NAT	61
Web User Interface	62
II-3-1 Port Redirection	62
II-3-2 DMZ Host	66
II-3-3 Open Ports	69
II-3-4 ALG.....	71
II-4 Applications	72
Web User Interface	73
II-4-1 Dynamic DNS	73
II-4-2 Schedule.....	76
II-4-3 UPnP	79
II-4-4 IGMP.....	80
<i>II-4-4-1 General Setting</i>	<i>80</i>
<i>II-4-4-2 Working Status</i>	<i>81</i>
Application Notes	82
<i>A-1 How to use DrayDDNS?</i>	<i>82</i>
<i>A-2 How to Configure Customized DDNS?.....</i>	<i>87</i>
II-5 Routing.....	91
Web User Interface	92
II-5-1 Static Route	92
Part III Security.....	97
III-1 Firewall.....	98
Web User Interface	100
III-1-1 General Setup	100
III-1-2 Filter Setup	104
III-1-3 Defense Setup.....	113
<i>III-1-3-1 DoS Defense</i>	<i>113</i>
<i>III-1-3-2 Spoofing Defense</i>	<i>116</i>
Application Notes	117
<i>A-1 How to Configure Certain Computers Accessing to Internet</i>	<i>117</i>
III-2 Central Security Management (CSM).....	121
Web User Interface	122
III-2-1 URL Content Filter Profile	122
Application Notes	126
<i>A-1 How to Create an Account for MyVigor</i>	<i>126</i>
Part IV Management	131
IV-1 System Maintenance	132
Web User Interface	133
VI-1-1 System Status.....	133
IV-1-2 TR-069	135

IV-1-3 Administrator Password	137
IV-1-4 Configuration Backup.....	138
IV-1-5 Syslog/Mail Alert	141
IV-1-6 Time and Date.....	144
IV-1-7 Management	145
IV-1-8 Self-Signed Certificate	148
IV-1-9 Panel Control	150
IV-1-10 Reboot System.....	151
IV-1-11 Firmware Upgrade	152
Part V Others.....	153
V-1 Objects Settings.....	154
Web User Interface	155
V-1-1 IP Object	155
V-1-2 IP Group.....	158
V-1-3 IPv6 Object.....	159
V-1-4 IPv6 Group	161
V-1-5 Service Type Object.....	162
V-1-6 Service Type Group	164
V-1-7 Keyword Object.....	166
V-1-8 Keyword Group	168
V-1-9 File Extension Object	169
V-1-10 Objects Backup/Restore	171
Part VI Troubleshooting	173
VI-1 Diagnostics	174
Web User Interface	175
VI-1-1 Dial-out Triggering.....	175
VI-1-2 Routing Table.....	176
VI-1-3 ARP Cache Table	177
VI-1-4 IPv6 Neighbour Table	178
VI-1-5 DHCP Table	179
VI-1-6 NAT Sessions Table	180
VI-1-7 DNS Cache Table	181
VI-1-8 Ping Diagnosis	182
VI-1-9 Data Flow Monitor	183
VI-1-10 Trace Route	185
VI-1-11 IPv6 TSPC Status	186
VI-1-12 DSL Status	186
VI-1-13 DoS Flood Table	187
VI-2 Checking If the Hardware Status Is OK or Not	188
VI-3 Checking If the Network Connection Settings on Your Computer Is OK or Not.....	189

VI-4 Pinging the Router from Your Computer	192
VI-5 Checking If the ISP Settings are OK or Not.....	194
VI-6 Backing to Factory Default Setting If Necessary	195
VI-7 Contacting DrayTek	196
Part IX Telnet Commands.....	197
Accessing Telnet of Vigor Device	198
Index	353

Part I Installation



Installation

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

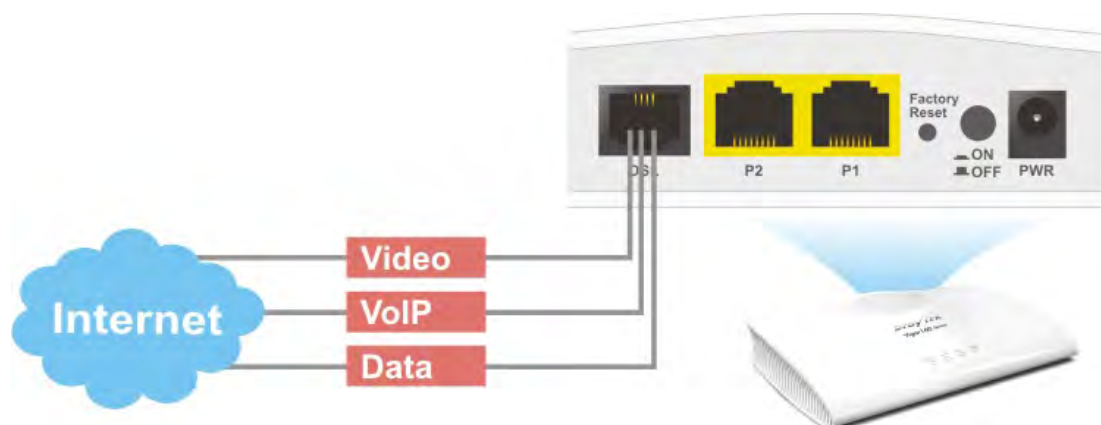
I-1 Introduction

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.

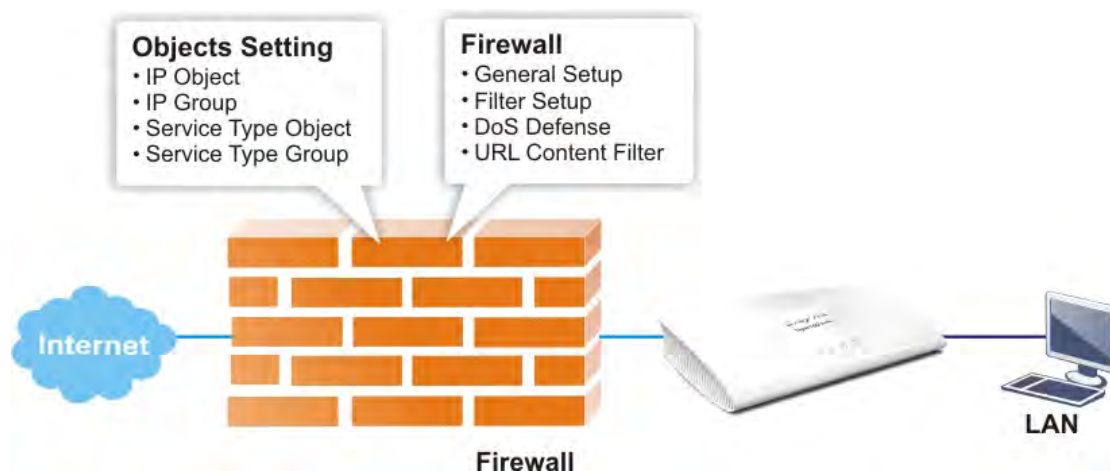
Vigor160 series (family member including Vigor165) is a 35b/G.Fast Modem. As the following figure shown, Vigor160 series supports triple play application like Video, VoIP and Data via the Internet.

Triple Play

VDSL2 and ADSL2+ Fall-back



The object-based design used in SPI (Stateful Packet Inspection) firewall allows users to set firewall policy with ease. It is flexible and makes your network be safe. By the way, DoS prevention and URL content filter strengthen the security outside and control inside.

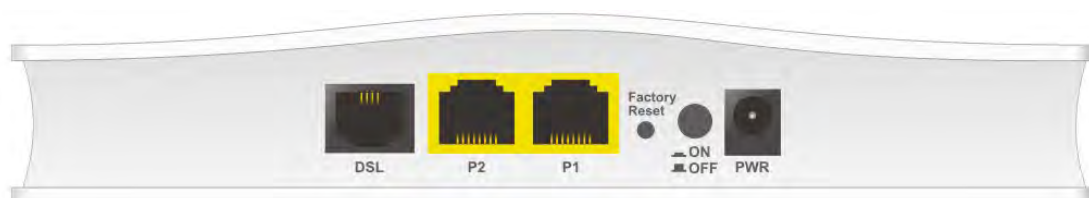




I-1-1 Indicators and Connectors

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



LED	Status	Explanation
ACT	Off	The system is not ready or is failed.
	Blinking	The system is ready and can work normally.
P1/P2	On	A normal connection is through its corresponding port.
	Off	LAN is disconnected.
	Blinking	Data is transmitting (sending/receiving).
DSL	On	DSL connection synchronized.
	Blinking	DSL connection is synchronizing.



Interface	Description
DSL	Connector for accessing the Internet through VDSL2/ADSL2/2+.
P2-P1	Connector for local networked devices.
Factory Reset	Restore the default settings. Usage: Turn on the modem. Press the button and keep for more than 10 seconds. Then the modem will restart with the factory default configuration.
	ON/OFF: Power switch.
	Connector for a power adapter.

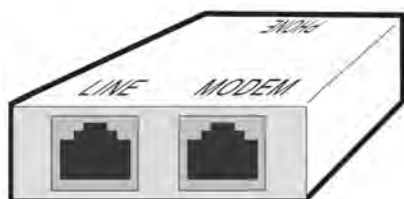
I-2 Hardware Installation

I-2-1 Installing Vigor Router

This section will guide you to install the modem through hardware connection and configure the modem's settings through web browser.

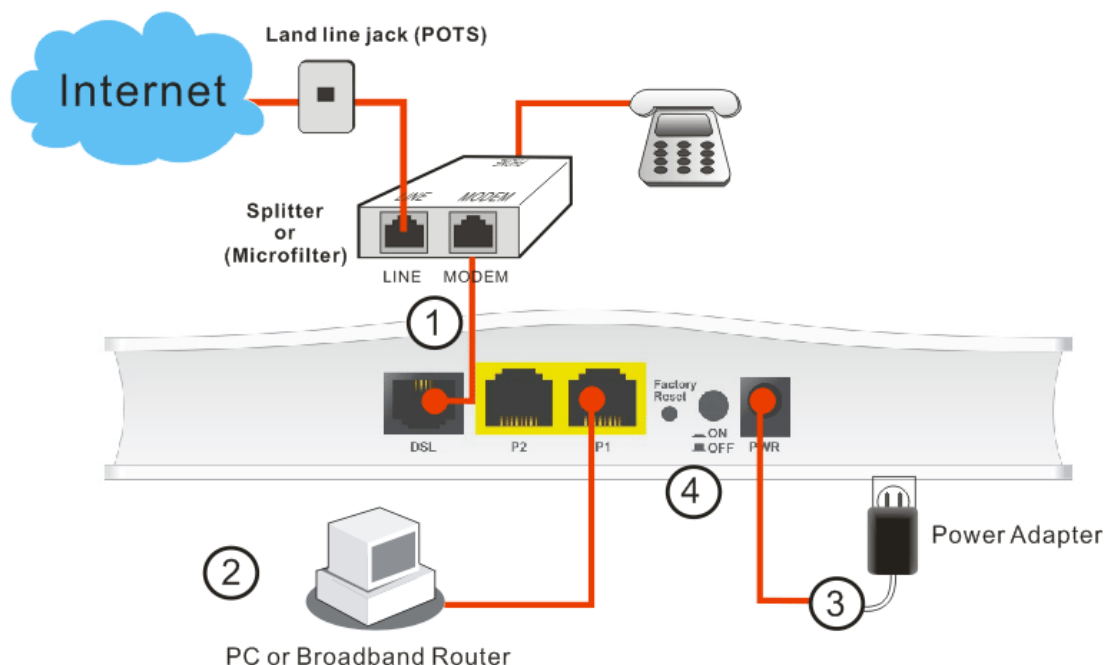
Before starting to configure the modem, you have to connect your devices correctly.

1. Connect the DSL interface to the MODEM port of external splitter with a DSL line cable.



(splitter)

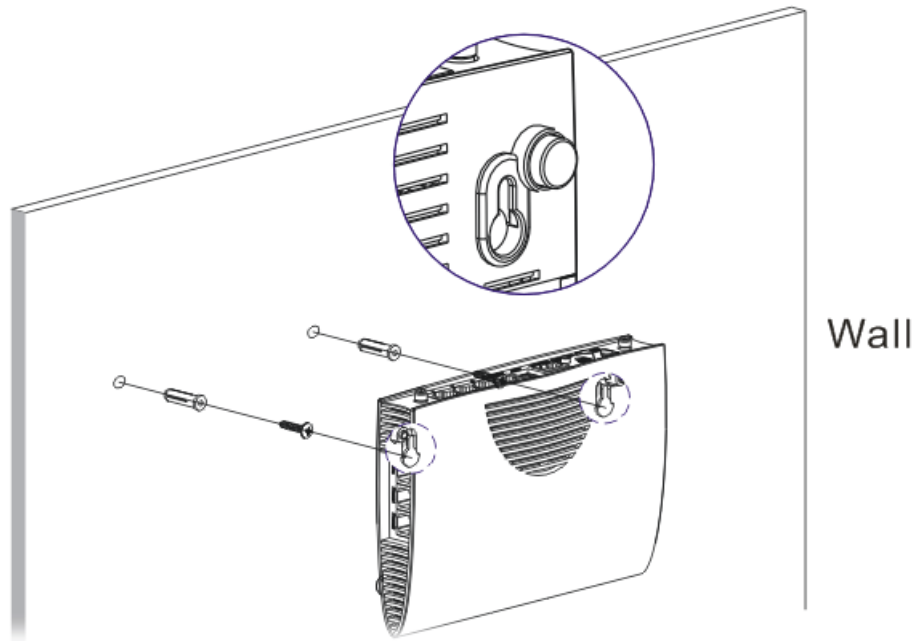
2. Connect the LAN port to your computer with a RJ-45 cable.
3. Connect one end of the power adapter to the Power port of this device. Connect the other end to the wall outlet of electricity.
4. Power on the modem.
5. Check the POWER, ACT, LAN, DSL and INTERNET LEDs to assure network connections.



I-2-2 Wall-Mounted Installation

Vigor160 series has keyhole type mounting slots on the underside.

1. A template is provided on the Vigor160 series 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-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. Take Vigor165 as an example.

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



Info

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

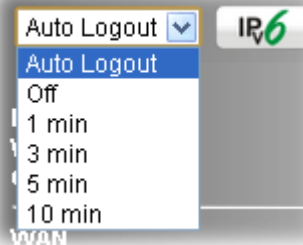
4. Now, the Main Screen will appear.



Info

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

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



I-4 Changing Password

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

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

System Maintenance >> Administrator Password Setup

Administrator Password

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

☐ Enable 'admin' account login to Web UI from the Internet

Note:

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

OK

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 83 characters.

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

The image shows the login interface of a DrayTek Vigor165 router. At the top, there is a red banner with the DrayTek logo on the left and 'Vigor165' on the right. Below the banner, the word 'Login' is displayed in a black box. The main area contains two input fields: 'Username' with the text 'admin' and 'Password' with five dots. A 'Login' button is positioned below the password field. At the bottom, a security warning states: 'Security Warning: You are logging in without encryption which is not recommended. To login securely click here.' with a blue link. The footer text reads: 'Copyright © 2000- 2019 DrayTek Corp. All Rights Reserved.'



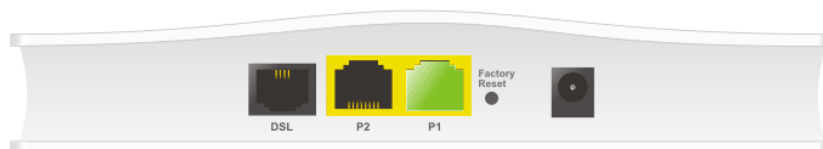
Info

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

I-5 Dashboard

The Dashboard (home page) shows the connection status including System Information, IPv4 Internet Access, Interface (physical connection) and Quick Access.

Dashboard



System Information

Model Name	Vigor165	System Up Time	3:7:52
Router Name	DrayTek	Current Time	2000 Jan 1 Sat 3:7:42
Firmware Version	4.0.2_STD	Build Date/Time	Jan 21 2019 11:27:27
DSL Version	8B2607_A/B/C HW: B	LAN MAC Address	00-1D-AA-93-7F-B4

Quick Access

System Status
Dynamic DNS
TR-069
Schedule
SysLog / Mail Alert
Firewall Object Setting

IPv4 Internet Access

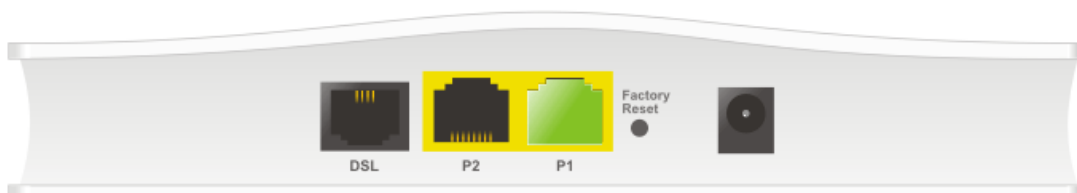
	Line / Mode	IP Address	MAC Address	Up Time
WAN1	VDSL / Static IP	Disconnected	00-1D-AA-93-7F-B5	00:00:00

Interface

DSL	Connected : Down Stream : 0Kbps / Up Stream : 0Kbps
WAN	Connected : 0, WAN1
LAN	Connected : 0, Port1 Port2

I-5-1 Virtual Panel

On the top of the Dashboard, a virtual panel (simulating the physical panel of the modem) displays the physical interface connection. It will be refreshed every five seconds.







Port	Color Displayed	Explanation
LED	Black	It means the modem or the function is not working.
	Green	It means the modem or the function is working.

I-5-2 Name with a Link

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

System Information			
Model Name	Vigor165	System Up Time	3:7:52
Router Name	DrayTek	Current Time	2000 Jan 1 Sat 3:7:42
Firmware Version	4.0.2_STD	Build Date/Time	Jan 21 2019 11:27:27
DSL Version	8B2607_A/B/C HW: B	LAN MAC Address	00-1D-AA-93-7F-B4

IPv4 Internet Access				
	Line / Mode	IP Address	MAC Address	Up Time
WAN1	VDSL / Static IP	Disconnected	00-1D-AA-93-7F-B5	00:00:00

Interface	
DSL	Connected : Down Stream : 0Kbps / Up Stream : 0Kbps
WAN	Connected : 0,  WAN1
 LAN	Connected : 0,  Port1  Port2


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
Schedule
SysLog / Mail Alert
Firewall Object Setting

The function links of System Status, Dynamic DDNS, TR-069, Schedule, Syslog/Mail Alert, RADIUS, and Firewall Object Setting 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.

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

Interface			
DSL	Connected : Down Stream : 0Kbps / Up Stream : 0Kbps		
WAN	Connected : 0,  WAN1		
 LAN	Connected : 0,  Port1  Port2		
	Host ID	IP Address	MAC

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

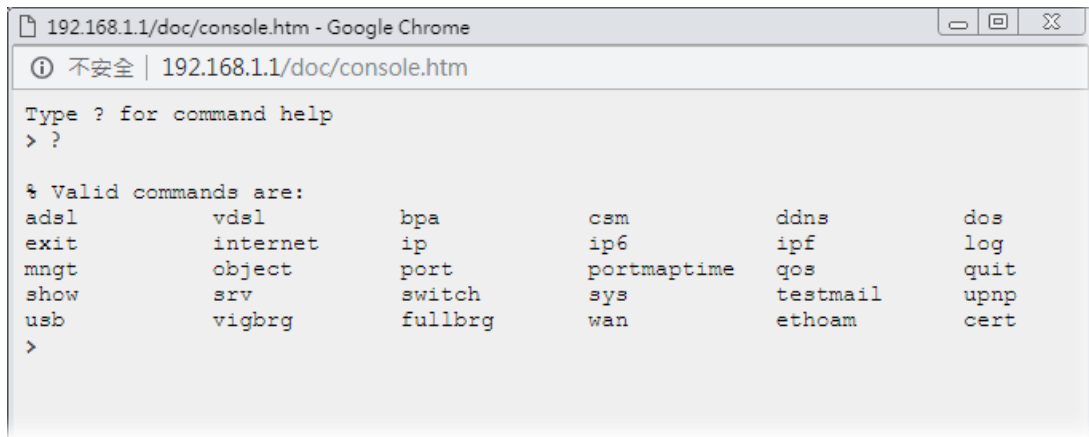
Wizards	Quick Start Wizard	Applications	Dynamic DNS
Online Status	Physical Connection		Schedule
	Virtual WAN		UPnP
Internet Access	General Setup	System Maintenance	IGMP
	PPPoE/PPPoA		System Status
	MPoA / Static or dynamic IP		TR-069
	IPv6		Administrator Password
LAN	Multi-PVC/LAN		Configuration Backup
	General Setup		SysLog / Mail Alert
Routing	Bind IP to MAC		Time and Date
	Static Route		Management
			Self-Signed Certificate
			Panel Control
			Reboot System

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



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: 19:14:0	
IPv4		IPv6			
LAN Status					
IP Address	TX Packets		RX Packets	Router Primary DNS:	Router Secondary DNS:
192.168.1.1	25775		8327	8.8.8.8	8.8.4.4
WAN Status					
Enable	Line	Name	Mode	Up Time	
Yes	VDSL2		PPPoE	00:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
---	---	0	0	0	0
>> Dial PPPoE					
VDSL2 Information (VDSL2 Firmware Version: 8B0F07_A/B/C)					
Profile	State	UP Speed	Down Speed	SNR Upstream	SNR Downstream
	TRAINING	0 (Kbps)	0 (Kbps)	0 (dB)	0 (dB)

Physical Connection for IPv6 Protocol

Online Status

Physical Connection		System Uptime: 0day 19:14:43	
IPv4		IPv6	
LAN Status			
IP Address			
FE80::BE80:75E6:EA9E:D7B6/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
304	0	23,712	0
WAN1 IPv6 Status			
Enable	Mode	Up Time	
No	Offline	---	
IP	Gateway IP		
---	---		

Detailed explanation (for IPv4) is shown below:

Item	Description
LAN Status	<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> <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>
WAN1 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>

Item	Description
	<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 entering the password, please click **Next**.

Quick Start Wizard

Enter login password

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

Old Password

New Password

Confirm Password

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

< Back

Next >

Finish

Cancel

PPPoE

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

Quick Start Wizard

Connect to Internet

WAN 1

Protocol: **PPPoE / PPPoA**

For ADSL Only:

Encapsulation: **PPPoE LLC/SNAP**

VPI: **1** Auto detect

VCI: **32**

Fixed IP: ☒ Yes ☐ No(Dynamic IP)

IP Address: **0.0.0.0**

Subnet Mask: **0.0.0.0**

Default Gateway: **0.0.0.0**

Primary DNS: **8.8.8.8**

Second DNS: **8.8.4.4**

VLAN Tag insertion (**ADSL**): **Enable**

Tag value: **7** (0~4095)

Priority: **0** (0~7)

VLAN Tag insertion (**VDSL2**): **Disable**

Tag value: **0** (0~4095)

Priority: **0** (0~7)

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
For ADSL Only	<p>You have to select an appropriate WAN connection type for connecting to the Internet through this modem according to the settings that your ISP provided.</p> <p>Auto detect - Click it to detect suitable values below by the modem automatically.</p> <p>Encapsulation - Select an IP mode for this WAN interface. There are several available modes for Internet access such as PPPoE, PPPoA.</p> <p>VPI - Stands for Virtual Path Identifier. It is an 8-bit header inside each ATM cell that indicates where the cell should be routed. The ATM, is a method of sending data in small packets of fixed sizes. It is used for transferring data to client computers.</p> <p>VCI - Stands for Virtual Channel Identifier. It is a 16-bit field inside ATM cell's header that indicates the cell's next destination as it travels through the network. A virtual channel is a logical connection between two end devices on the network.</p>
Fixed IP	<p>Click Yes to specify a fixed IP for the modem. Otherwise, click No (Dynamic IP) to allow the modem choosing a dynamic IP. If you choose No, the following IP Address, Subnet Mask and Default Gateway will not be changed.</p>

IP Address	Assign an IP address for the protocol that you select.
Subnet Mask	Assign a subnet mask value for the protocol of MPoA/Static or Dynamic IP.
Default Gateway	Assign an IP address to the gateway for the protocol of MPoA/Static or Dynamic IP.
Primary DNS	Assign an IP address to the primary DNS.
Second DNS	Assign an IP address to the secondary DNS.
VLAN Tag insertion (VDSL2)/(ADSL)	<p>The settings configured in this field are available for WAN1 and WAN2.</p> <p>Enable - Enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the WAN while sending them out. Please type the tag value and specify the priority for the packets sending by WAN1.</p> <p>Disable - Disable the function of VLAN with tag.</p> <p>Tag value - Type the value as the VLAN ID number. The range is from 0 to 4095.</p> <p>Priority - Type the packet priority number for such VLAN. The range is from 0 to 7.</p>
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

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

Quick Start Wizard

Set PPPoE / PPPoA

WAN 1	
Service Name (Optional)	<input type="text" value="service"/>
Username	<input type="text" value="84005756@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.
User Name	Type in the valid user name (maximum 63 characters) provided by the ISP in this field.
Password	Type a valid password provided by the ISP.

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

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

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN1
Physical Mode:	undefined
VPI:	1
VCI:	32
Protocol / Encapsulation:	PPPoE / LLC
Fixed IP:	Yes
IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Default Gateway:	0.0.0.0
Primary DNS:	8.8.8.8
Secondary DNS:	8.8.4.4

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

Quick Start Wizard Setup OK!

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

MPoA / Static or Dynamic IP

1. Choose **WAN1** as WAN Interface and click the **Next** button; you will get the following page. Choose **MPoA / Static or Dynamic IP** as the protocol.

Quick Start Wizard

Connect to Internet

WAN 1	
Protocol	MPoA / Static or Dynamic IP ▼
For ADSL Only:	
Encapsulation	1483 Bridged IP LLC ▼
VPI	1 Auto detect
VCI	32
Fixed IP <input checked="" type="radio"/> Yes <input type="radio"/> No(Dynamic IP)	
IP Address	192.168.1.52
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.11
Primary DNS	8.8.8.8
Second DNS	8.8.4.4
VLAN Tag insertion (ADSL):	
Tag value	7 (0~4095)
Priority	0 (0~7)
VLAN Tag insertion (VDSL2):	
Tag value	0 (0~4095)
Priority	0 (0~7)

< Back Next > Finish Cancel

2. Please enter 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:	undefined
VPI:	1
VCI:	32
Protocol / Encapsulation:	1483 Bridge LLC
Fixed IP:	Yes
IP Address:	192.168.1.52
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.11
Primary DNS:	8.8.8.8
Secondary DNS:	8.8.4.4

< Back Next > Finish Cancel

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

Quick Start Wizard Setup OK!

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

I-7 Registering Vigor Device

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

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



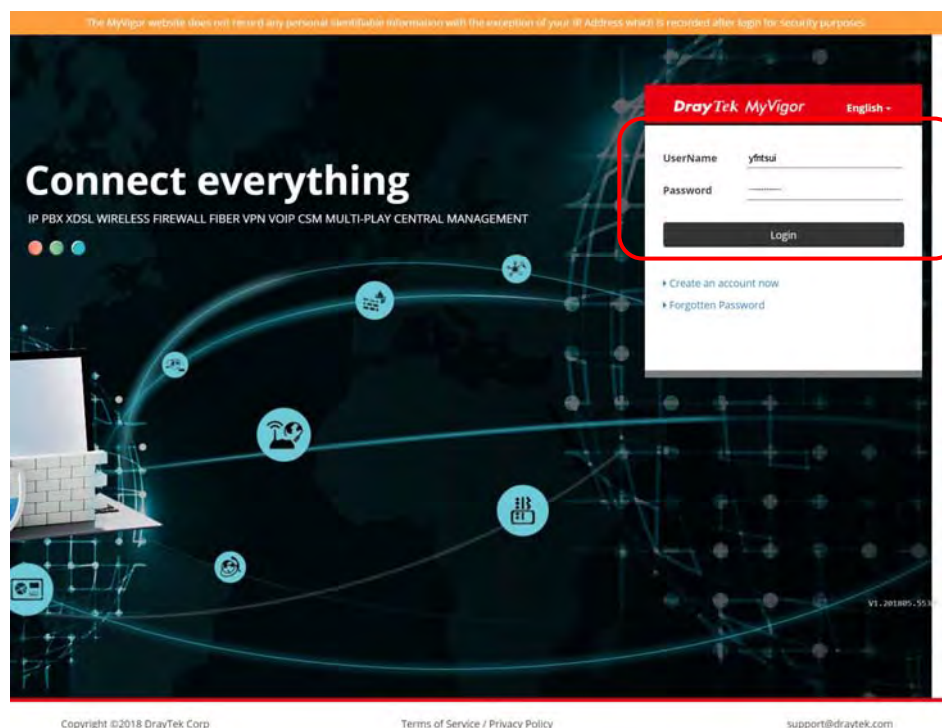
The image shows the login page for a DrayTek Vigor165 router. At the top, there is a red header with the "DrayTek" logo on the left and "Vigor165" on the right. Below the header, the word "Login" is displayed in a black box. The main area contains two input fields: "Username" with the text "admin" and "Password" with five dots. A "Login" button is positioned below the password field. A security warning message states: "Security Warning: You are logging in without encryption which is not recommended. To login securely [click here](#)." At the bottom, a copyright notice reads: "Copyright © 2000- 2019 DrayTek Corp. All Rights Reserved."

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



A rectangular button with a grey gradient background. The text "Support Area" is in a larger, bold font, and "Product Registration" is in a smaller font below it.

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



The image shows the DrayTek MyVigor website login page. The background is dark with a network diagram. On the right, there is a white login box with a red header containing "DrayTek MyVigor" and a language selector "English". Inside the box, there are input fields for "UserName" (containing "yftsu") and "Password". Below these is a "Login" button. Links for "Create an account now" and "Forgotten Password" are at the bottom of the box. A red rectangle highlights the login fields and button. At the top of the page, a small orange banner contains a disclaimer: "The MyVigor website does not intend any personal sensitive information with the exception of your IP Address which is recorded after login for security purposes." At the bottom of the page, there is a footer with "Copyright ©2018 DrayTek Corp.", "Terms of Service / Privacy Policy", and "support@draytek.com".



Info

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

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

DrayTek MyVigor

Login User : carrieni (Logout)

My Information - My Products

Registration Device :

Nickname :

Registration Date : 01-17-2017

Serial number : 2017011710270702

Last login time : 2018-09-12 13:53:29
Last login from : 111.251.222.175

Rows : 10 Page : 1

Serial Number / Host ID	Device Name	Model	Note
111900325027	2130	Vigor2130	
2013030811172502	vigor2760	Vigor2760	
2015022415571701	Vigor2132ac	Vigor2132	
2015030413341201	Vigor2925ac	Vigor2925	
APM-00055DE4D8EE	Carrie_APM	VigorAPM	

Copyrights © DrayTek Corp.

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

Your device has been successfully added to the database.



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

DrayTek MyVigor

Login User : carrieni (Logout)

My Information - My Products

Last login time : 2018-09-12 13:53:29
Last login from : 111.251.222.175

Rows : 10 Page : 1

Serial Number / Host ID	Device Name	Model	Note
111900325027	2130	Vigor2130	
2013030811172502	vigor2760	Vigor2760	
2015022415571701	Vigor2132ac	Vigor2132	
2015030413341201	Vigor2925ac	Vigor2925	
2017011710270702	Carrie_Vigor165	Vigor165	
APM-00055DE4D8EE	Carrie_APM	VigorAPM	

Copyrights © DrayTek Corp.

Part II Connectivity



WAN

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



LAN

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



NAT

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



Applications

DDNS, Schedule, UPnP, IGMP.



Routing

Static Route

II-1 Internet Access

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

Internet Access
General Setup
PPPoE / PPPoA
MPoA / Static or dynamic IP
IPv6
Multi-PVC/LAN
LAN

II-1-1 General Setup

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

Internet Access >> General Setup

WAN 1

Display Name:	<input type="text"/>		
Physical Mode:	ADSL		
DSL Mode:	ADSL only ▼		
DSL Modem Code:	Default ▼		
VLAN Tag insertion	Customer	Service	
ADSL	Enable ▼ Tag value 7 (0~4095) Priority 0 (0~7)		
VDSL2	Enable ▼ Tag value 7 (0~4095) Priority 0 (0~7)	Disable ▼ Tag value 0 (0~4095) Priority 0 (0~7)	

Note:

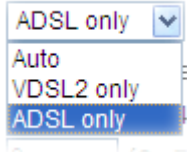
In DSL auto mode, the router will reboot automatically while switching between VDSL2 and ADSL lines.

OK

Cancel

Available settings are explained as follows:

Item	Description
Display Name	Type the description for such WAN interface.
Physical Mode	Display the physical mode of such WAN interface.
DSL Mode	Specify which DSL mode can be used for such WAN connection. Auto - The system will choose the suitable one automatically.

	
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 packets sending by WAN interface.</p> <p>Disable - Disable the function of VLAN with tag.</p> <p>Tag value - Type the value as the VLAN ID number. The range is from 0 to 4095.</p> <p>Priority - Type the packet priority number for such VLAN. The range is from 0 to 7.</p>

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

II-1-2 PPPoE/PPPoA

PPPoA, included in RFC1483, can be operated in either Logical Link Control-Subnetwork Access Protocol or VC-Mux mode. As a CPE device, Vigor modem encapsulates the PPP session based for transport across the ADSL loop and your ISP's Digital Subscriber Line Access Multiplexer (SDLAM).

To choose PPPoE or PPPoA as the accessing protocol of the internet, please select PPPoE/PPPoA from the **Internet Access** menu. The following web page will be shown.

Internet Access >> PPPoE / PPPoA

PPPoE / PPPoA Client Mode

PPPoE/PPPoA Client <input checked="" type="radio"/> Enable <input type="radio"/> Disable	
DSL Modem Settings (for ADSL mode only)	
Multi-PVC channel	Channel 1
VPI	0
VCI	33
Encapsulating Type	LLC/SNAP
Protocol	PPPoE
Modulation	Multimode
PPPoE Pass-through	
<input checked="" type="checkbox"/> For Wired LAN ²	
WAN Connection Detection	
Mode	ARP Detect
MTU 1492 (Max: 1500)	
ISP Access Setup	
Service Name ¹	
Username	
Password	
PPP Authentication	PAP or CHAP
IP Address From ISP	WAN IP Alias
Fixed IP	<input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP)
Fixed IP Address	
<input checked="" type="radio"/> Default MAC Address	
<input type="radio"/> Specify a MAC Address	
MAC Address: 00 . 1D . AA : 93 . 0C . 91	
Index(1-15) in Schedule Setup:	
=> , , ,	

Note:

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

OK

Available settings are explained as follows:

Item	Description
PPPoE/PPPoA Client	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.
DSL Modem Settings	Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP. Multi-PVC channel - The selections displayed here are determined by the page of Internet Access - Multi PVCs . VPI - Type in the value provided by ISP. VCI - Type in the value provided by ISP. Encapsulating Type - Drop down the list to choose the type provided by ISP. Protocol - Drop down the list to choose the protocol, PPPoE or PPPoA.

	Modulation - Choose a suitable method for PPPoE/PPoA connection.
PPPoE Pass-through	<p>The modem offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor modem. When PPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPoA 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>
WAN Connection Detection	<p>Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.</p> <p>Mode - Choose ARP Detect or Ping Detect for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items.</p> <ul style="list-style-type: none"> ● Primary/Secondary Ping IP - If you choose Ping Detect as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation. ● Ping Interval - Type the interval for the system to execute the PING operation. ● Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
MTU	It means Max Transmit Unit for packet. The default setting will be 1492.
ISP Access Setup	<p>Enter your allocated username, password and authentication parameters according to the information provided by your ISP.</p> <p>Service Name - 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>PPP Authentication - Select PAP only or PAP or CHAP for PPP.</p>
IP Address From ISP	<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</p>

would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.

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

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

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

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

Schedule

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 here, please click **OK** to activate them.

II-1-3 MPoA /Static or dynamic IP

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

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 **MPoA /Static or dynamic IP** as the accessing protocol of the Internet, select **MPoA** mode. The following web page will appear.

MPoA / Static or dynamic IP

MPoA (RFC1483/2684) <input checked="" type="radio"/> Enable <input type="radio"/> Disable	
DSL Modem Settings (for ADSL mode only) Multi-PVC channel Channel 2 ▼ Encapsulation 1483 Bridged IP LLC ▼ VPI 1 VCI 32 Modulation Multimode ▼	
WAN Connection Detection Mode ARP Detect ▼	
MTU 1500 (Max:1500)	
RIP Protocol <input type="checkbox"/> Enable RIP	
Bridge Mode <input checked="" type="checkbox"/> Enable Full Bridge Mode <input type="checkbox"/> Enable Bridge Mode	
WAN IP Network Settings <input type="radio"/> Obtain an IP address automatically Router Name Vigor * Domain Name * <input type="checkbox"/> DHCP Client Identifier * Username Password <input checked="" type="radio"/> Specify an IP address WAN IP Alias IP Address 0.0.0.0 Subnet Mask 0.0.0.0 Gateway IP Address 0.0.0.0 <input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: 00 · 1D · AA · 93 · 7F · B5 DNS Server IP Address Primary IP Address 8.8.8.8 Secondary IP Address 8.8.4.4	

Advanced You can configure DHCP client options here.

*: Required for some ISPs

Full Bridge Mode supports forwarding packets with VLAN tags.

Full Bridge Mode doesn't support wireless LAN.

OK

Available settings are explained as follows:

Item	Description
MPoA	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.
DSL Modem Settings	<p>Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP.</p> <p>Multi-PVC channel - The selections displayed here are determined by the page of Internet Access - Multi PVCs.</p> <p>Encapsulating Type - Drop down the list to choose the type provided by ISP.</p> <p>VPI - Type in the value provided by ISP.</p> <p>VCI - Type in the value provided by ISP.</p> <p>Modulation - Choose a suitable method for such connection.</p>
WAN Connection Detection	<p>Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.</p> <p>Mode - Choose ARP Detect, 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.

	<ul style="list-style-type: none"> ● Ping Gateway IP - If you choose Ping Detect as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation. ● Ping Interval - Type the interval for the system to execute the PING operation. ● Ping Retry - Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
MTU	It means Max Transmit Unit for packet.
RIP Protocol	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how modems exchange routing tables information. Click Enable RIP for activating this function.
Bridge Mode	<p>Enable Bridge Mode - If the function is enabled, the router will work as a bridge modem.</p> <p>Enable Full Bridge Mode - If the function is enabled, the router will work as a bridge modem which is able to forward incoming packets with VLAN tags.</p>
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>Obtain an IP address automatically - Click this button to obtain the IP address automatically.</p> <p>Router Name - Type in the modem name provided by ISP.</p> <p>Domain Name - Type in the domain name that you have assigned.</p>
DHCP Client Identifier	<p>This feature is offered for certain ISP with special request. Check this box to enable the function of DHCP client identifier for some ISP.</p> <p>Username - Type a username used for such function.</p> <p>Password - Type a password used for such function.</p>
Specify an IP address	<p>Click this radio button to specify some data.</p> <p>WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.</p>

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

OK Clear All Close

IP Address - Type in the private IP address.

Subnet Mask - Type in the subnet mask.

Gateway IP Address - Type in gateway IP address.

Default MAC Address

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

MAC Address - Type in the MAC address for the modem manually.

DNS Server IP Address

Type in the primary IP address for the modem. 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-1-4 IPv6

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

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

Internet Access >> IPv6

WAN 1

Internet Access Mode	Offline
Connection Type	

OK Cancel

II-1-4-2 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.

Internet Access >> IPv6

WAN 1

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

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

OK

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 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.
--	---

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

Online Status

Physical Connection		System Uptime: 0:2:32	
IPv4	IPv6		
LAN Status			
IP Address			
2001:B010:7300:201:21D:AAFF:FEA6:2568/64 (Global)			
FE80::21D:AAFF:FEA6:2568/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
7	4	690	328
WAN2 IPv6 Status			
>> Drop PPP			
Enable	Mode	Up Time	
Yes	PPP	0:02:08	
IP	Gateway IP		
2001:B010:7300:201:21D:AAFF:FEA6:256A/128 (Global)	FE80::90:1A00:242:AD52		
FE80::1D:AAFF: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-1-4-3 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

Internet Access Mode	
Connection Type	TSPC ▼
TSPC Configuration	
Username	<input type="text"/>
Password	<input type="password"/>
Tunnel Broker	<input type="text"/>
WAN Connection Detection	
Mode	Always On ▼

OK

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	<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.

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

II-1-4-4 Details Page for IPv6 – AICCU

Internet Access >> IPv6

WAN 1

Internet Access Mode
Connection Type AICCU

AICCU Configuration
☐ Always On
Username
Password
Tunnel Broker
Tunnel ID
Subnet Prefix /

WAN Connection Detection
Mode NS Detect

Note:

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

OK

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 NS Detect or Ping Detect. Mode - Choose Always On , Ping Detect or NS Detect for the system to execute for WAN detection. With NS Detect mode,

	<p>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.
--	--

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

II-1-4-5 Details Page for IPv6 – DHCPv6 Client

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

Internet Access >> IPv6

WAN 1

Internet Access Mode	
Connection Type	DHCPv6 Client ▼
DHCPv6 Client Configuration	
IAID (Identity Association ID)	44178403
WAN Connection Detection	
Mode	NS Detect ▼
Bridge Mode	
<input type="checkbox"/> Enable Bridge Mode	

OK

Available settings are explained as follows:

Item	Description
DHCPv6 Client Configuration	IAID - Type a number as IAID.
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	Enable Bridge Mode - If the function is enabled, the router will work as a bridge modem.

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

II-1-4-6 Details Page for IPv6 – Static IPv6

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

Internet Access >> IPv6

WAN 1

Internet Access Mode
Connection Type Static IPv6

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

Current IPv6 Address Table

Index	IPv6 Address/Prefix Length	Scope
-------	----------------------------	-------

Static IPv6 Gateway Configuration
IPv6 Gateway Address

WAN Connection Detection
Mode NS Detect

Bridge Mode
☐ Enable Bridge Mode

OK

Available settings are explained as follows:

Item	Description
Static IPv6 Address configuration	IPv6 Address - Type the IPv6 Static IP Address. Prefix Length - Type the fixed value for prefix length. Add - Click it to add a new entry. Update - Click it to modify an existed entry. Delete - Click it to remove an existed entry.
Current IPv6 Address Table	Display current interface IPv6 address.
Static IPv6 Gateway Configuration	IPv6 Gateway Address - Type your IPv6 gateway address here.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through NS Detect or Ping Detect. Mode - Choose Always On, Ping Detect or NS Detect for the system to execute for WAN detection. With NS Detect mode, the system will check if network connection is established or not, like IPv4 ARP Detect. Always On means no detection

	<p>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	Enable Bridge Mode - If the function is enabled, the router will work as a bridge modem.

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

II-1-4-7 Details Page for IPv6 – 6in4 Static Tunnel

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.

Internet Access >> IPv6

WAN 1

Internet Access Mode
Connection Type 6in4 Static Tunnel

6in4 Static Tunnel
Remote Endpoint IPv4 Address
6in4 IPv6 Address / (default: 64)
LAN Routed Prefix / (default: 64)
Tunnel TTL (default: 255)

WAN Connection Detection
Mode NS Detect

OK

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 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</p>

	be on always. ● Ping IP/Hostname - If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. ● TTL (Time to Live) -If you choose Ping Detect as detection mode, you have to type TTL value.
--	---

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

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

Online Status

Physical Connection		System Uptime: 0day 0:4:16	
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-1-4-8 Details Page for IPv6 – 6rd

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

Internet Access >> IPv6

WAN 1

Internet Access Mode
Connection Type 6rd

6rd Settings
6rd Mode ☐ Auto 6rd ☒ Static 6rd

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

WAN Connection Detection
Mode NS Detect

OK

Available settings are explained as follows:

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

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	
15		113	
TX Bytes		RX Bytes	
1354		18040	
WAN1 IPv6 Status			
Enable		Mode	
Yes		6rd	
Up Time			
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	
13		29	
TX Bytes		RX Bytes	
967		2620	

II-1-3 Multi-PVC/VLAN

Multi-PVC/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-PVC/VLAN.

II-1-3-1 General

This page shows the basic configurations used by every channel.

Internet Access >> Multi-PVC/VLAN

Multi-PVC/VLAN

General		Advanced		
Channel	Enable	WAN Type	VPI/VCI	VLAN Tag
1	<input checked="" type="checkbox"/>	ADSL	0/33	None
3. WAN3	<input type="checkbox"/>	ADSL	1/43	None
4. WAN4	<input type="checkbox"/>	ADSL	1/44	None
5. WAN5	<input type="checkbox"/>	ADSL	1/45	None
6.	<input type="checkbox"/>	ADSL	1/46	None

Note:

Channel 2 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.

To configure a PVC/VLAN channel, click its channel number.

WAN links for Channel 3, 4 and 5 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 3, 4 and 5 to configure your router.

☒ Enable Channel 3:
WAN Type : ADSL

General Settings

VPI 1

VCI 43

Protocol PPPoA

Encapsulation VC MUX

☐ Add VLAN Header

VLAN Tag 0

Priority 0

ATM QoS

QoS Type UBR

PCR 0

SCR 0

MBS 0

☐ **Open Port-based Bridge Connection for this Channel**

Physical Members

☐ P1 ☐ P2

☐ **Open WAN Interface for this Channel**

WAN Application: ☐ Management ☐ IPTV

WAN Connection Detection

Mode ARP Detect

PPPoE/PPPoA Client

ISP Access Setup

ISP Name

Username

Password

PPP Authentication PAP Only

☒ Always On

Idle Timeout -1 second(s)

IP Address From ISP

Fixed IP ☐ Yes ☒ No (Dynamic IP)

Fixed IP Address

MPoA (RFC1483/2684)

☐ 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

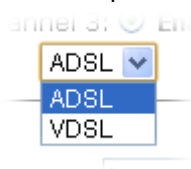
DNS Server IP Address

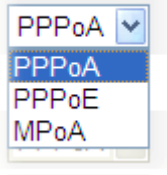
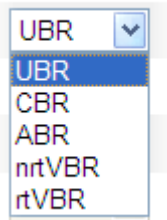
Primary IP Address 8.8.8.8

Secondary IP Address 8.8.4.4

OK
Cancel

Available settings are explained as follows:

Item	Description
Enable Channel 3/4/5	Check it to enable this channel.
WAN Type	<p>The connections and interfaces created in every channel may select a specific WAN type to be built upon.</p> 
General Settings	VPI - Type in the value provided by your ISP.


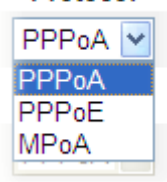
	<p>VCI - Type in the value provided by your ISP.</p> <p>Protocol - Select a proper protocol for this channel.</p> <p>Protocol</p>  <p>Encapsulation - Choose a proper type for this channel. The types will be different according to the protocol setting that you choose.</p> <p>Add VLAN Header - Check the box to enable VLAN tag configuration.</p> <p>VLAN Tag - Type the value as the VLAN ID number. Valid settings are in the range from 1 to 4095. The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value.</p> <p>Priority - Choose the number to determine the packet priority for such VLAN. The range is from 0 to 7.</p>
ATM QoS	<p>Such configuration is applied to upstream packets. Such information will be provided by ISP. Please contact with your ISP for detailed information.</p> <p>QoS Type - Select a proper QoS type for the channel.</p> <p>QoS Type</p>  <p>PCR - It represents Peak Cell Rate. The default setting is "0".</p> <p>SCR - It represents Sustainable Cell Rate. The value of SCR must be smaller than PCR.</p> <p>MBS - It represents Maximum Burst Size. The range of the value is 10 to 50.</p>
Open Port-based Bridge Connection for this Channel	<p>The settings here will create a bridge between the LAN ports selected and the WAN. The WAN interface of the bridge connection will be built upon the WAN type selected using the VLAN tag configured.</p> <p>Physical Members - Group the physical ports by checking the corresponding check box(es) for applying the port-based bridge connection.</p> <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.

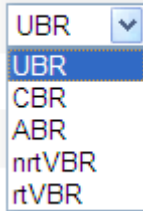
	<ul style="list-style-type: none"> ● IPTV - The IPTV configuration will allow the WAN interface to send IGMP packets to IPTV servers.
WAN Connection Detection	<p>Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.</p> <p>Mode - Choose ARP Detect or Ping Detect for the system to execute for WAN detection.</p> <p>Ping IP - If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.</p> <p>TTL (Time to Live) - Displays value for your reference. TTL value is set by telnet command.</p>
PPPoE/PPPoA Client	<p>Enter your allocated username, password and authentication parameters according to the information provided by your ISP.</p> <p>ISP Access Setup</p> <ul style="list-style-type: none"> ● ISP Name - Type in the name of your ISP. ● Username - Type in the username provided by ISP in this field. The maximum length of the name you can set is 80 characters. ● Password - Type in the password provided by ISP in this field. The maximum length of the password you can set is 48 characters. ● PPP Authentication - Select PAP only or PAP or CHAP for PPP. ● Always On - Check it to keep the network connection always. <p>Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action.</p> <p>IP Address From ISP</p> <ul style="list-style-type: none"> ● Fixed IP - Click Yes to use this function and type in a fixed IP address in the box of Fixed IP Address.
MPoA (RFC1483/2684)	<p>Obtain an IP address automatically - Click this button to obtain the IP address automatically.</p> <ul style="list-style-type: none"> ● Router Name - Type in the router name provided by ISP. ● Domain Name - Type in the domain name that you have assigned. <p>Specify an IP address - Click this radio button to specify some data.</p> <ul style="list-style-type: none"> ● IP Address - Type in the private IP address. ● Subnet Mask - Type in the subnet mask. ● Gateway IP Address - Type in gateway IP address. <p>DNS Server IP Address - Type in the primary IP address for the router if you want to use Static IP mode. If necessary, type in secondary IP address for necessity in the future.</p>

After finished the above settings, click **OK** to save the settings and return to previous page.
Click any index 6 to get the following web page:

<input checked="" type="checkbox"/> Enable Channel 6: WAN Type : ADSL ▾			
General Settings		ATM QoS	
VPI	<input type="text" value="1"/>	QoS Type	UBR ▾
VCI	<input type="text" value="46"/>	PCR	<input type="text" value="0"/>
Protocol	PPPoA ▾	SCR	<input type="text" value="0"/>
Encapsulation	VC MUX ▾	MBS	<input type="text" value="0"/>
<input type="checkbox"/> Add VLAN Header VLAN Tag <input type="text" value="0"/> Priority <input type="text" value="0"/>			
Bridge mode			
<input type="checkbox"/> Enable Physical Members <input type="checkbox"/> P1 <input type="checkbox"/> P2			

Available settings are explained as follows:

Item	Description
Enable Channel	Check it to enable this channel.
WAN Type	<p>The connections and interfaces created in every channel may select a specific WAN type to be built upon.</p> 
General Settings	<p>VPI - Type in the value provided by your ISP. VCI - Type in the value provided by your ISP. Protocol - Select a proper protocol for this channel.</p> <p>Protocol</p>  <p>Encapsulation - Choose a proper type for this channel. The types will be different according to the protocol setting that you choose. Add VLAN Header - Check the box to enable VLAN tag configuration. 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</p>

	<p>configure the same VLAN tag value.</p> <p>Priority - Choose the number to determine the packet priority for such VLAN. The range is from 0 to 7.</p>
ATM QoS	<p>Such configuration is applied to upstream packets. Such information will be provided by ISP. Please contact with your ISP for detailed information.</p> <p>QoS Type - Select a proper QoS type for the channel.</p> <p>QoS Type</p>  <p>PCR - It represents Peak Cell Rate. The default setting is "0".</p> <p>SCR - It represents Sustainable Cell Rate. The value of SCR must be smaller than PCR.</p> <p>MBS - It represents Maximum Burst Size. The range of the value is 10 to 50.</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-1-3-2 Advanced

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

Internet Access >> Multi-PVC/VLAN

Multi-PVC/VLAN

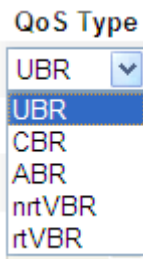
General		Advanced			
ATM QoS					
Channel	QoS Type	PCR	SCR	MBS	PVC to PVC Binding
1.	UBR	0	0	0	Disable
3.	UBR	0	0	0	Disable
4.	UBR	0	0	0	Disable
5.	UBR	0	0	0	Disable
6.	UBR	0	0	0	Disable

Note:

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

OK Cancel

Available settings are explained as follows:

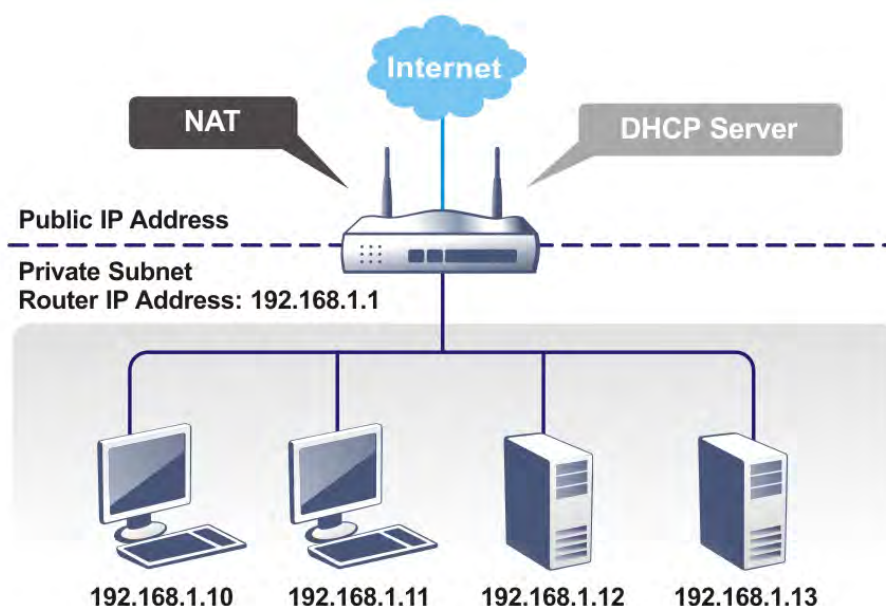
Item	Description
QoS Type	Select a proper QoS type for the channel. 
PCR	It represents Peak Cell Rate. The default setting is "0".
SCR -	It represents Sustainable Cell Rate. The value of SCR must be smaller than PCR.
MBS	It represents Maximum Burst Size. The range of the value is 10 to 50.
PVC to PVC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

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

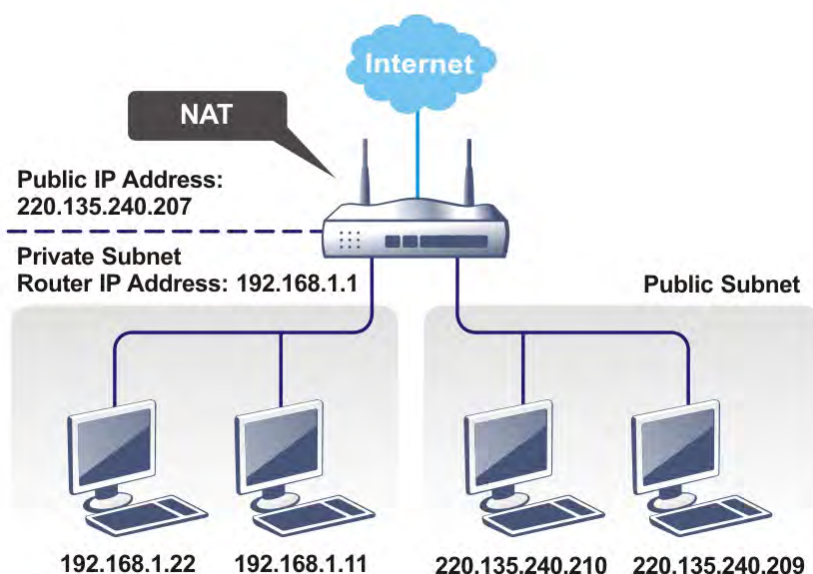
II-2 LAN

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.

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.

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

Ethernet TCP / IP and DHCP Setup	LAN 1 IPv6 Setup
LAN IP Network Configuration For NAT Usage 1st IP Address: <input type="text" value="192.168.1.1"/> 1st Subnet Mask: <input type="text" value="255.255.255.0 / 24"/> For IP Routing Usage: <input type="radio"/> Enable <input checked="" type="radio"/> Disable 2nd IP Address: <input type="text" value="192.168.2.1"/> 2nd Subnet Mask: <input type="text" value="255.255.255.0"/> <input type="button" value="2nd Subnet DHCP Server"/> RIP Protocol Control: <input type="text" value="Disable"/>	DHCP Server Configuration <input type="radio"/> Disable <input checked="" type="radio"/> Enable Server Relay Agent: <input type="radio"/> 1st Subnet <input type="radio"/> 2nd Subnet Start IP Address: <input type="text" value="192.168.1.10"/> IP Pool Counts: <input type="text" value="200"/> (max. 253) Gateway IP Address: <input type="text" value="192.168.1.1"/> Lease Time: <input type="text" value="86400"/> (s) <input type="button" value="Advanced"/> You can configure DHCP server options here. DNS Server IP Address Primary IP Address: <input type="text"/> Secondary IP Address: <input type="text"/> <input type="checkbox"/> Force router to use address for DNS

Available settings are explained as follows:

Item	Description
LAN IP Network Configuration	<p>For NAT Usage,</p> <p>1st IP Address - Type in private IP address for connecting to a local private network (Default: 192.168.1.1).</p> <p>1st Subnet Mask - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)</p> <p>For IP Routing Usage - Click Enable to invoke this function. The default setting is Disable.</p> <p>2nd Address - Type in secondary IP address for connecting to a subnet. (Default: 192.168.2.1/ 24)</p> <p>2nd Subnet Mask - An address code that determines the size of the network. (Default: 255.255.255.0/ 24)</p> <p>2nd Subnet DHCP Server - You can configure the modem to serve as a DHCP server for the 2nd subnet.</p>

Router Web Configurator - Windows Internet Explorer

http://192.168.1.1/doc/pwdhcp.htm

2nd DHCP Server

Start IP Address:

IP Pool Counts: (max. 10)

Index	Matched MAC Address	given IP Address

MAC Address:

- **Start IP Address:** Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 2nd IP address of your modem is 220.135.240.1, the starting IP address must be 220.135.240.2 or greater, but smaller than 220.135.240.254.
- **IP Pool Counts:** Enter the number of IP addresses in the pool. The maximum is 10. For example, if you type 3 and the 2nd IP address of your modem is 220.135.240.1, the range of IP address by the DHCP server will be from 220.135.240.2 to 220.135.240.11.
- **MAC Address:** Enter the MAC Address of the host one by one and click **Add** to create a list of hosts to be assigned, deleted or edited IP address from above pool. Set a list of MAC Address for 2nd DHCP server will help modem 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.

RIP Protocol Control,

Disable - deactivate the RIP protocol. It will lead to a stoppage of the exchange of routing information between modems. (Default)

- **1st Subnet** - Select the modem to change the RIP information of the 1st subnet with neighboring modems.
- **2nd Subnet** - Select the modem to change the RIP information of the 2nd subnet with neighboring modems.

DHCP Server Configuration

DHCP stands for Dynamic Host Configuration Protocol. The modem 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 modem enabled as a DHCP server if you do not have a DHCP server for your network.

If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.

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

Enable Server - Let the modem assign IP address to every

	<p>host in the LAN.</p> <ul style="list-style-type: none">● Relay Agent - (1st subnet/2nd subnet) Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.● DHCP Server IP Address -Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.● Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your modem is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.● IP Pool Counts - Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.● Gateway IP Address - Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the modem, which means the modem is the default gateway.● Lease Time - Enter the time to determine how long the IP address assigned by DHCP server can be used. <p>Advanced - If required, click it to set option number for DHCP.</p>																			
DNS Server IP Address	<p>DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.</p> <p>Primary IP Address -You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server.</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> <div><p>Online Status</p><hr/><div>Physical ConnectionSystem Uptime: 22:22:45</div><table><thead><tr><th colspan="2">IPv4</th><th colspan="2">IPv6</th></tr></thead><tbody><tr><td>LAN Status</td><td colspan="3">Primary DNS: 8.8.8.8</td><td>Secondary DNS: 8.8.4.4</td></tr><tr><td>IP Address</td><td>TX Packets</td><td colspan="2">RX Packets</td><td></td></tr><tr><td>192.168.1.1</td><td>0</td><td colspan="2">41533</td><td></td></tr></tbody></table></div> <p>If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.</p> <p>If the IP address of a domain name is already in the DNS 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.</p> <p>Force router to use address for DNS- Force Vigor modem to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).</p>	IPv4		IPv6		LAN Status	Primary DNS: 8.8.8.8			Secondary DNS: 8.8.4.4	IP Address	TX Packets	RX Packets			192.168.1.1	0	41533		
IPv4		IPv6																		
LAN Status	Primary DNS: 8.8.8.8			Secondary DNS: 8.8.4.4																
IP Address	TX Packets	RX Packets																		
192.168.1.1	0	41533																		

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 LAN1 – IPv6 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. Below shows the settings page for IPv6.

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::BE80:75E6:EA9E:D7B6/64	Link

DNS Server IPv6 Address
Deploy when WAN is up

Primary DNS Server
2001:4860:4860::8888

Secondary DNS Server
2001:4860:4860::8844

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

DHCPv6 Server

☒ Enable Server
☐ Disable Server

☐ IPv6 Address Random Allocation

☒ Auto IPv6 range

Start IPv6 Address

End IPv6 Address

Advance setting
Edit

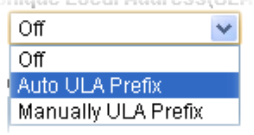
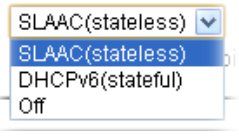
Advance setting
Edit

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 IPv6	Check the box to enable the configuration of LAN 1 IPv6 Setup.
WAN Primary Interface	Use the drop down list to specify a WAN interface for IPv6.
Static IPv6 Address 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	Unique Local Addresses (ULAs) are private IPv6 addresses

(ULA) configuration	<p>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 Server - 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	<p>Enable Server -Click it to enable DHCPv6 server. DHCPv6 Server could assign IPv6 address to PC according to the Start/End IPv6 address configuration.</p> <p>Disable Server -Click it to disable DHCPv6 server.</p> <p>Auto IPv6 range - After check the box, Vigor router will assign the IPv6 range automatically.</p>

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.

LAN >> General Setup

DHCPv6 Server

Authentication Protocol: None

Prefix Delegation: ☐ Enable ☐ Disable

Prefix: /

DHCPv6 Prefix Delegation

New Prefix: ::/64

Suffix: :

New Prefix Length: (0~64)

Client Link Local Address:

Client DUID(option):

Add

Prefix	Prefix Length	Link Local	DUID
--------	---------------	------------	------

OK Cancel

Advance setting

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

Router Advertisement Configuration

☒ Enable ☐ Disable

Hop Limit: 64

Min Interval Time(sec): 200

Max Interval Time(sec): 600

Default Lifetime(sec): 1800 (High Availability secondary is 0)

Default Preference: Medium

MTU: 0 ☒ Auto

Extension WAN

Available WAN:

Selected WAN:

>> <<

OK Close

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, Vigor160 can be treated as the default gateway.

Default Preference - It determines the priority of the host

	<p>behind the router when RA (Router Advertisement) packets are transmitted.</p> <p>MTU - It means Max Transmit Unit for packet. If Auto is selected, the router will determine the MTU value for LAN.</p> <p>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.</p> <p>Available WAN - Additional WANs available but not currently selected to carry IPv6 traffic.</p> <p>Selected WAN - Additional WANs selected to carry IPv6 traffic.</p>
--	--

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-2-2 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.

LAN >> Bind IP to MAC

Bind IP to MAC

☐ Enable ☒ Disable

☐ Strict Bind

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

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

IP Address

Mac Address : : : : :

Comment Max: 12 characters

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

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

Backup IP Bind List :

Upload From File: 未選擇檔案

Note:

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

OK

Available settings are explained as follows:

Item	Description
Enable	Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.
Disable	Click this radio button to disable this function. All the settings on this page will be invalid.
Strict Bind	Check the box to block the connection of the IP/MAC which is not listed in IP Bind List.
ARP Table	This table is the LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be

	selected and added to IP Bind List by clicking Add below.
Select All	Select all entries in the ARP Table for manipulation.
Sort	Reorder the entry based on the IP address.
Refresh	Refresh the ARP table listed below to obtain the newest ARP table information.
Add / Update to IP Bind List	<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>
IP Bind List	It displays a list for the IP bind to MAC information.
Backup IP Bind List	Click Backup and enter a filename to back up IP Bind List to a file.
Upload From File	Click Browse... to select an IP Bind List backup file. Click Restore to restore the backup and overwrite the existing list.



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-3 NAT

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

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

The benefit of the NAT includes:

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



Info

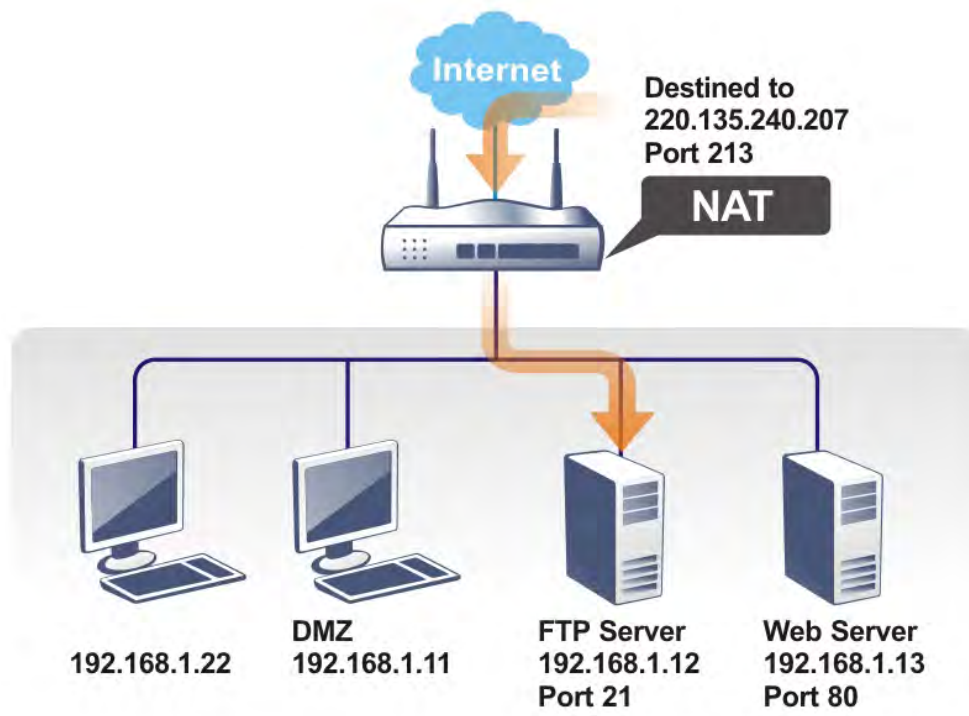
On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by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

Web User Interface

Routing
NAT
Port Redirection
DMZ Host
Open Ports
ALG
Firewall

II-3-1 Port Redirection

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



The port redirection can only apply to incoming traffic.

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

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

Index	Enable	Service Name	WAN Interface	Protocol	Public Port	Source IP	Private IP
1.	<input type="checkbox"/>		All			Any	
2.	<input type="checkbox"/>		All			Any	
3.	<input type="checkbox"/>		All			Any	
4.	<input type="checkbox"/>		All			Any	
5.	<input type="checkbox"/>		All			Any	
6.	<input type="checkbox"/>		All			Any	
7.	<input type="checkbox"/>		All			Any	
8.	<input type="checkbox"/>		All			Any	
9.	<input type="checkbox"/>		All			Any	
10.	<input type="checkbox"/>		All			Any	
11.	<input type="checkbox"/>		All			Any	
12.	<input type="checkbox"/>		All			Any	
13.	<input type="checkbox"/>		All			Any	
14.	<input type="checkbox"/>		All			Any	
15.	<input type="checkbox"/>		All			Any	
16.	<input type="checkbox"/>		All			Any	
17.	<input type="checkbox"/>		All			Any	
18.	<input type="checkbox"/>		All			Any	
19.	<input type="checkbox"/>		All			Any	
20.	<input type="checkbox"/>		All			Any	

OK

Cancel

Backup settings:

Backup

Upload From File: 選擇檔案 未選擇任何檔案

Restore

Note:

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

Each item is explained as follows:

Item	Description
Index	Display the number of the profile.
Enable	Check the box to enable 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.

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
Protocol	TCP ▼
WAN Interface	ALL ▼
Public Port	0
Source IP	Any ▼ IP Object
Private IP	
Private Port	0

Note:

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

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable such port redirection setting.
Mode	Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select Range . In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered, the system will calculate and display the ending IP of private IP automatically.
Service Name	Enter the description of the specific network service.
Protocol	Select the transport layer protocol (TCP or UDP).
WAN Interface	Select the WAN 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.

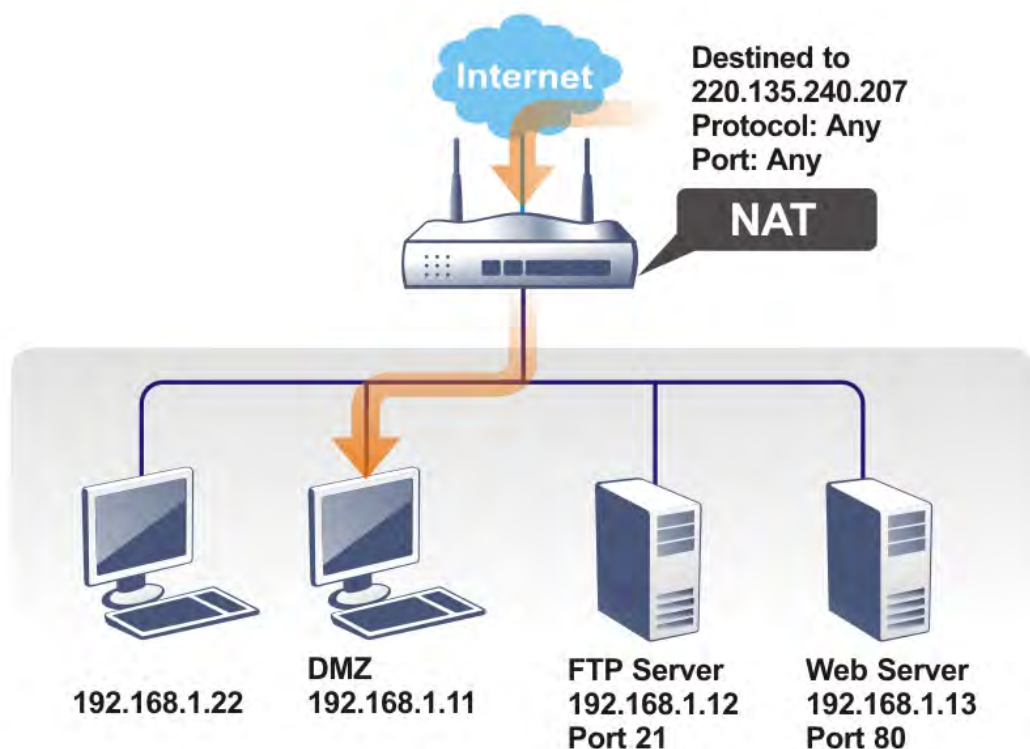
System Maintenance >> Management



IPv4 Management Setup		IPv6 Management Setup	
Router Name <input type="text" value="DrayTek"/>			
<input type="checkbox"/> Default:Disable Auto-Logout		Management Port Setup <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports	
Internet Access Control <input type="checkbox"/> Allow management from the Internet Domain name allowed <input type="text"/>		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)	
<input type="checkbox"/> FTP Server <input type="checkbox"/> HTTP Server <input checked="" type="checkbox"/> Enforce HTTPS Access <input checked="" type="checkbox"/> HTTPS Server <input type="checkbox"/> Telnet Server <input type="checkbox"/> TR069 Server <input type="checkbox"/> SSH Server <input checked="" type="checkbox"/> Disable PING from the Internet		SNMP Setup <input type="checkbox"/> Enable SNMP Agent	
Access List from the Internet <input type="checkbox"/> Apply Access List to PING		Get Community <input type="text" value="public"/> Set Community <input type="text" value="private"/> Manager Host IP <input type="text"/> Trap Community <input type="text" value="public"/>	
List	IP	Subnet Mask	
1	<input type="text"/>	<input type="text"/>	
2	<input type="text"/>	<input type="text"/>	

II-3-2 DMZ Host

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



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

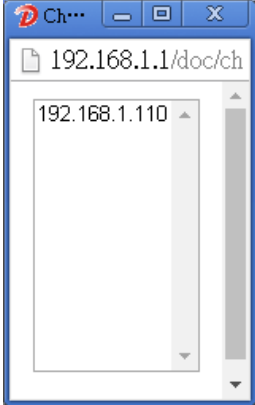

Click **DMZ Host** to open the following page. You can set different DMZ host for each WAN interface. Click the WAN tab to switch into the configuration page for that WAN.

NAT >> DMZ Host Setup

DMZ Host Setup

WAN1	
WAN 1	
<div>None</div>	
Private IP	<div></div> <div>Choose IP</div>
MAC Address of the True IP DMZ Host	<div>00 · 00 · 00 : 00 · 00 · 00</div>
Note: If True-IP DMZ is enabled the routers WAN connection will be forced to remain on.	
<div>OK</div>	

Available settings are explained as follows:

Item	Description
WAN1	Choose Private IP, Active True 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> <p>NAT >> DMZ Host Setup</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

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

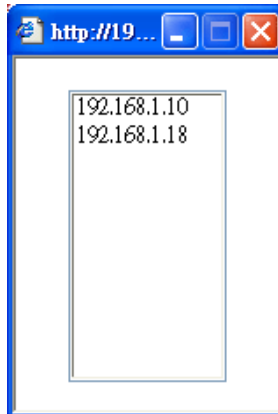
OK Clear

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

Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.



When you have selected one private IP from the above dialog, the IP address will be shown on the screen. Click OK to save the setting.

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

II-3-3 Open Ports

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

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

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

NAT >> Open Ports

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

Index	Enable	Comment	WAN Interface	Source IP	Local IP Address
<u>1.</u>	<input type="checkbox"/>			Any	
<u>2.</u>	<input type="checkbox"/>			Any	
<u>3.</u>	<input type="checkbox"/>			Any	
<u>4.</u>	<input type="checkbox"/>			Any	
<u>5.</u>	<input type="checkbox"/>			Any	
<u>6.</u>	<input type="checkbox"/>			Any	
<u>7.</u>	<input type="checkbox"/>			Any	
<u>8.</u>	<input type="checkbox"/>			Any	
<u>9.</u>	<input type="checkbox"/>			Any	
<u>10.</u>	<input type="checkbox"/>			Any	
<u>11.</u>	<input type="checkbox"/>			Any	
<u>12.</u>	<input type="checkbox"/>			Any	
<u>13.</u>	<input type="checkbox"/>			Any	
<u>14.</u>	<input type="checkbox"/>			Any	
<u>15.</u>	<input type="checkbox"/>			Any	
<u>16.</u>	<input type="checkbox"/>			Any	
<u>17.</u>	<input type="checkbox"/>			Any	
<u>18.</u>	<input type="checkbox"/>			Any	
<u>19.</u>	<input type="checkbox"/>			Any	
<u>20.</u>	<input type="checkbox"/>			Any	

Backup settings: <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"/>
---	---

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](#).

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.
Enable	Check it to enable the profile.
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.
Backup	Click it to backup current settings of Open Ports as a file.
Restore	Click it to restore Open Ports configuration file.

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

☒ Enable Open Ports

Comment

WAN Interface WAN1

Source IP Any [IP Object](#)

Private IP [Choose IP](#)

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

Available settings are explained as follows:

Item	Description
Enable Open Ports	Check to enable this entry.
Comment	Make a name for the defined network application/service.
WAN Interface	Specify the WAN interface that will be used for this entry.
Source IP	Use the drop down list to specify an IP object. Or click IP Object link to create a new one for applying.
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.

II-3-4 ALG

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

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

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

NAT >> ALG

ALG (Application Layer Gateway)

| [Set to Factory Default](#) |

☒ Enable ALG

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

OK

Available settings are explained as follows:

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

II-4 Applications

Dynamic DNS

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

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

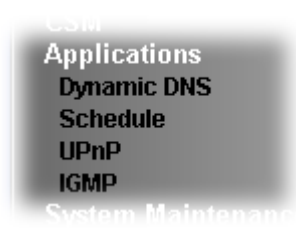
Schedule

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.

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.

Web User Interface



II-4-1 Dynamic DNS

Enable the Function and Add a Dynamic DNS Account

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

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
1.	<input type="checkbox"/>	
2.	<input type="checkbox"/>	
3.	<input type="checkbox"/>	
4.	<input type="checkbox"/>	
5.	<input type="checkbox"/>	
6.	<input type="checkbox"/>	

[OK](#) [Clear All](#)

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.
-------------	---

- 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: (max. 64 characters)

☐ 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###&c
md=update&offline=0

Auth Type: basic

Connection Type: Http

Server Response:

Login Name: chronic5563 (max. 64 characters)

Password: (max. 64 characters)

☐ 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.

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-4-3 UPnP

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



Info

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

Applications >> UPnP

UPnP

<input type="checkbox"/> Enable UPnP Service	Default WAN ▾
<input type="checkbox"/> Enable Connection Control Service	
<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-4-4 IGMP

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

II-4-4-1 General Setting

Applications >> IGMP

General setting

Working status

☐ **IGMP Proxy**

IGMP Proxy acts as a multicast proxy for hosts on the LAN side. Enable IGMP proxy to access any multicast group. This function **takes no effect when Bridge Mode is enabled**.

Interface

WAN1

IGMP version

Auto

General Query Interval

125

(seconds)

Add PPP header

☐

(Encapsulate IGMP in PPPoE)

Enable IGMP syslog

☐

☐ **IGMP Snooping**

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

☐ **IGMP Fast Leave**

The router stops forwarding multicast traffic to a LAN port as soon as it receives a leave message from that port.
Each LAN port should have no more than one IGMP host connected.

OK

Cancel

Available settings are explained as follows:

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

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

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

II-4-4-2 Working Status

Applications >> IGMP

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

| [Refresh](#) |

Multicast Group Table

Index	Group ID	P1	P2
-------	----------	----	----

IGMP Device Table

Index	MAC Address	IP Address	Interface	IGMP Version
-------	-------------	------------	-----------	--------------

Available settings are explained as follows:

Item	Description
Refresh	Click this link to renew the working multicast group status.
Group ID	This field displays the ID port for the multicast group. The available range for IGMP starts from 224.0.0.0 to 239.255.255.254.
P1 to P2	It indicates the LAN port used for the multicast group.

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-active the service after expiry.

Domain Name : .drayddns.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).

Next > **Cancel**

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

Service Activation Wizard

Please confirm your settings

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

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

< Back **Activate** **Cancel**

- 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 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

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

Domain Name Get domain

Determine Real WAN IP

Determine WAN IP

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 DrayTek Global (www.drayddns.com) ▼

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

Domain Name 115.100.154.drayddns.com Edit domain

Determine Real WAN IP WAN IP ▼

Determine WAN IP WAN 1 ▲
WAN 2
WAN 3
WAN 4 ▼

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 DrayTek Global (www.drayddns.com) ▼

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

Domain Name 115.100.154.drayddns.com Edit domain

Determine Real WAN IP WAN IP ▼

Determine WAN IP WAN 1 ▲
WAN 2
WAN 3
WAN 4 ▼

OK Clear Cancel

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

My information - My Products

Device Information

Device Name: FWT995
Serial Number: 11504994194
Model: Vigor2525 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	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="drayddns.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	<input type="text" value="DrayTek Global (www.drayddns.com)"/>
Status	Activated [Start Date:2017-02-23 Expire Date:2018-02-23]
Domain Name	<input type="text" value="XXXX25"/> <input type="text" value="drayddns.com"/> <input type="button" value="Sync domain"/>
WAN Interfaces	<input type="text" value="WAN IP"/>
	<input type="text" value="WAN 1"/> <input type="text" value="WAN 2"/> <input type="text" value="WAN 3"/> <input type="text" value="WAN 4"/>
Determine WAN IP	


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


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




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

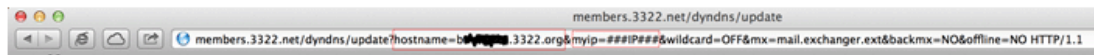
Username: bi*****

Password: 88*****

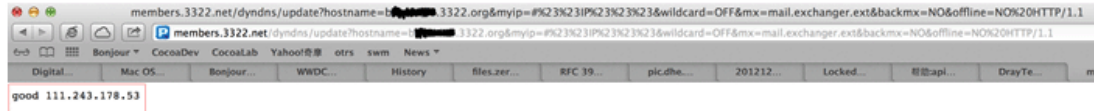
Host name: bi*****.3322.org

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 CloudDNS.net.

The top part of the image shows a web browser window with the URL `ipv4.cloudns.net/api/dynamicURL/?q=MTUzMTE3OjE0NTA1MzA6MDAyODE3MDliZGQ3ZjNiZmE2M...`. Below the browser window, the text "OK" is visible.

The bottom part of the image shows a screenshot of the "Applications >> Dynamic DNS Setup >> Dynamic DNS Account Setup" configuration window. The window is titled "Index : 1". It contains the following fields and options:

- ☒ Enable Dynamic DNS Account
- Service Provider: User-Defined (with a help icon)
- 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: (empty field)
- Login Name: chronic6633 (max. 64 characters)
- Password: (masked with asterisks) (max. 64 characters)
- ☐ Wildcards
- ☐ Backup MX
- Mail Extender: (empty field)
- Determine Real WAN IP: WAN IP

At the bottom of the window are three buttons: OK, Clear, and Cancel. A red arrow points from the "Login Name" field in the configuration window to the "member@3322.net" field in the browser window.

II-5 Routing

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.



Info

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

Web User Interface



II-5-1 Static Route

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	Mask	Gateway	Interface
1.	<input type="checkbox"/>				
2.	<input type="checkbox"/>				
3.	<input type="checkbox"/>				
4.	<input type="checkbox"/>				
5.	<input type="checkbox"/>				
6.	<input type="checkbox"/>				

34.	<input type="checkbox"/>				
35.	<input type="checkbox"/>				
36.	<input type="checkbox"/>				
37.	<input type="checkbox"/>				
38.	<input type="checkbox"/>				
39.	<input type="checkbox"/>				
40.	<input type="checkbox"/>				

Backup settings: <input type="button" value="Backup"/>	Upload From File: <input type="button" value="選擇檔案"/> 未選擇檔案 <input type="button" value="Restore"/>
---	---

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.

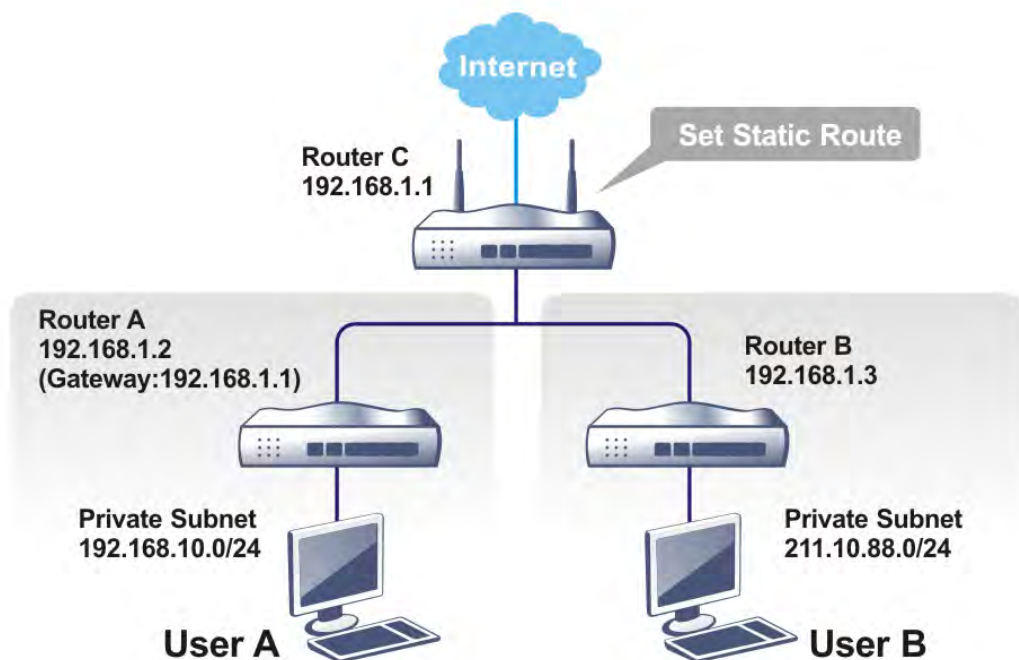
	<div>Diagnostics >> View Routing Table</div> <div><div>Current Running Routing TableIPv6 Routing TableRefresh</div><div>Key: C - connected, S - static, R - RIP, * - default, ~ - private C~ 192.168.1.0/ 255.255.255.0 directly connected LAN1</div></div>
Index	The number (1 to 30) under Index allows you 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.
Backup	Click it to backup current settings of static route as a file.
Restore	Click it to restore static route configuration file.

Add Static Routes to Private and Public Networks

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

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

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



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



Info

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

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

Routing >> Static Route Setup

Index No. 1

<input type="checkbox"/> Enable	
Destination IP Address	???
Subnet Mask	255.255.255.255 / 32 ▼
Gateway IP Address	
Network Interface	LAN ▼

Note:

WAN3, WAN4, WAN5 are PVCs or VLANs that can be configured on the [Multi-PVC/VLAN](#) page.

OK Cancel Delete

Available settings are explained as follows:

Item	Description
Enable	Click it to enable this profile.
Destination IP Address	Type an IP address as the destination of such static route.
Subnet Mask	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**.

Routing >> Static Route Setup

Index No. 1

<input type="checkbox"/> Enable	
Destination IP Address	211.100.88.0
Subnet Mask	255.255.255.255 / 32 ▼
Gateway IP Address	192.168.1.3
Network Interface	LAN ▼

Note:

WAN3, WAN4, WAN5 are PVCs or VLANs that can be configured on the [Multi-PVC/VLAN](#) page.

OK Cancel Delete

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

Diagnostics >> View Routing Table

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	Gateway	Interface	
1.	<input type="checkbox"/>				
2.	<input type="checkbox"/>				
3.	<input type="checkbox"/>				
4.	<input type="checkbox"/>				
5.	<input type="checkbox"/>				
6.	<input type="checkbox"/>				
7.	<input type="checkbox"/>				
8.	<input type="checkbox"/>				
9.	<input type="checkbox"/>				
10.	<input type="checkbox"/>				
11.	<input type="checkbox"/>				
12.	<input type="checkbox"/>				
13.	<input type="checkbox"/>				
14.	<input type="checkbox"/>				
15.	<input type="checkbox"/>				
16.	<input type="checkbox"/>				
17.	<input type="checkbox"/>				
18.	<input type="checkbox"/>				
19.	<input type="checkbox"/>				
20.	<input type="checkbox"/>				
21.	<input type="checkbox"/>				
22.	<input type="checkbox"/>				
23.	<input type="checkbox"/>				
24.	<input type="checkbox"/>				
25.	<input type="checkbox"/>				
26.	<input type="checkbox"/>				
27.	<input type="checkbox"/>				
28.	<input type="checkbox"/>				
29.	<input type="checkbox"/>				
30.	<input type="checkbox"/>				
31.	<input type="checkbox"/>				
32.	<input type="checkbox"/>				
33.	<input type="checkbox"/>				
34.	<input type="checkbox"/>				
35.	<input type="checkbox"/>				
36.	<input type="checkbox"/>				
37.	<input type="checkbox"/>				
38.	<input type="checkbox"/>				
39.	<input type="checkbox"/>				
40.	<input type="checkbox"/>				

Backup settings: <input type="button" value="Backup"/>	Upload From File: 選擇檔案 未選擇檔案 <input type="button" value="Restore"/>
---	--

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all of the settings and return to factory default

	settings.
Viewing 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.
Backup	Click it to backup current settings of static route as a file.
Restore	Click it to restore static route configuration file.

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
 LAN1 ▼

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.

Part III Security



Firewall

While the broadband users demand more bandwidth for multimedia, interactive applications, or distance learning, security has been always the most concerned. The firewall of the Vigor router helps to protect your local network against attack from unauthorized outsiders. It also restricts users in the local network from accessing the Internet.



CSM

CSM is an abbreviation of Central Security Management which is used to filter the web content and URL content to reach a goal of security management.

III-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:

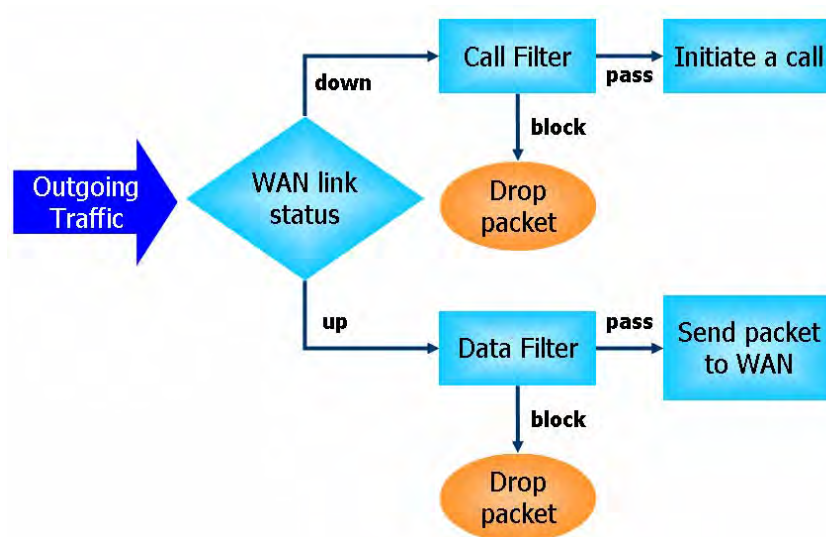
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

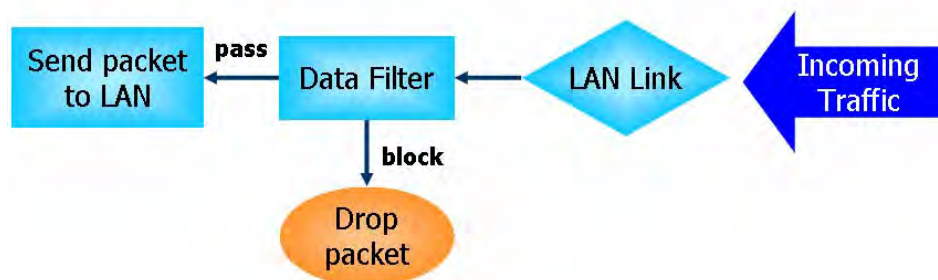
IP Filters

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.

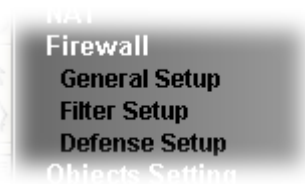
Also the Vigor router monitors the traffic. Any abnormal traffic flow violating the pre-defined parameter, such as the number of thresholds, is identified as an attack and the Vigor router will activate its defense mechanism to mitigate in a real-time manner.

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.



III-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

☒ Enable
☐ Disable

Start Filter Set Set#1 ▼

Data Filter

☒ Enable
☐ Disable

Start Filter Set Set#2 ▼

☒ Allow pass inbound fragmented large packets (required for certain games and streaming)

☒ Enable Strict Security Firewall

Block routing connections initiated from WAN ☐ IPv4 ☒ IPv6

Note:
Packets are filtered by firewall functions in the following order:
1.Data Filter Sets and Rules 2.Block routing connections initiated from WAN 3.Default Rule

OK

Cancel

Backup Firewall :

Backup

Restore Firewall: 選擇檔案 未選擇任何檔案

Restore

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="checkbox"/>
Sessions Control	0 / 10000	<input type="checkbox"/>
URL Content Filter	None	<input type="checkbox"/>

Advance Setting Edit

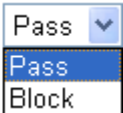
OK Cancel

Backup Firewall : Backup
Restore Firewall: 選擇檔案 未選擇檔案 Restore

Note:

This will not backup the detail setting of Quality of Service and Schedule.

Available settings are explained as follows:

Item	Description
Filter	<p>Select Pass or Block for the packets that do not match with the filter rules.</p> <p>Filter </p>
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.
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>
Advance Setting	Click Edit to open the following window. However, it is strongly recommended to use the default settings here.

	<p>Firewall >> General Setup</p> <div data-bbox="715 271 1385 495"> <p>Advance Setting</p> <p>Codepage: ANSI(1252)-Latin I</p> <p>Window size: 65535</p> <p>Session timeout: 1440 Minute</p> <p>OK 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 dialog box.</p> <div data-bbox="703 904 1406 1330"> </div> <p>Window size - It determines the size of TCP protocol (0~65535). The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper.</p> <p>Session timeout - Setting timeout for sessions can make the best utilization of network resources.</p>
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.

III-1-2 Filter Setup

Click Firewall and click Filter Setup to open the setup page.

Firewall >> Filter Setup

Filter Setup				Set to Factory Default	
Set	Comments	Set	Comments		
1.	Default Call Filter	7.			
2.	Default Data Filter	8.			
3.		9.			
4.		10.			
5.		11.			
6.		12.			

To edit or add a filter, click on the set number to edit the individual set. The following page will be shown. Each filter set contains up to 7 rules. Click on the rule number button to edit each rule. Check **Active** to enable the rule.

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1

Comments :

Rule	Active	Comments	Direction	Src IP	Dst IP	Service Type	Action	CSM	Move Up	Move Down
1	<input checked="" type="checkbox"/>	Block NetBios	LAN/DMZ/RT/VPN -> WAN	Any	Any	TCP/UDP, Port: from 137~139 to any	Block Immediately			Down
2	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
3	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
4	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
5	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
6	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
7	<input type="checkbox"/>		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	

Filter Set 1 2 3 4 5 6 7 8 9 10 11 12

Next Filter Set

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

Available settings are explained as follows:

Item	Description
Filter Rule	Click a button numbered (1 ~ 7) to edit the filter rule. Click the button will open Edit Filter Rule web page. For the detailed information, refer to the following page.
Active	Enable or disable the filter rule.
Comment	Enter filter set comments/description. Maximum length is 23-character long.
Direction	Display the direction of packet.
Src IP / Dst IP	Display the IP address of source /destination.
Service Type	Display the type and port number of the packet.

Action	Display the packets to be passed /blocked.
CSM	Display the content security managed
Move Up/Down	Use Up or Down link to move the order of the filter rules.
Next Filter Set	Set the link to the next filter set to be executed after the current filter run. Do not make a loop with many filter sets.
Wizard Mode	Allow to configure frequently used settings for filter rule via several setting pages.
Advance Mode	Allow to configure detailed settings of filter rule.

To use Wizard Mode, simple do the following steps:

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

Firewall >> Edit Filter Set >> Edit Filter Rule Wizard

Filter Set 1 Rule 1

Firewall Rule applies to packets that meet the following criteria

Comments:

Direction:

Source IP:

Start IP Address

End IP Address

Subnet Mask

Destination IP:

Start IP Address

End IP Address

Subnet Mask

Protocol:

Source Port ~

Destination Port ~

Available settings are explained as follows:

Item	Description
Comments	Enter filter set comments/description. Maximum length is 14- character long.
Direction	Set the direction of packet flow. It is for Data Filter only. For the Call Filter , this setting is not available since Call Filter is only applied to outgoing traffic. Note: RT means routing domain for 2nd subnet or other LAN.
Source/Destination IP	To set the IP address manually, please choose Any Address/Single Address/Range Address/Subnet Address as the Address Type and enter them in this field.
Protocol	Specify the protocol(s) which this filter rule will apply to.
Source Port / Destination Port	(=) - when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type.

	<p>(!=) - when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.</p> <p>(>) - the port number greater than this value is available.</p> <p>(<) - the port number less than this value is available for this profile.</p>
--	---

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

Firewall >> Edit Filter Set >> Edit Filter Rule Wizard

Filter Set 1 Rule 1

Based on the settings in the previous pages, we guess you want to have: **Pass**

The current setting is :

☒ Pass Immediately

URL Content Filter: None

☐ Block Immediately

Available settings are explained as follows:

Item	Description
Pass Immediately	<p>Packets matching the rule will be passed immediately.</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>
Block Immediately	Packets matching the rule will be dropped immediately.

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

Firewall >> Edit Filter Set >> Edit Filter Rule Wizard

Filter Set 1 Rule 1 Configuration Summary

Comments :	Block NetBios
Direction	
LAN/RT/VPN -> WAN	
Criteria	
Source IP	Any
Destination IP	Any
Protocol	TCP/UDP, Port: from 137 ~ 139 to any
More options	
Pass Immediately	URL Content Filter : None

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

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

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

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 1

☒ Enable

Comments: Block NetBios

Schedule Profile: None, None, None, None
☐ Clear sessions when schedule is ON

Direction: LAN/RT -> WAN **Advanced**

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 / 10000	<input type="checkbox"/>
MAC Bind IP	Non-Strict	<input type="checkbox"/>
URL Content Filter	None	<input type="checkbox"/>

Advance Setting **Edit**

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable the filter rule.
Comments	Enter filter set comments/description. Maximum length is 14- character long.
Schedule Profile	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. Note: RT means routing domain for 2nd subnet or other LAN.
Source/Destination IP	Click Edit to access into the following dialog to choose the source/destination IP or IP ranges.

To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose **Group and Objects** as the Address Type.

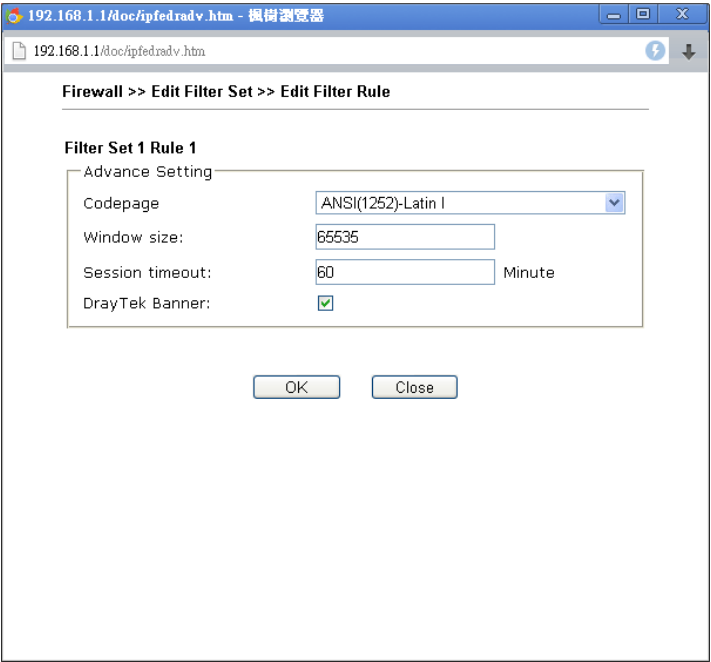
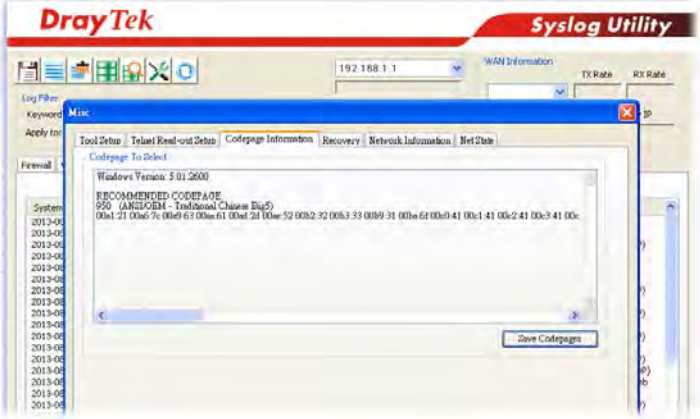
From the **IP Group** drop down list, choose the one that you want to apply. Or use the **IP Object** drop down list to choose the object that you want.

Service Type

Click **Edit** to access into the following dialog to choose a suitable service type.

To set the service type manually, please choose **User defined** as the Service Type and type them in this dialog. In addition, if you want to use the service type from defined groups or objects, please choose **Group and Objects** as the Service Type.

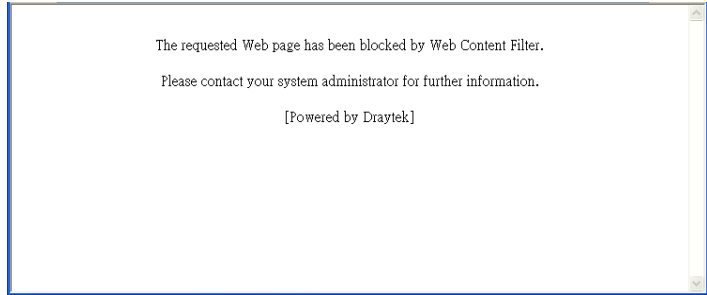
	<div> <div>User defined</div> <div> <div>User defined</div> <div>Group and Objects</div> </div> </div> <p>Protocol - Specify the protocol(s) which this filter rule will apply to.</p> <p>Source/Destination Port -</p> <p>(=) - when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type.</p> <p>(!=) - when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.</p> <p>(>) - the port number greater than this value is available.</p> <p>(<) - the port number less than this value is available for this profile.</p> <p>Service Group/Object - Use the drop down list to choose the one that you want.</p>
Fragments	<p>Specify the action for fragmented packets. And it is used for Data Filter only.</p> <p><i>Don't care</i> -No action will be taken towards fragmented packets.</p> <p><i>Unfragmented</i> -Apply the rule to unfragmented packets.</p> <p><i>Fragmented</i> - Apply the rule to fragmented packets.</p> <p><i>Too Short</i> - Apply the rule only to packets that are too short to contain a complete header.</p>
Filter	<p>Specifies the action to be taken when packets match the rule.</p> <p>Block Immediately - Packets matching the rule will be dropped immediately.</p> <p>Pass Immediately - Packets matching the rule will be passed immediately.</p> <p>Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped.</p> <p>Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through.</p>
Branch to other Filter Set	<p>If the packet matches the filter rule, the next filter rule will branch to the specified filter set. Select next filter rule to branch from the drop-down menu. Be aware that the router will apply the specified filter rule for ever and will not return to previous filter rule any more.</p>
Sessions Control	<p>The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.</p>
MAC Bind IP	<p>Strict - Make the MAC address and IP address settings configured in IP Object for Source IP and Destination IP are bound for applying such filter rule.</p> <p>Non-Strict - no limitation.</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</p>

	<p>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>
Advance Setting	<p>Click Edit to open the following window. However, it is strongly recommended to use the default settings here.</p>  <p>Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage.</p> <p>If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.</p>  <p>Window size - It determines the size of TCP protocol (0~65535). The more the value is, the better the performance will be. However, if the network is not stable,</p>

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.



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

III-1-3 Defense Setup

As a sub-functionality of IP Filter/Firewall, there are 15 types of detect/ defense function in the DoS Defense setup. The DoS Defense functionality is disabled for default.

III-1-3-1 DoS Defense

Click Firewall and click Defense Setup to open the setup page.

Firewall >> Defense Setup

DoS Defense

Spoofing Defense

DoS defense

☐ Enable DoS Defense

Select All

White/Black List Option

Log:

Enable

☐ Enable SYN flood defense

Threshold

2000

packets / sec

Timeout

10

sec

☐ Enable UDP flood defense

Threshold

2000

packets / sec

Timeout

10

sec

☐ Enable ICMP flood defense

Threshold

250

packets / sec

Timeout

10

sec

☐ Enable Port Scan detection

Threshold

2000

packets / sec

☐ Block IP options

☐ Block TCP flag scan

☐ Block Land

☐ Block Tear Drop

☐ Block Smurf

☐ Block Ping of Death

☐ Block trace route

☐ Block ICMP fragment

☐ Block SYN fragment

☐ Block Unassigned Numbers

☐ Block Fraggle Attack

OK

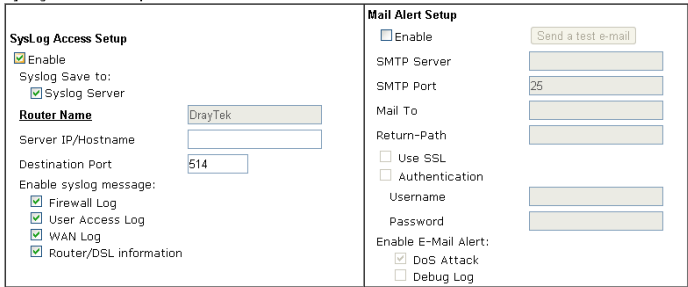
Clear All

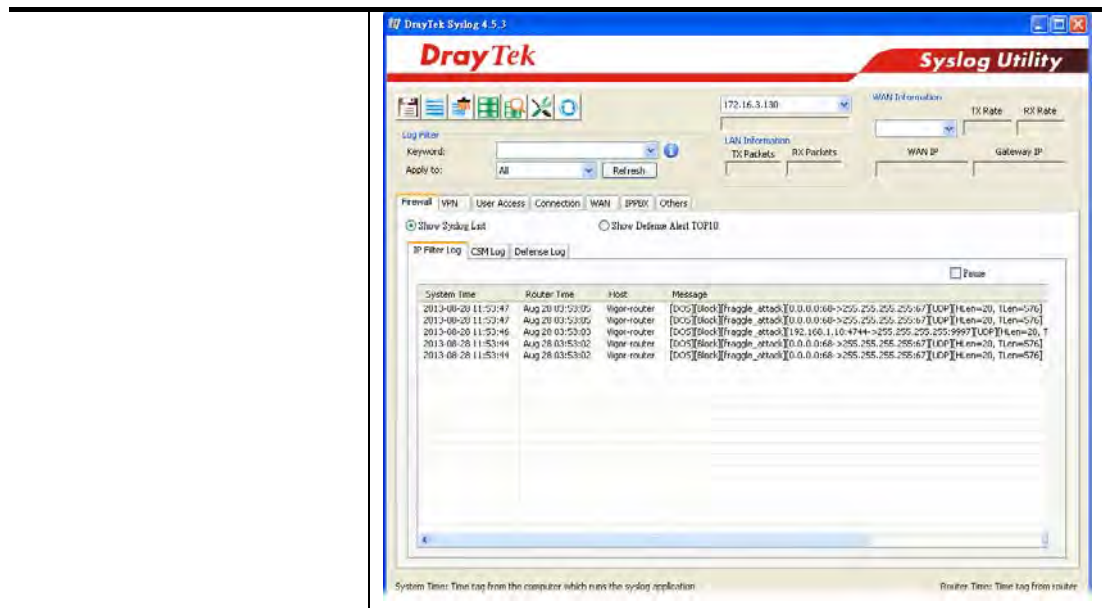
Cancel

Available settings are explained as follows:

Item	Description
Enable Dos Defense	Check the box to activate the DoS Defense Functionality. Select All - Click this button to select all the items listed below. White/Black List Option - Set white/black list of IPv4/IPv6 address.
Enable SYN flood defense	Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent TCP SYN packets for a period defined in Timeout. The goal for this is prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor router. By default, the threshold and timeout values are set to 2000 packets per second and 10 seconds, respectively. That means, when 2000 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.

Enable UDP flood defense	<p>Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent UDP packets for a period defined in Timeout.</p> <p>The default setting for threshold and timeout are 2000 packets per second and 10 seconds, respectively. That means, when 2000 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.</p>
Enable ICMP flood defense	<p>Check the box to activate the ICMP flood defense function. Similar to the UDP flood defense function, once if the Threshold of ICMP packets from Internet has exceeded the defined value, the router will discard the ICMP echo requests coming from the Internet.</p> <p>The default setting for threshold and timeout are 250 packets per second and 10 seconds, respectively. That means, when 250 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.</p>
Enable 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	<p>Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include <i>no flag scan</i>, <i>FIN without ACK scan</i>, <i>SYN FINscan</i>, <i>Xmas scan</i> and <i>full Xmas scan</i>.</p>
Block Tear Drop	<p>Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.</p>
Block Ping of Death	<p>Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.</p>
Block ICMP Fragment	<p>Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.</p>
Block Unassigned Numbers	<p>Check the box to activate the Block Unknown Protocol function. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and reject this kind of packets.</p>
Warning Messages	<p>We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client.</p> <p>All the warning messages related to DoS Defense will be sent to user and user can review it through Syslog daemon. Look for the keyword DoS in the message, followed by a name to indicate what kind of attacks is detected.</p> <p>System Maintenance >> SysLog / Mail Alert Setup</p> 



III-1-3-2 Spoofing Defense

Open Firewall >> Defense Setup and click Spoofing Defense to open the setup page.

Firewall >> Defense Setup

DoS Defense Spoofing Defense

ARP Spoofing Defense

- ☒ Block ARP replies with inconsistent source MAC addresses.
- ☒ Block ARP replies with inconsistent destination MAC addresses.
- ☒ Decline VRRP MAC into ARP table.

IP Spoofing Defense

- ☒ Block IP packet from WAN with inconsistent source IP addresses.
- ☐ Block IP packet from LAN with inconsistent source IP addresses.

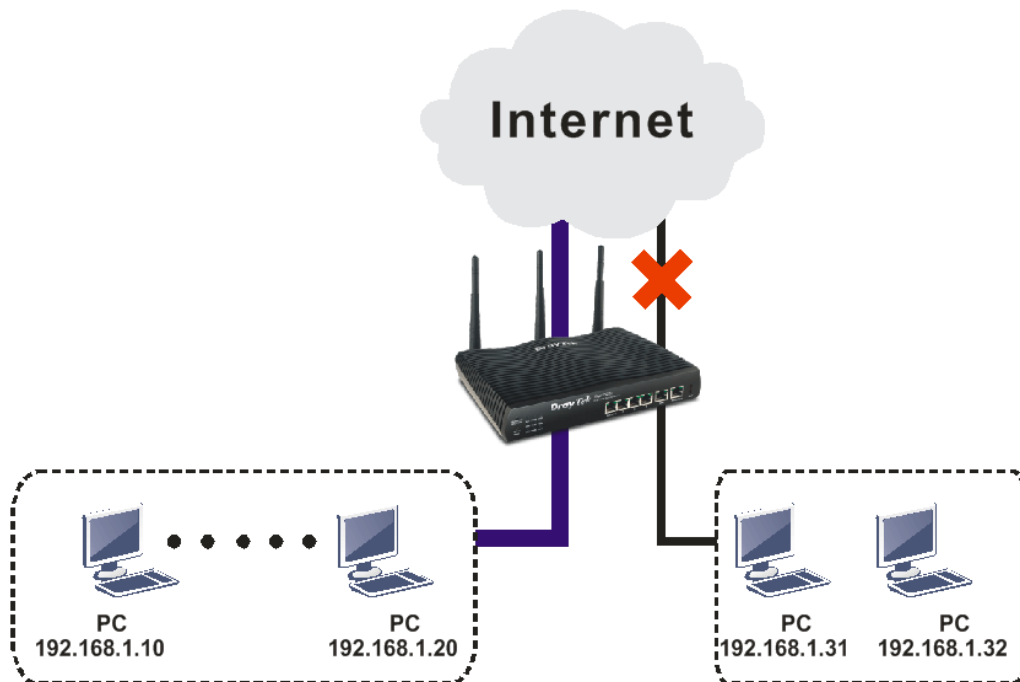
OK

Cancel

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.

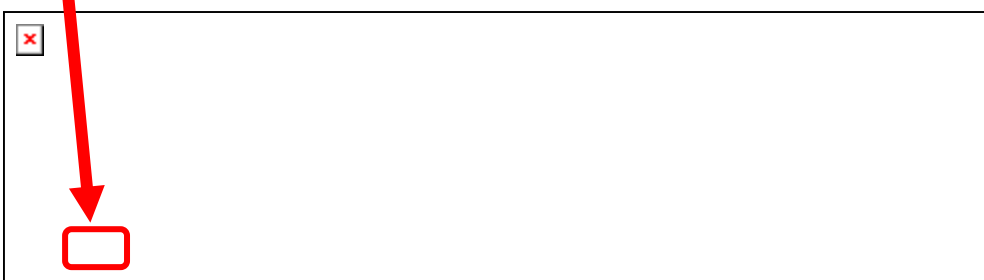


The way we can use is to set two rules under Firewall. For Rule 1 of Set 2 under Firewall>>Filter Setup is used as the default setting, we have to create a new rule starting from Filter Rule 2 of Set 2.

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: ☐

6. A dialog box will be popped up. Choose **Range Address** as **Address Type** by using the drop down list. Type 192.168.1.10 in the field of **Start IP**, and type 192.168.1.20 in the field of **End IP**. Then, click **OK** to save the settings. The computers within the range can access into the Internet.

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 ▼

7. Now, check the content of **Source IP** is correct or not. The action for **Filter** shall be set with **Pass Immediately**. Then, click **OK** to save the settings.

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

Destination IP: Any

Service Type: Any

Fragments: Don't Care ▼

Application

Filter: Action/Profile ▼

Branch to Other Filter Set: None ▼

Syslog ☐


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="text" value="1"/>	<input checked="" type="checkbox"/>	xNetBios -> DNS		<u>Down</u>
<input type="text" value="2"/>	<input checked="" type="checkbox"/>	block_all	<u>UP</u>	<u>Down</u>
<input type="text" value="3"/>	<input checked="" type="checkbox"/>	open_ip	<u>UP</u>	<u>Down</u>
<input type="text" value="4"/>	<input type="checkbox"/>		<u>UP</u>	<u>Down</u>
<input type="text" value="5"/>	<input type="checkbox"/>		<u>UP</u>	<u>Down</u>
<input type="text" value="6"/>	<input type="checkbox"/>		<u>UP</u>	<u>Down</u>
<input type="text" 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.

III-2 Central Security Management (CSM)

CSM is an abbreviation of **Central Security Management** which is used to control URL content to reach a goal of security management.

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 User Interface

Objects Setting
CSM
URL Content Filter Profile
Applications

III-2-1 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>
<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: Either : URL Access Control First ▼ Log: None ▼

1.URL Access Control

☐ Enable URL Access Control
☐ Prevent web access from IP address

Action: Pass ▼

Group/Object Selections

Edit

☐ Exception List
 Edit

2.Web Feature

☐ Enable Web Feature Restriction

Action: Pass ▼

File Extension Profile: None ▼
☐ Cookie
☐ Proxy
☐ Upload

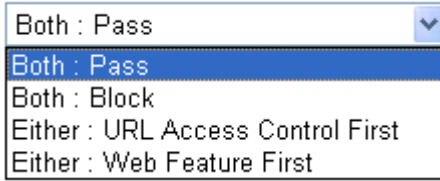
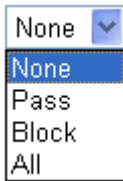
OK

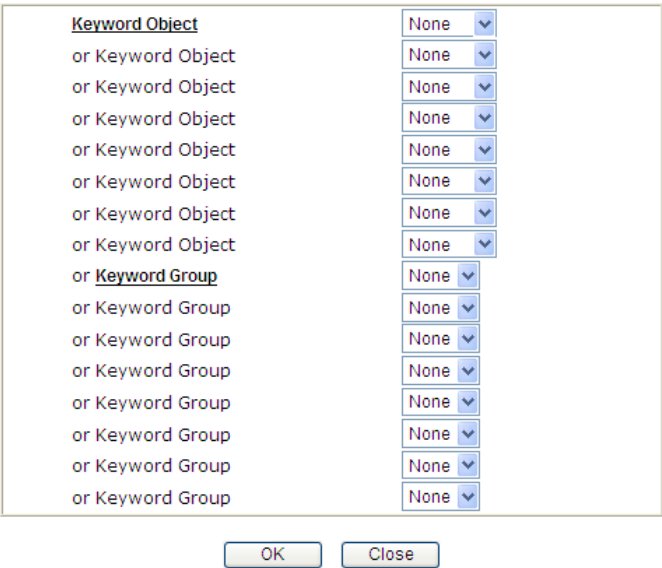
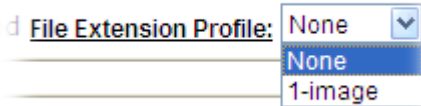
Clear

Cancel

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
Priority	<p>It determines the action that this router will apply.</p> <p>Both: Pass - The router will let all the packages that match with the conditions specified in URL Access Control and Web Feature below passing through. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.</p> <p>Both:Block -The router will block all the packages that match with the conditions specified in URL Access Control and Web Feature below. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.</p> <p>Either: URL Access Control First - When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for URL first, then Web feature second.</p> <p>Either: Web Feature First -When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for</p>

	<p>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"> ● Pass - Allow accessing into the corresponding webpage with the keywords listed on the box below. ● Block - Restrict accessing into the corresponding webpage with the keywords listed on the box below. If the web pages do not match with the keyword set here, it will be processed with reverse action. <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>

	<p>Object/Group Edit</p> 
Web Feature	<p>Enable Restrict Web Feature - Check this box to make the keyword being blocked or passed.</p> <p>Action - This setting is available only when Either: URL Access Control First or Either: Web Feature First is selected.</p> <p>Pass - Allow accessing into the corresponding webpage with the keywords listed on the box below.</p> <p>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.</p> <p>Cookie - Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy.</p> <p>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.</p> <p>Upload - Check the box to block the file upload by way of web page.</p> <p>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.</p> 

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

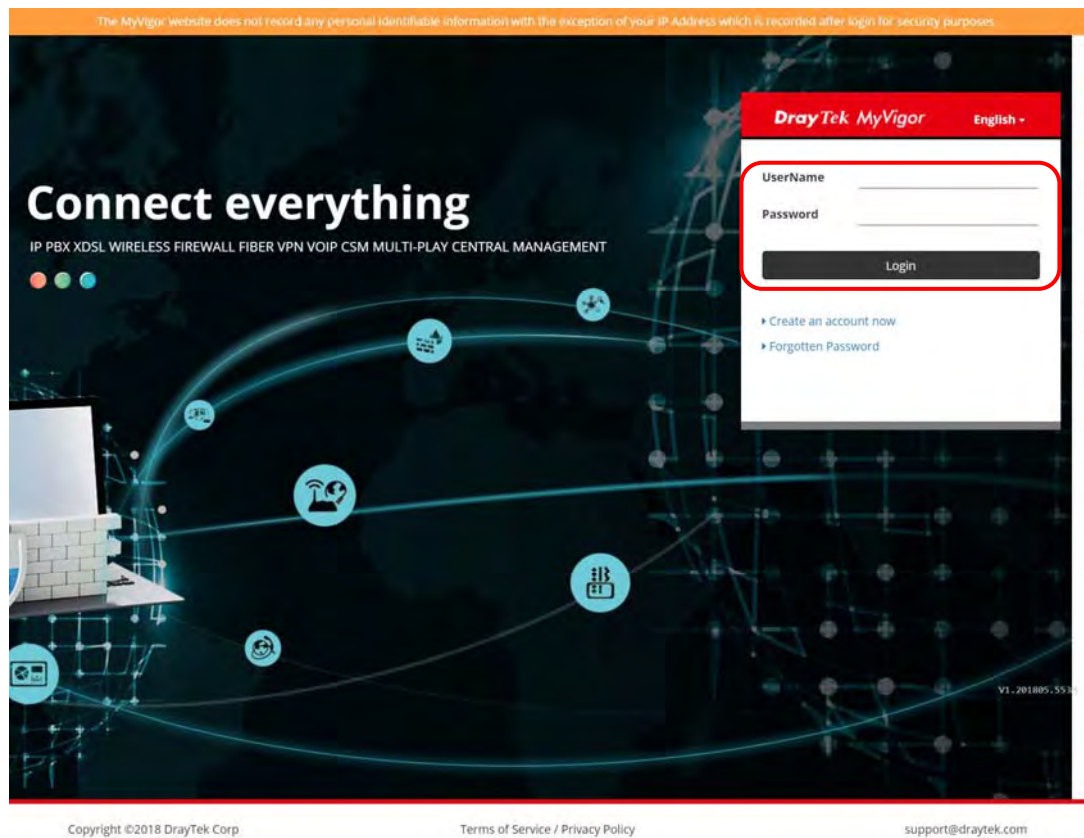
Application Notes

A-1 How to Create an Account for MyVigor

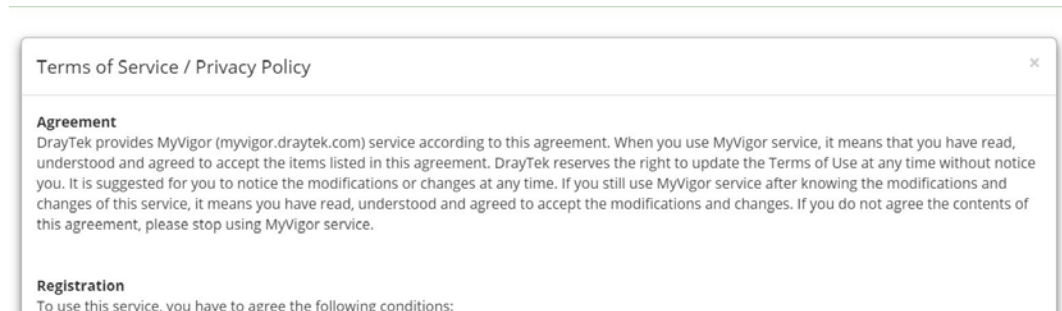
The website of MyVigor (a server located on <http://myvigor.draytek.com>) provides several useful services (such as Anti-Spam, Web Content Filter, Anti-Intrusion, and etc.) to filtering the web pages for the sake of protecting your system.

To access into MyVigor for getting more information, please create an account for MyVigor.

1. Access into <http://myvigor.draytek.com>.
2. A login page for MyVigor web site will pop up automatically.



3. Click the link of Create an account now.
4. The system will ask if you are 16 years old or over.
 - If yes, click I am 16 or over.



About Us
 DrayTek Corporation
 Address: No. 26, Fushing Rd., Hukou, Hsinchu Industrial Park, Hsinchu, 303, Taiwan
 Tel: + 886 3 5972727
 Fax: + 886 3 5972121
 Personal Data Related Issue: privacy@draytek.com
 Data Protection Officer: dpo@draytek.com

DrayTek Corp.
 Version: V3.5
 Date: 21 May, 2018

- If not, click I am under 16 years old to get the following page. Then, click I and my legal guardian agree.

THIS SECTION IS:

About Us
 DrayTek Corporation
 Address: No. 26, Fushing Rd., Hukou, Hsinchu Industrial Park, Hsinchu, 303, Taiwan
 Tel: + 886 3 5972727
 Fax: + 886 3 5972121
 Personal Data Related Issue: privacy@draytek.com
 Data Protection Officer: dpo@draytek.com

DrayTek Corp.
 Version: V3.5
 Date: 21 May, 2018

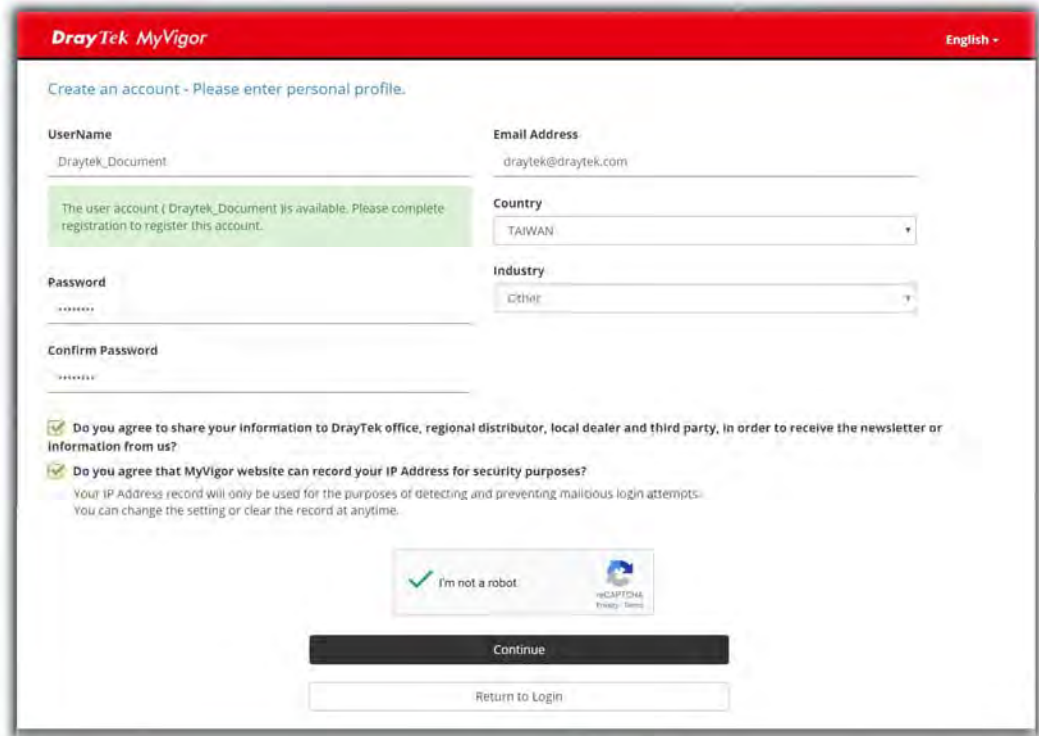
5. After reading the terms of service/privacy policy, click Agree.

THIS SECTION IS:

About Us
 DrayTek Corporation
 Address: No. 26, Fushing Rd., Hukou, Hsinchu Industrial Park, Hsinchu, 303, Taiwan
 Tel: + 886 3 5972727
 Fax: + 886 3 5972121
 Personal Data Related Issue: privacy@draytek.com
 Data Protection Officer: dpo@draytek.com

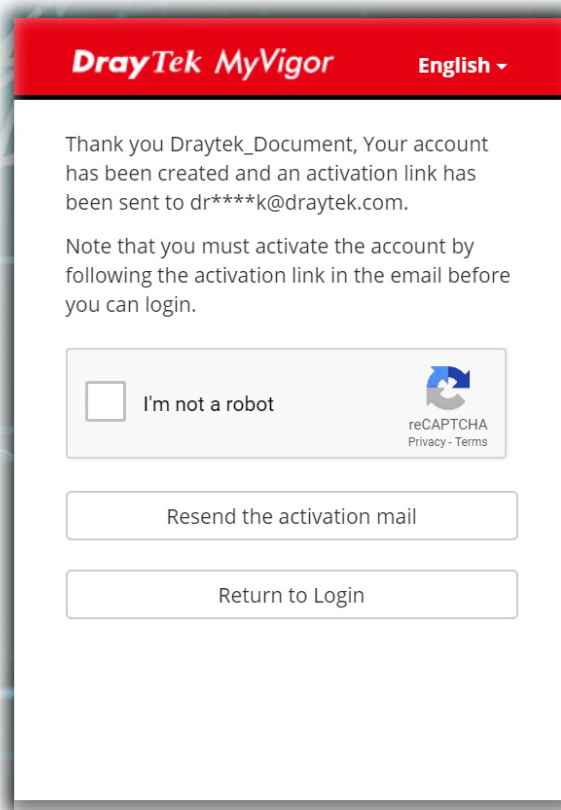
DrayTek Corp.
 Version: V3.5
 Date: 21 May, 2018

6. In the following page, enter your personal information in this page and then click **Continue**.



The image shows the 'Create an account' page of the DrayTek MyVigor website. The page has a red header with the 'DrayTek MyVigor' logo and a language dropdown set to 'English'. The main heading is 'Create an account - Please enter personal profile.' The form includes fields for 'UserName' (filled with 'Draytek_Document'), 'Email Address' (filled with 'draytek@draytek.com'), 'Country' (a dropdown menu showing 'TAIWAN'), 'Industry' (a dropdown menu showing 'Other'), 'Password', and 'Confirm Password'. A green message box states: 'The user account (Draytek_Document) is available. Please complete registration to register this account.' Below the form are two checkboxes for terms and conditions, a reCAPTCHA 'I'm not a robot' widget, and two buttons: 'Continue' and 'Return to Login'.

7. Choose proper selection for your computer and click **Continue**.



The image shows the account confirmation page of the DrayTek MyVigor website. The page has a red header with the 'DrayTek MyVigor' logo and a language dropdown set to 'English'. The main text reads: 'Thank you Draytek_Document, Your account has been created and an activation link has been sent to dr****k@draytek.com. Note that you must activate the account by following the activation link in the email before you can login.' Below the text is a reCAPTCHA 'I'm not a robot' widget. At the bottom are two buttons: 'Resend the activation mail' and 'Return to Login'.

8. Now you have created an account successfully. Click **START**.
9. Check to see the confirmation *email* with the title of **New Account Confirmation Letter from myvigor.draytek.com**.

***** This is an automated message from myvigor.draytek.com.*****

Thank you (**Mary**) for creating an account.

Please click on the activation link below to activate your account

Link : [Activate my Account](#)

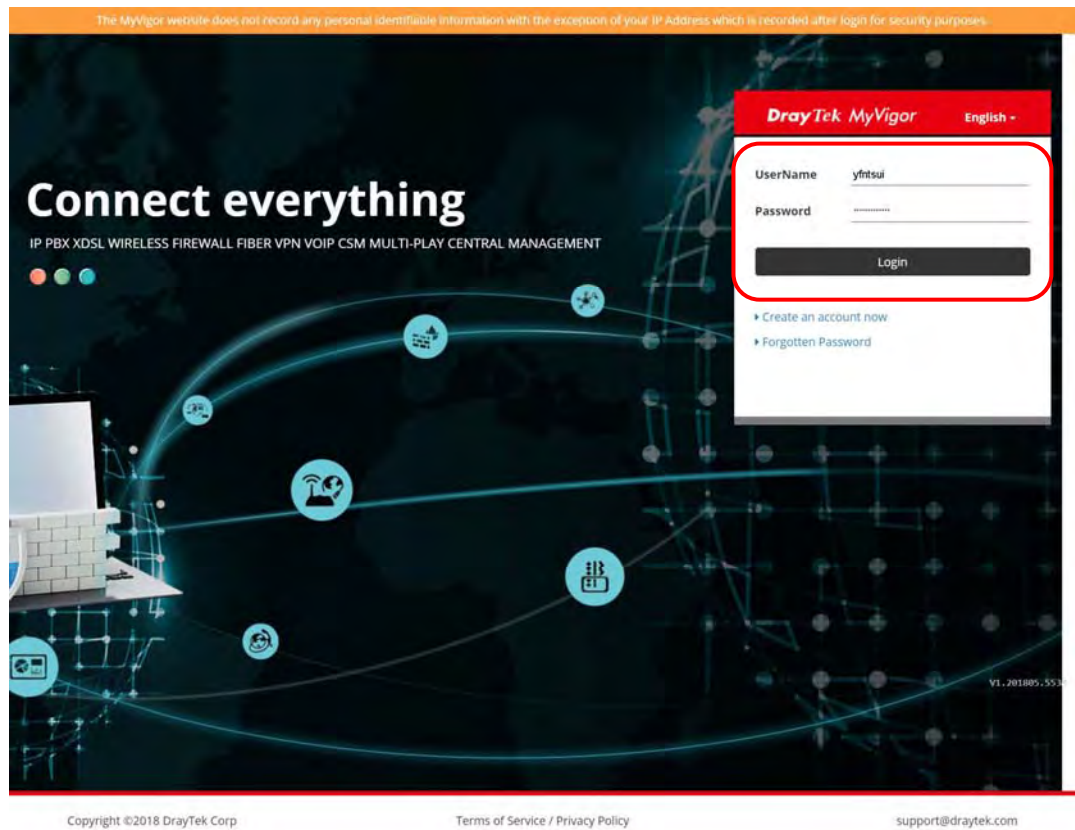
10. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.

Register Search for this site

Register Confirm

Thank for your register in VigorPro Web Site
The Register process is completed

11. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**.



12. Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

Part IV 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.

IV-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, Configuration Backup, Syslog /Mail Alert, Time and Date, Management, Self-Signed Certificate, Panel Control, Reboot System, and Firmware Upgrade.

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 : Vigor165
Firmware Version : 4.0.2 STD
Build Date/Time : Jan 21 2019 11:27:27

LAN				
MAC Address	1st IP Address	1st Subnet Mask	DHCP Server	DNS
LAN 00-1D-AA-93-7F-B4	192.168.1.1	255.255.255.0	ON	8.8.8.8

WAN					
Link Status	MAC Address	Connection	IP Address	Default Gateway	
WAN1 Disconnected	00-1D-AA-93-7F-B5	Static IP	0.0.0.0	0.0.0.0	

IPv6		
Address	Scope	Internet Access Mode
LAN FE80::A39:8A6B:7850:1758/64	Link	---

Available settings are explained as follows:

Item	Description
Model Name	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
Build Date/Time	Display the date and time of the current firmware build.
LAN	MAC Address - Display the MAC address of the LAN Interface. IP Address - Display the IP address of the LAN interface. Subnet Mask - Display the subnet mask address of the LAN interface. DHCP Server - Display the current status of DHCP server of the LAN interface. DNS - Display the assigned IP address of the primary DNS.
WAN	Link Status - Display current connection status. MAC Address - Display the MAC address of the WAN Interface. Connection - Display the connection type. IP Address - Display the IP address of the WAN interface. Default Gateway

	- Display the assigned IP address of the default gateway.
IPv6	<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>

IV-1-2 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through an Auto Configuration Server, e.g., VigorACS.

System Maintenance >> TR-069 Setting

ACS and CPE Settings

Export Parameters

TR-069

☒ Disable ☐ Enable

ACS Server On

Internet ▼

ACS Server


URL Wizard

☐ Acquire URL from DHCP option 43

Username Max: 31 characters

Password Max: 31 characters

Test With Inform Event Code PERIODIC ▼

Last Inform Response Time :(NA) 

CPE Client

Protocol ☒ HTTP ☐ HTTPS

URL

Port 8069

Username vigor

Password

Note: Please enable TR-069 server to allow access from Internet on [System Maintenance >> Management](#) page.

Periodic Inform Settings

☐ Enable ☒ Disable

Time Interval 900 second(s)

STUN Settings

☐ Enable ☒ Disable

Server Address

Server **STUN** Port 3478

Minimum Keep Alive Period 60 second(s)

Maximum Keep Alive Period -1 second(s)

OK Clear

Available settings are explained as follows:

Item	Description
TR-069	Click Enable to activate the settings on this page.
ACS Server On	Choose the interface for the router connecting to ACS server.
ACS Server	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 STUN 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>

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

IV-1-3 Administrator Password

This page allows you to set new password.

System Maintenance >> Administrator Password Setup

Administrator Password

Old Password	<input type="text" value="Max: 83 characters"/>
New Password	<input type="text" value="Max: 83 characters"/>
Confirm Password	<input type="text" value="Max: 83 characters"/>
<input type="checkbox"/> Enable 'admin' account login to Web UI from the Internet	

Note:

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

OK

Available settings are explained as follows:

Item	Description
Administrator Password	<p>Old Password - Type in the old password. The factory default setting for password is "admin".</p> <p>New Password -Type in new password in this field. The length of the password is limited to 23 characters.</p> <p>Confirm Password -Type in the new password again.</p> <p>Enable 'admin' account login to Web UI from the Internet - The default setting is enabled. It can ensure any user accessing into web user interface of Vigor router through Internet by username/password of "admin/admin".</p>

When you click OK, the login window will appear. Please use the new password to access into the web user interface again.

IV-1-4 Configuration Backup

Such function can be used to apply the router settings configured by Vigor165 to other Vigor device.

Backup the Configuration

Follow the steps below to backup your configuration.

1. Go to **System Maintenance >> Configuration Backup**. The following page will be popped-up, as shown below.

System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restore
Restore settings from a configuration file.

☒ 選擇檔案 未選擇檔案

☐ Restore configuration except the login password.

Note:
This will work only if the selected configuration file was created from this device.

Restore

Backup
Back up the current settings into a configuration file.

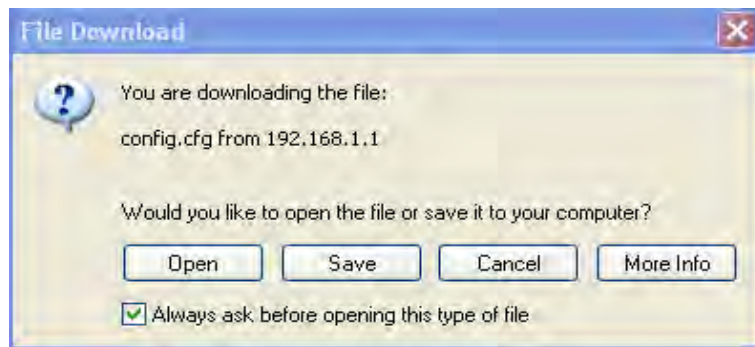
☐ Protect with password

Backup

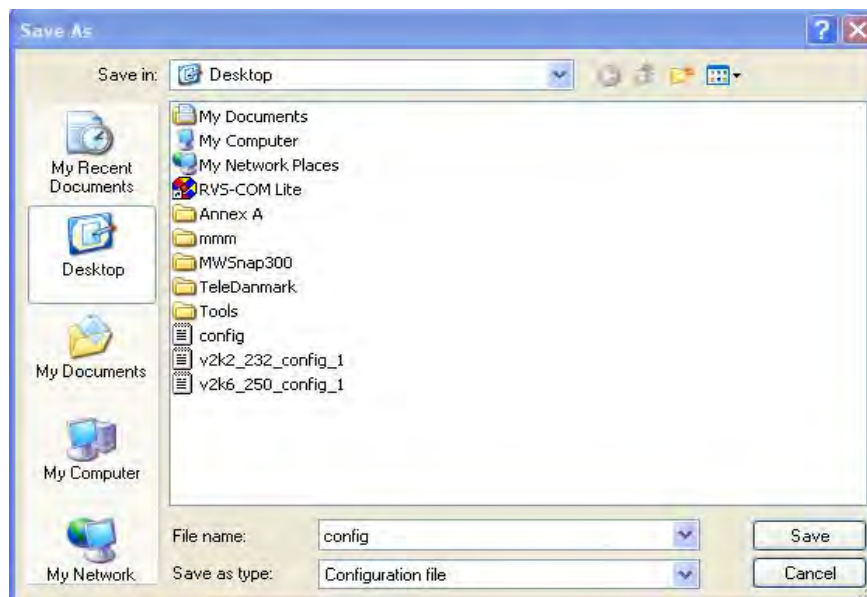
Available settings are explained as follows:

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 Vigor160, 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>
Backup	<p>Click it to perform the configuration backup of this router.</p> <p>Protect with password- For the sake of security, the configuration file for the router can be encrypted.</p> <div>Backup Back up the current settings into a configuration file. <input checked="" type="checkbox"/> Protect with password Password <input type="text"/> (Max. 23 characters allowed) Confirm Password <input type="text"/> (Max. 23 characters allowed) Backup</div> <p>Note: When loading a configuration file from a model in the Supported Model List please:</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.

2. Click **Backup** button to get into the following dialog. Click **Save** button to open another dialog for saving configuration as a file.



3. In Save As dialog, the default filename is **config.cfg**. You could give it another name by yourself.



4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

The above example is using **Windows** platform for demonstrating examples. The **Mac** or **Linux** platform will appear different windows, but the backup function is still available.



Info

Backup for Certification must be done independently. The Configuration Backup does not include information of Certificate.

Restore Configuration

1. Go to **System Maintenance >> Configuration Backup**. The following windows will be popped-up, as shown below.

Configuration Backup / Restoration

Restore Restore settings from a configuration file. <input checked="" type="radio"/> 選擇檔案 <input type="radio"/> 未選擇檔案 <input type="checkbox"/> Restore configuration except the login password. Note: This will work only if the selected configuration file was created from this device. <input type="button" value="Restore"/>
Backup Back up the current settings into a configuration file. <input type="checkbox"/> Protect with password <input type="button" value="Backup"/>

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.

IV-1-5 Syslog/Mail Alert

SysLog function is provided for users to monitor router.

System Maintenance >> SysLog / Mail Alert Setup

SysLog / Mail Alert Setup

SysLog Access Setup	Mail Alert Setup
<input type="checkbox"/> Enable	<input type="checkbox"/> Enable Send a test e-mail
Syslog Save to: <input checked="" type="checkbox"/> Syslog Server	SMTP Server <input type="text"/>
Router Name <input type="text" value="DrayTek"/>	SMTP Port <input type="text" value="25"/>
Server IP/Hostname <input type="text"/>	Mail To <input type="text"/>
Destination Port <input type="text" value="514"/>	Return-Path <input type="text"/>
Enable syslog message: <input checked="" type="checkbox"/> Firewall Log <input checked="" type="checkbox"/> User Access Log <input checked="" type="checkbox"/> WAN Log <input checked="" type="checkbox"/> Router/DSL information	<input type="checkbox"/> Use SSL <input type="checkbox"/> Authentication Username <input type="text"/> Password <input type="text"/>
	Enable E-Mail Alert: <input checked="" type="checkbox"/> DoS Attack <input type="checkbox"/> Debug Log

Available settings are explained as follows:

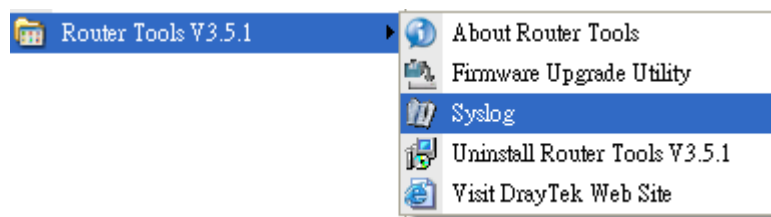
Item	Description
SysLog Access Setup	<p>Enable - Check Enable to activate function of syslog.</p> <p>Syslog Save to - Check Syslog Server to save the log to Syslog server.</p> <p>Check USB Disk to save the log to the attached USB storage disk.</p>
Router Name	<p>Display the name for such router configured 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 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>
--	---

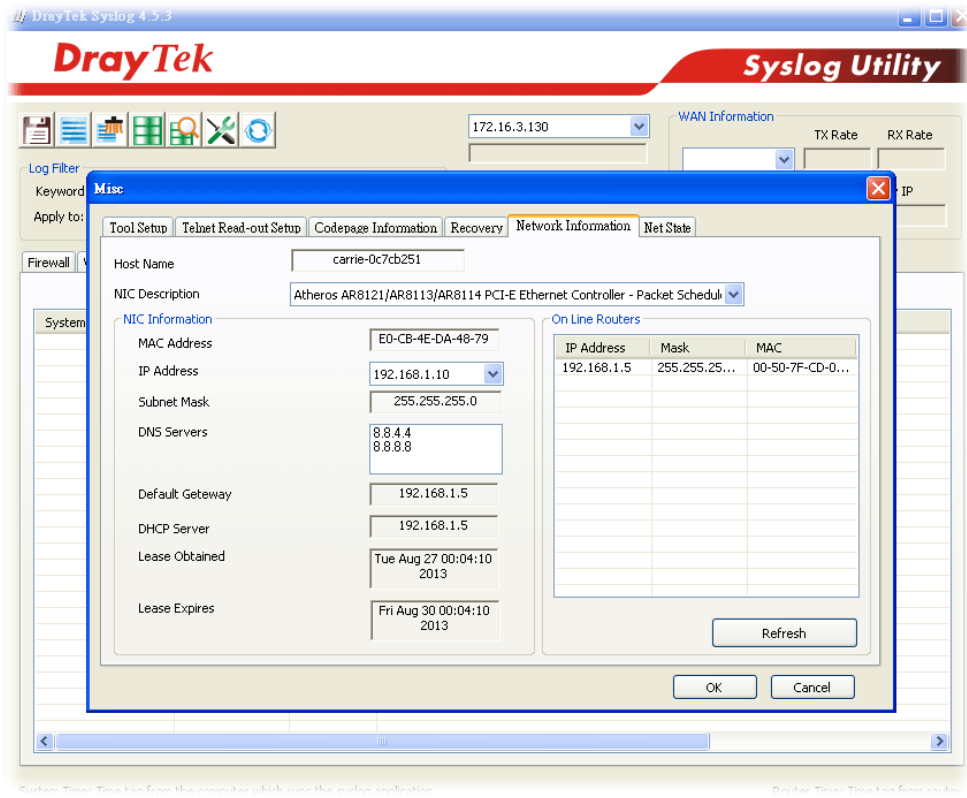
Click **OK** to save these settings.

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

IV-1-6 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

<input type="radio"/> Use Browser Time	
<input checked="" type="radio"/> Use Internet Time	
Time Server	pool.ntp.org
Priority	Auto
Time Zone	(GMT) Greenwich Mean Time : Dublin
Enable Daylight Saving	<input type="checkbox"/> Advanced
Automatically Update Interval	30 min
Send NTP Request Through	Auto

OK Cancel

Available settings are explained as follows:

Item	Description
Current System Time	Click Inquire Time to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.
Time Server	Type the web site of the time server.
Priority	Choose Auto or IPv6 First as the priority.
Time Zone	Select the time zone where the router is located.
Enable Daylight Saving	<p>Check the box to enable the daylight saving. Such feature is available for certain area.</p> <p>Advanced - Click it to open a pop up dialog.</p> <div>Daylight Saving Advanced <input checked="" type="radio"/> Default Start: No Daylight Saving End: No Daylight Saving <input type="radio"/> Date Range Start: Year Month Day 00 : 00 End: Year Month Day 00 : 00 <input type="radio"/> Yearly Start: Yearly On Januai First Sunda 00 : 00 End: Yearly On Januai First Sunda 00 : 00</div> <p>OK Close</p>
Automatically Update Interval	Select a time interval for updating from the NTP server.

Send NTP Request Through	Specify a WAN interface to send NTP request for time synchronization.
--------------------------	---

Click OK to save these settings.

IV-1-7 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
Router Name <input type="text" value="DrayTek"/>	
<input type="checkbox"/> Default: Disable Auto-Logout	Management Port Setup <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports
Internet Access Control <input type="checkbox"/> Allow management from the Internet Domain name allowed <input type="text"/>	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)
<input type="checkbox"/> FTP Server <input type="checkbox"/> HTTP Server <input checked="" type="checkbox"/> Enforce HTTPS Access <input checked="" type="checkbox"/> HTTPS Server <input type="checkbox"/> Telnet Server <input type="checkbox"/> TR069 Server <input type="checkbox"/> SSH Server <input checked="" type="checkbox"/> Disable PING from the Internet	SNMP Setup <input type="checkbox"/> Enable SNMP Agent Get Community <input type="text" value="public"/> Set Community <input type="text" value="private"/> Manager Host IP <input type="text"/> Trap Community <input type="text" value="public"/> Notification Host IP <input type="text"/> Trap Timeout <input type="text" value="10"/> seconds
LAN Access Control <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 <input checked="" type="checkbox"/> LAN1 <input checked="" type="checkbox"/> IP Routed Subnet	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
Access List from the Internet <input type="checkbox"/> Apply Access List to PING List IP Subnet Mask 1 <input type="text"/> <input type="text"/> <input type="text"/> 2 <input type="text"/> <input type="text"/> <input type="text"/> 3 <input type="text"/> <input type="text"/> <input type="text"/>	<input checked="" type="checkbox"/> Device Management <input type="checkbox"/> Respond to external device <input checked="" type="checkbox"/> Broadcast DSL status to router in LAN

OK

Available settings are explained as follows:

Item	Description
Router Name	Type in the router name provided by ISP.
Default: Disable Auto-Logout	If it is enabled, the function of auto-logout for web user interface will be disabled.

	 <p>The web user interface will be open until you click the Logout icon manually.</p>
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>
LAN Access Control	<p>Allow management from the LAN - Enable the checkbox to allow system administrators to login from LAN side. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.</p> <p>Apply To Subnet - Check the box(es) to apply the control to selected LAN port and/or IP routed subnet.</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>Apply Access List to PING - The behavior of this feature is related to the function of Disable PING from the Internet.</p> <p>When Disable PING from the Internet is disabled (unchecked) and Apply Access List to PING is enabled (checked), Vigor router will ping only the IPs list below (index in IP Object). When both Disable PING from the Internet and Apply Access List to PING are disabled (unchecked), Vigor router allows ping job of any IP.</p> <p>List IP - Indicate an IP address allowed to login to the modem.</p> <p>Subnet Mask - Represent a subnet mask allowed to login to the modem.</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>
SNMP Setup	<p>Enable SNMP Agent - Check it to enable this function..</p> <p>Get Community - Set the name for getting community by typing a proper character. The default setting is public.</p> <p>Set Community - Set community by typing a proper name. The default setting is private.</p> <p>Manager Host IP - Set one host as the manager to execute</p>

	<p>SNMP function. Please type in IPv4 address to specify certain host.</p> <p>Trap Community - Set trap community by typing a proper name. The default setting is public.</p> <p>Notification Host IP - Set the IPv4 address of the host that will receive the trap community.</p> <p>Trap Timeout - The default setting is 10 seconds.</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 Vigor device.</p> <p>Respond to external device - If it is enabled, Vigor device will be regarded as slave device. When the external device (master device) sends request packet to Vigor device, Vigor device would send back information to respond the request coming from the external device which is able to manage Vigor device.</p> <p>Broadcast DSL status to LAN - Clients in LAN can get current DSL connection status if such function is enabled.</p>

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

For IPv6

System Maintenance >> Management



IPv4 Management Setup	IPv6 Management Setup								
Management Access Control <input type="checkbox"/> Allow management from the Internet <input type="checkbox"/> Telnet Server (Port : 23) <input type="checkbox"/> HTTP Server (Port : 80) <input type="checkbox"/> Enforce HTTPS Access <input type="checkbox"/> HTTPS Server (Port : 443) <input type="checkbox"/> SSH Server (Port : 22) <input checked="" type="checkbox"/> Disable PING from the Internet IPv6 Address Security Option <input checked="" type="checkbox"/> Enable Random Interface Identifiers(IIDs) instead of EUI-64 IIDs									
Access List <table border="1"> <thead> <tr> <th>List</th> <th>IPv6 Address / Prefix Length</th> </tr> </thead> <tbody> <tr> <td>1.</td> <td><input type="text"/> / <input type="text"/></td> </tr> <tr> <td>2.</td> <td><input type="text"/> / <input type="text"/></td> </tr> <tr> <td>3.</td> <td><input type="text"/> / <input type="text"/></td> </tr> </tbody> </table>		List	IPv6 Address / Prefix Length	1.	<input type="text"/> / <input type="text"/>	2.	<input type="text"/> / <input type="text"/>	3.	<input type="text"/> / <input type="text"/>
List	IPv6 Address / Prefix Length								
1.	<input type="text"/> / <input type="text"/>								
2.	<input type="text"/> / <input type="text"/>								
3.	<input type="text"/> / <input type="text"/>								
Note: Telnet / Http server port is the same as IPv4.									
<input type="button" value="OK"/>									

Available settings are explained as follows:

Item	Description
Management Access	Allow management from the Internet - Enable the checkbox

certificate), subject alternative name type and relational settings for subject name. Then click **GENERATE**.

System Maintenance >> Regenerate Self-Signed Certificate

Regenerate Self-Signed Certificate

Certificate Name	self-signed
Subject Alternative Name	
Type	IP Address ▾
IP	<input type="text"/>
Subject Name	
Country (C)	<input type="text"/>
State (ST)	<input type="text"/>
Location (L)	<input type="text"/>
Organization (O)	<input type="text"/>
Organization Unit (OU)	<input type="text"/>
Common Name (CN)	<input type="text"/>
Email (E)	<input type="text"/>
Key Type	RSA ▾
Key Size	2048 Bit ▾

Generate

IV-1-9 Panel Control

The behavior of the Factory Reset button of the Vigor router can be customized as desired. The **Factory Reset** is enabled by default and can be enabled or disabled if required. Disabling the Factory Reset button will prevent tampering by unauthorized parties. Click the **Button** tab to get the following page.

System Maintenance >> Panel Control

Button

Refresh

Enable

Button

☒

Factory Reset

OK

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.

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

IV-1-10 Reboot System

The Web user interface may be used to restart your router. Click **Reboot System** from **System Maintenance** to open the following page.

System Maintenance >> Reboot System

Reboot System

Do you want to reboot your router ?

- ☒ Using current configuration
- ☐ Using factory default configuration

Reboot Now

Auto Reboot Time Schedule

Schedule Profile : None None None None

Note: Action and Idle Timeout settings will be ignored.

OK

Cancel

Schedule Profile - You can type in four sets of time schedule for performing system reboot. All the schedules can be set previously in **Applications >> Schedule** web page and you can use the number that you have set in that web page.

If you want to reboot the router using the current configuration, check **Using current configuration** and click **Reboot Now**. To reset the router settings to default values, check **Using factory default configuration** and click **Reboot Now**. The router will take 5 seconds to reboot the system.



Info

When the system pops up Reboot System web page after you configure web settings, please click Reboot Now to reboot your router for ensuring normal operation and preventing unexpected errors of the router in the future.

IV-1-11 Firmware Upgrade

Click **System Maintenance>> Firmware Upgrade** to proceed to firmware upgrade.

System Maintenance >> Firmware Upgrade



Web Firmware Upgrade

Select a firmware file.

選擇檔案

未選擇任何檔案

Click Upgrade to upload the file.

Upgrade

Preview

Note:

Upgrade using the ALL file will retain existing router configuration, whereas using the RST file will reset the configuration to factory defaults.

Click **Select** to specify the one you just download.

When the above page appears, click **Upgrade**. The system will upgrade the firmware of the router automatically.

Part V Others



Objects Settings

Define objects such as IP address, service type, keyword, file extension and others. These pre-defined objects can be applied in CSM.

V-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

Firewall
Objects Setting
IP Object
IP Group
IPv6 Object
IPv6 Group
Service Type Object
Service Type Group
Keyword Object
Keyword Group
File Extension Object
Objects Backup/Restore
CSM

V-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.			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](#) >>

[Objects Backup/Restore](#)

Available settings are explained as follows:

Item	Description
View	Use the drop down list to choose a type (Single Address, Range Address, Subnet Address, Mac Address or all) that IP object with the selected type will be shown on this page.
Set to Factory Default	Clear all 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.

To set a new profile, please do the steps listed below:


1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:

Objects Setting >> IP Object

Profile Index : 1

Name:	RD Department
Interface:	Any
Address Type:	Range Address
Mac Address:	00 : 00 : 00 : 00 : 00 : 00
Start IP Address:	192.168.1.59
End IP Address:	192.168.1.65
Subnet Mask:	
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/RT or any IP address. If you choose LAN/RT as the Interface here, and choose LAN/RT as the direction setting in Edit Filter Rule, then all the IP addresses specified with LAN/RT 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.</p> <p>Select Single Address if this object contains one IP address only.</p> <p>Select Range Address if this object contains several IPs within a range.</p> <p>Select Subnet Address if this object contains one subnet for IP address.</p>

	<p>Select Any Address if this object contains any IP address. Select Mac Address if this object contains Mac address.</p> <div> Range Address ▾ Any Address Single Address Range Address Subnet Address Mac Address </div>
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.

V-1-2 IP Group

This page allows you to bind several IP objects into one IP group.

Objects Setting >> IP Group

IP Group Table:

[Set to Factory Default](#)

Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

[Objects Backup/Restore](#)

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:	<input type="text"/>
Interface:	<input type="text" value="Any"/>
Available IP Objects	Selected IP Objects
<div>1-RD Department 2-Financial Dept 3-HR Department</div>	<div></div>
	<div>>> <<</div>

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.

V-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](#) >>

Objects Backup/Restore

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:	SubnetAddress ▾
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:	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.

V-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.	

[Objects Backup/Restore](#)

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

>>

<<

OK

Clear

Cancel

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.

V-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](#) >>

[Objects Backup/Restore](#)

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:

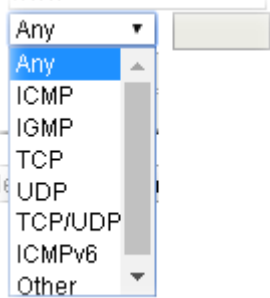
Objects Setting >> Service Type Object Setup

Profile Index : 1

Name	www	
Protocol	Any	
Source Port	= 1	~ 65535
Destination Port	= 1	~ 65535

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Protocol	Specify the protocol(s) which this profile will apply to. 
Source/Destination Port	<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>

V-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>	

[Objects Backup/Restore](#)

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: VoIP

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.

V-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](#) >>

Objects Backup/Restore

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	
<div>OK Clear Cancel</div>	

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.

V-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	Objects	Index	Name	Objects
1.			17.		
2.			18.		
3.			19.		
4.			20.		
5.			21.		
6.			22.		
7.			23.		
8.			24.		
9.			25.		
10.			26.		
11.			27.		
12.			28.		
13.			29.		
14.			30.		
15.			31.		
16.			32.		

[Objects Backup/Restore](#)

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all 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 (Up to 16)

>>


<<

OK

Clear

Cancel

Available settings are explained as follows:

Item	Description
Name	Type a name for this group. Maximum 15 characters are allowed.
Available Keyword Objects	You can gather keyword objects from Keyword Object page within one keyword group. All the available Keyword objects that you have created will be shown in this box.
Selected Keyword Objects	Click  button to add the selected Keyword objects in this box.

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

V-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>	

Objects Backup/Restore

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="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
<input type="button" value="Clear All"/>	
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="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
<input type="button" value="Clear All"/>	
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="checkbox"/> .ra <input type="checkbox"/> .ram <input type="checkbox"/> .vox <input type="checkbox"/> .wav <input type="checkbox"/> .wma
<input type="button" value="Clear All"/>	
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="checkbox"/> .jse <input type="checkbox"/> .jsp <input type="checkbox"/> .jtk
<input type="button" value="Clear All"/>	
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.

V-1-10 Objects Backup/Restore

All of the 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 objects at the same time.

Simply check the box for the object type that you want to backup.

Objects Setting >> Objects Backup/Restore

Backup
☐ Select All
☐ IP Object
☐ IP Group
☐ IPv6 Object
☐ IPv6 Group
☐ Service Type Object
☐ Service Type Group
☐ Keyword Object
☐ Keyword Group
☐ File Extension Object
☒ Backup the current IP Objects with a CSV file
☐ Download the default CSV template to edit

Restore
 未選擇檔案

Note:

For better compatibility, it's suggested to edit IP Objects with the provided default CSV template.

Available settings are explained as follows:

Item	Description
Backup	<ul style="list-style-type: none">● Backup the current IP Objects with a CSV file - Click it to backup current IP objects as a CSV file. Such file can be restored for future use.● Download the default CSV template to edit - After clicking it, press Download to store the default CSM template (a table without any input data) to your hard disk.● Download - Download the CSV file from Vigor router and store in your hard disk.
Restore	<p>Select - Click it to specify a predefined CSV file.</p> <p>Restore - Import the selected CSV file onto Vigor router.</p>

This page is left blank.

Part VI 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.

VI-1 Diagnostics

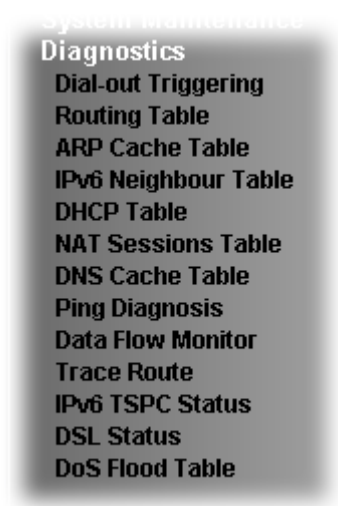
This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

- 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.

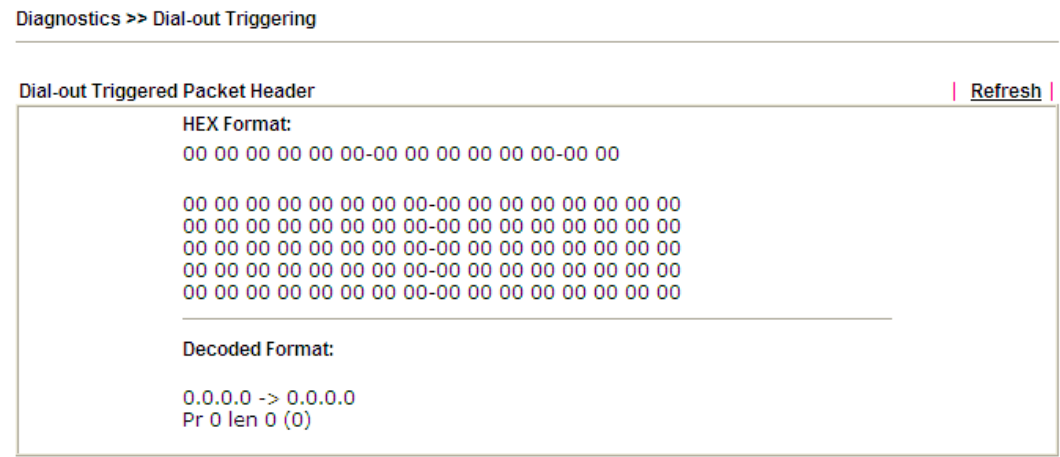
Web User Interface

Fisrt, take a look at the menu items under Diagnostics. Diagnostic Tools provide a useful way to view or diagnose the status of your Vigor router.



VI-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.



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.

VI-1-2 Routing Table

Click Diagnostics and click Routing Table to open the web page.

Diagnostics >> View Routing Table

IPv4 Routing Table

[Refresh](#)

Key	Destination	Gateway	Interface
C~	192.168.1.0/ 255.255.255.0	directly connected	LAN

Key

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

IPv6 Routing Table

☐ Show Detail | [Refresh](#)

Destination	Interface	Flags	Metric	Next Hop
FE80::/64	LAN1	U	256	::
FE80::/64	DMZ	U	256	::
FF00::/8	LAN1	U	256	::
FF00::/8	DMZ	U	256	::

Flag

U: Route UP F: Default Route G: Use Next Hop S: Static Route R: RIPng

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

VI-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

Ethernet ARP Cache Table

Clear

Refresh

IP Address	MAC Address	HOST ID	Port
192.168.1.5	60-A4-4C-E6-5A-4F		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.

VI-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.

VI-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

DHCP IP Assignment Table

[Refresh](#)

DHCP server: Running				
Index	IP Address	MAC Address	Leased Time	HOST ID

☐ Show Comment

DHCPv6 IP Assignment Table

[Refresh](#)

DHCPv6 server binding client:				
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.

VI-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.

VI-1-7 DNS Cache Table

Click **Diagnostics** and click **DNS Cache Table** to open the web page.

The record of domain Name and the mapping IP address for answering the DNS query from LAN will be stored on Vigor router's Cache temporarily and displayed on **Diagnostics >> DNS Cache Table**.

Diagnostics >> DNS Cache Table

IPv4 DNS Cache Table

ClearRefresh

Domain Name	IP Address	TTL (s)
-------------	------------	---------

IPv6 DNS Cache Table

ClearRefresh

Domain Name	IP Address	TTL (s)
-------------	------------	---------

Note:
The LAN DNS entry's TTL is static.

☐ When an entry's TTL is larger than s, this entry will be deleted from the table.

OK

Available settings are explained as follows:

Item	Description
Clear	Click this link to remove the result on the window.
Refresh	Click it to reload the page.
When an entry's TTL is larger than....	Check the box the type the value of TTL (time to live) for each entry. Click OK to enable such function. It means when the TTL value of each DNS query reaches the threshold of the value specified here, the corresponding record will be deleted from router's Cache automatically.

VI-1-8 Ping Diagnosis

Click Diagnostics and click Ping Diagnosis to open the web page.

Diagnostics >> Ping Diagnosis

Ping Diagnosis

The screenshot shows the 'Ping Diagnosis' web interface for IPv4. At the top, there are radio buttons for 'IPV4' (selected) and 'IPV6'. Below them is a 'Source IP' dropdown menu set to 'Auto'. The 'Ping to' dropdown menu is open, showing options: 'Host / IP' (selected), 'DNS', and 'Gateway'. To the right of the dropdown is an 'IP Address' text input field. Below the dropdown is a 'Run' button. At the bottom, there is a 'Result' label and a large empty text area for displaying results. A 'Clear' link is located at the bottom right of the result area.

or

Diagnostics >> Ping Diagnosis

Ping Diagnosis

The screenshot shows the 'Ping Diagnosis' web interface for IPv6. At the top, there are radio buttons for 'IPV4' and 'IPV6' (selected). Below them is a 'Ping IPv6 Address' text input field. To the right of the input field is a 'Run' button. At the bottom, there is a 'Result' label and a large empty text area for displaying results. A 'Clear' link is located at the bottom right of the result area.

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.

VI-1-9 Data Flow Monitor

This page displays the running procedure for the IP address monitored and refreshes the data in an interval of several seconds.

Click **Diagnostics** and click **Data Flow Monitor** to open the web page. You can click **IP Address**, **TX rate**, **RX rate** or **Session** link for arranging the data display.


Diagnostics >> Data Flow Monitor

[illegible]

Note:

1. Click "Block" to prevent specified PC from surfing Internet for 5 minutes.
2. The IP blocked by the router will be shown in red, and the session column will display the remaining time that the specified IP will be blocked.
3. When Data Flow Monitor is enabled, the function of Hardware Acceleration will not take effect, if it is enabled, to prevent from session conflicts.
4. (Kbps): shared bandwidth
+ : residual bandwidth used
Current/Peak are average.

Available settings are explained as follows:

Item	Description
Enable Data Flow Monitor	Check this box to enable this function.
Refresh Seconds	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically. Refresh Seconds: 
Refresh	Click this link to refresh this page manually.
Index	Display the number of the data flow.
IP Address	Display the IP address of the monitored device.
TX rate (kbps)	Display the transmission speed of the monitored device.
RX rate (kbps)	Display the receiving speed of the monitored device.
Sessions	Display the session number that you specified in Limit Session web page.

Action	<p>Block - can prevent specified PC accessing into Internet within 5 minutes.</p> <p>Unblock -The device with the IP address will be blocked for five minutes. The remaining time will be shown on the session column. Click it to cancel the IP address blocking.</p>
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>

VI-1-10 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:

Run

Result

Clear

or

Diagnostics >> Trace Route

Trace Route

☐ IPv4

☒ IPv6

Trace Host / IP Address:

Run

Result

Clear

Available settings are explained as follows:

Item	Description
IPv4 / IPv6	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.

VI-1-11 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:0000:0000:10b9 Router DNS name : 88886666.broker.freenet6.net Remote Endpoint v4 Address : 81.171.72.11 Remote Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:10b8 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.

VI-1-12 DSL Status

DSL status web page could help you to diagnose the connection status of DSL.

Diagnostics >> DSL Status

General	Tone Information	Refresh
ATU-R Information Type: ADSL2/2+ Hardware: Annex A Firmware: 08-08-00-0F-00-07 Power Mngt Mode: DSL_G997_PMS_NA Line State: TRAINING Running Mode: Vendor ID: fe004452 41590000		
ATU-C Information Vendor ID: 00000000 00000000 [-----]		
Line Statistics		
	Downstream	Upstream
Actual Rate	0 Kbps	0 Kbps
Attainable Rate	0 Kbps	0 Kbps
Path Mode	Fast	Fast
Interleave Depth	0	0
Actual PSD	0.0 dB	0.0 dB

VI-1-13 DoS Flood Table

This page can display content of IP connection detected by DoS Flooding Defense mechanism. It is useful and convenient for network engineers (e.g., MIS engineer) to inspect the network environment to find out if there is any abnormal connection.

Information of IP traced and destination port used for SYN Flood, UDP Flood and ICMP Flood attacks will be detected and shown respectively on different pages.

Moreover, IP address detected and suspected to attack the network system can be blocked shortly by clicking the **Block** button shown on pages of SYN Flood, UDP Flood and ICMP Flood.

Diagnostics >> DoS Flood Table

IPv4

SYN Flood	UDP Flood	ICMP Flood	Refresh				
<table><tr><th>Tracing IP</th><th>Destination Port</th></tr><tr><td colspan="2">.....</td></tr></table>				Tracing IP	Destination Port	
Tracing IP	Destination Port						
.....							

IPv6

SYN Flood	UDP Flood	ICMP Flood	Refresh				
<table><tr><th>Tracing IP</th><th>Destination Port</th></tr><tr><td colspan="2">.....</td></tr></table>				Tracing IP	Destination Port	
Tracing IP	Destination Port						
.....							

Note:
You need to enable SYN/UDP/ICMP flood defense in [Firewall >> Defense Setup](#) to make this table effective.



Info

The icon - (⊗) - means there is something wrong (e.g., attacking the system) with that IP address.

VI-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.

VI-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.

All Programs

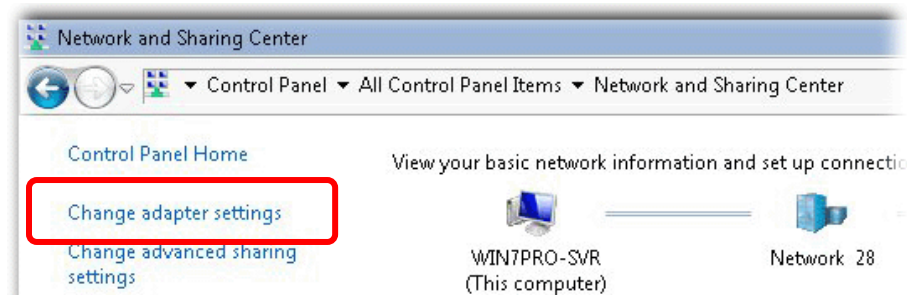
Getting Started

Network and Sharing Center

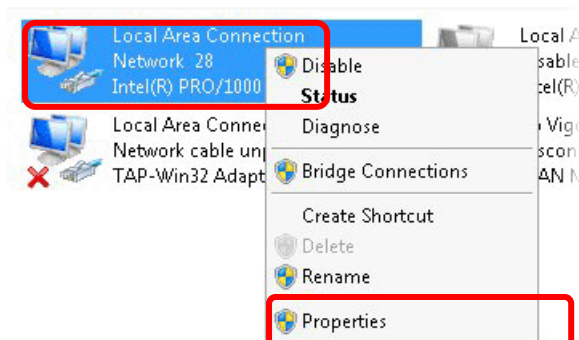
Personalization

Recovery

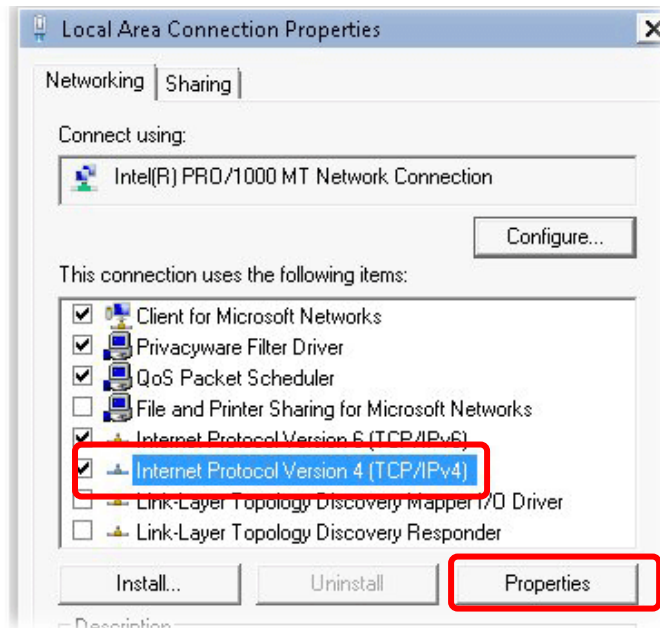
2. In the following window, click Change adapter settings.



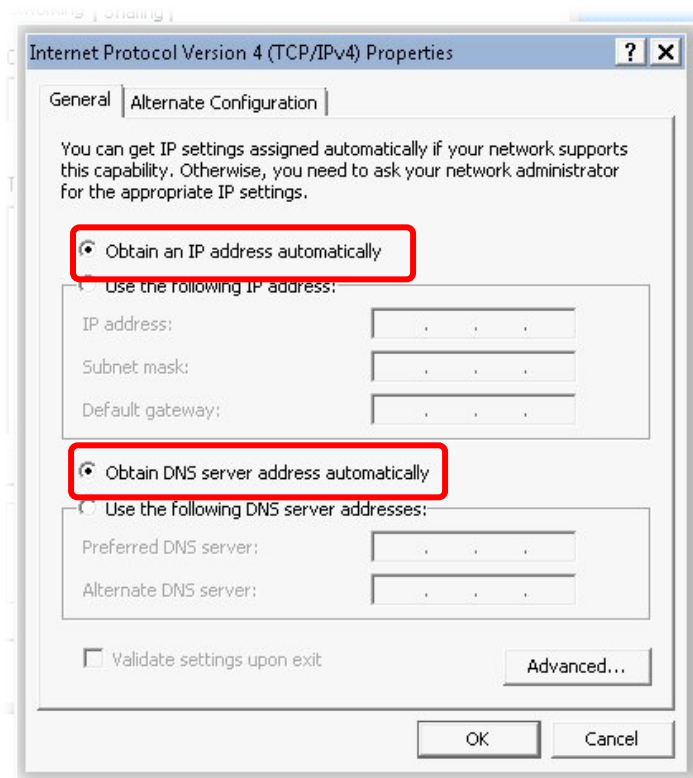
3. Icons of network connection will be shown on the window. Right-click on Local Area Connection and click on Properties.



4. Select **Internet Protocol Version 4 (TCP/IP)** and then click **Properties**.

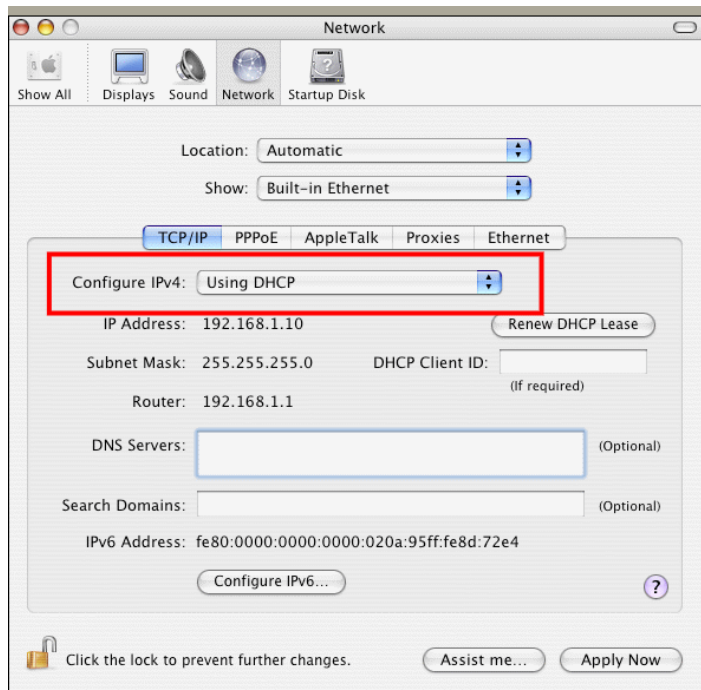


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



For Mac OS

1. Double click on the current used Mac OS on the desktop.
2. Open the **Application** folder and get into **Network**.
3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.



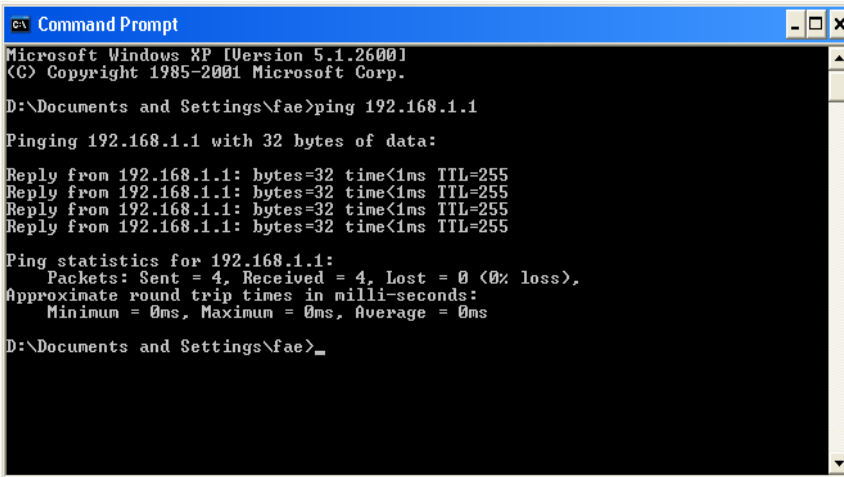
VI-4 Pinging the Router from Your Computer

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.



```

C:\ Command Prompt
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 ttty1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$
```

VI-5 Checking If the ISP Settings are OK or Not

If WAN connection cannot be up, check if the LEDs (according to the LED explanations listed on section I-1-1) are correct or not. If the LEDs are off, please:

- Change the **Physical Type** from **Auto negotiation** to other values (e.g., 100M full duplex).
- Next, 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 **Internet Access** page and then check whether the ISP settings are set correctly.

VI-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

Schedule Profile : None, None, None, None

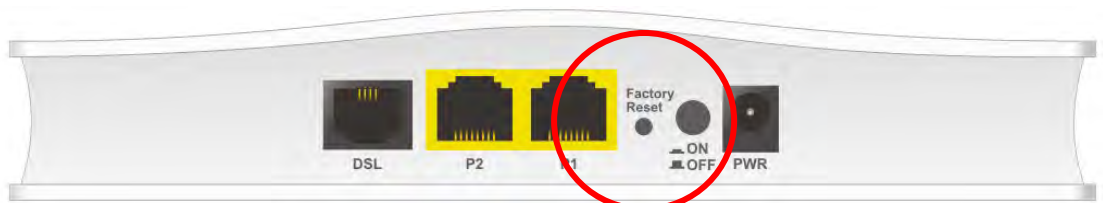
Note: Action and Idle Timeout settings will be ignored.

OK

Cancel

Hardware Reset

While the router is running (ACT LED blinking), press the **Factory Reset** button and hold for more than 5 seconds. When you see the **ACT LED** blinks rapidly, please release the button. Then, the router will restart with the default configuration.



After restore the factory default setting, you can configure the settings for the router again to fit your personal request.

VI-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.

Part IX Telnet Commands

Accessing Telnet of Vigor Device

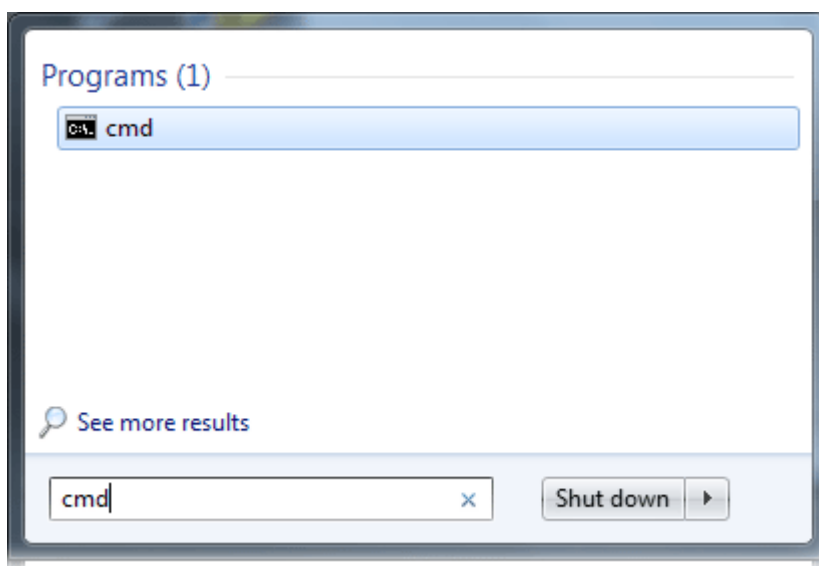
This chapter also gives you a general description for accessing telnet and describes the firmware versions for the routers explained in this manual.



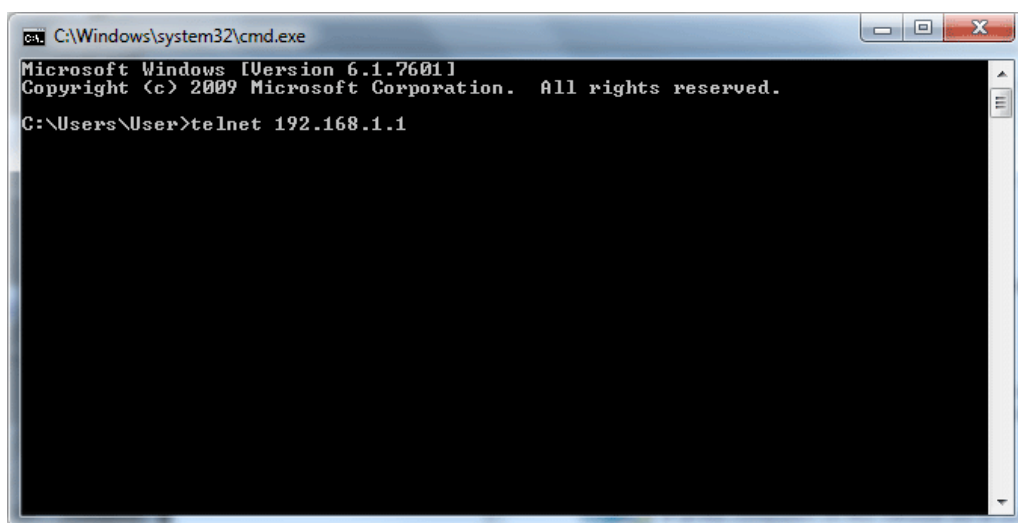
Info

For Windows 7 user, please make sure the Windows Features of Telnet Client has been turned on under **Control Panel>>Programs**.

Type `cmd` and press Enter. The Telnet terminal will be open later.

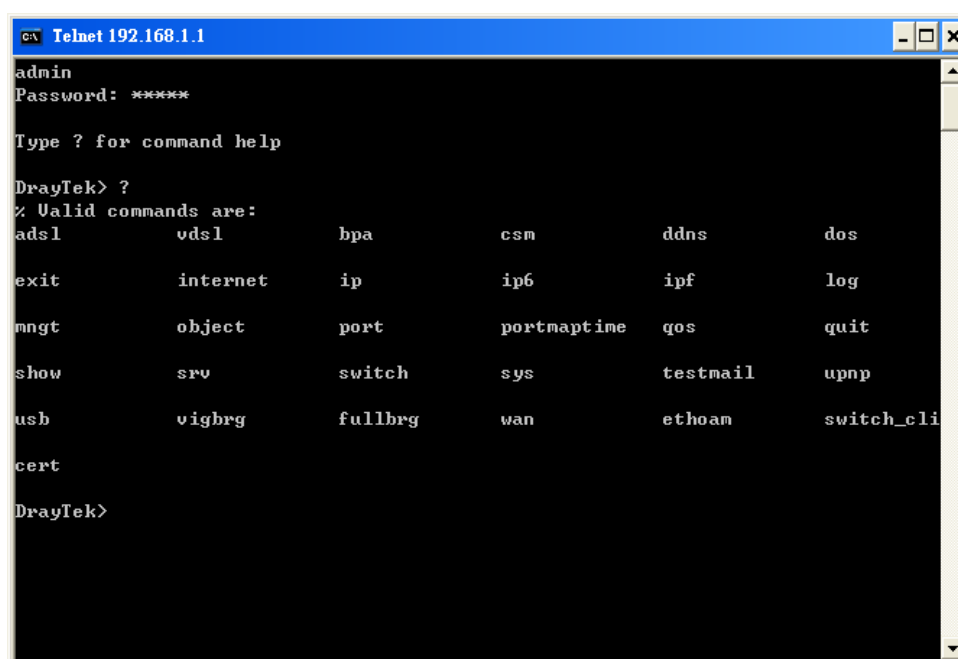
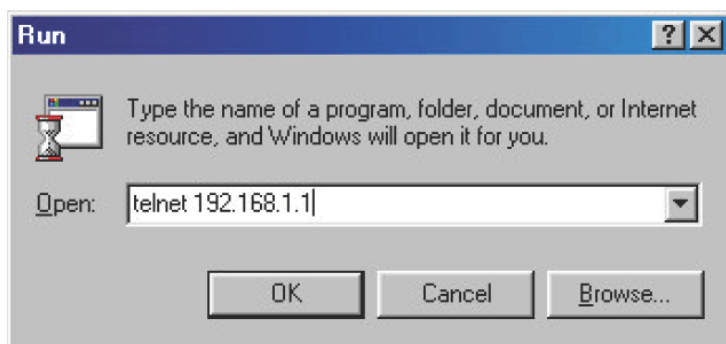


In the following window, type `Telnet 192.168.1.1` as below and press Enter. Note that the IP address in the example is the default address of the router. If you have changed the default, enter the current IP address of the router.



Next, type `admin/admin` for Account/Password. Then, type `?`. You will see a list of valid/common commands depending on the router that your use.

For users using previous Windows system (e.g., 2000/XP), simply click **Start >> Run** and type **Telnet 192.168.1.1** in the Open box as below. Next, type **admin/admin** for Account/Password. And, type **?** to get a list of valid/common commands.



Telnet Command: adsl txpct /adsl rxpct

This command allows the user to adjust the percentage of data transmission for QoS application.

Syntax

adsl txpct [auto:percent]

adsl rxpct [auto:percent]

Parameter	Description
auto	It means auto detection of ADSL transmission packet.
percent	It means to specify the percentage of ADSL transmission packet. Available range is 10-100.

Example

```
Vigor> adsl txpct auto
% percentage : 80
Vigor> adsl txpct 100
% percentage : 100
Vigor> adsl rxpct 100
% percentage : 100
```

Telnet Command: adsl status

This command is used to display current status of ADSL setting.

Syntax

adsl status

Example

```
Vigor> adsl status ?
----- ATU-R Info (hw: annex A, f/w: annex A) -----
Running Mode      : T1.413      State      : TRAINING
DS Actual Rate    : 0 bps      US Actual Rate    : 0 bps
DS Attainable Rate : 0 bps      US Attainable Rate : 0 bps
DS Path Mode      : Fast       US Path Mode      : Fast
DS Interleave Depth : 0        US Interleave Depth : 0
NE Current Attenuation : 0 dB    Cur SNR Margin    : 0 dB
DS actual PSD     : 0.0 dB      US actual PSD     : 0.0 dB
ADSL Firmware Version : 05-04-04-04-00-01
----- ATU-C Info -----
Far Current Attenuation : 0 dB    Far SNR Margin    : 0 dB
CO ITU Version[0]      : 00000000    CO ITU Version[1] : 00000000
DSLAM CHIPSET VENDOR   : < ADI >
```

Telnet Command: adsl ppp

This command can set the Internet Access mode for the router.

Syntax

adsl ppp [? / pvc_no vci vpi Encap Proto modu acqIP idle [Username Password]

Syntax Description

Parameter	Description
?	Display the command syntax of "adsl ppp".
pvc_no	It means the PVC number and the adjustable range is from 0 (Channel-1) to 7(Channel-8).
Encap	Different numbers represent different modes. 0 : VC_MUX, 1: LLC/SNAP, 2: LLC_Bridge, 3: LLC_Route, 4: VCMUX_Bridge 5: VCMUX_Route, 6: IPoE.
Proto	It means the protocol used to connect Internet. Different numbers represent different protocols. 0: PPPoA, 1: PPPoE, 2: MPoA.
Modu	0: T1.413, 2: G.dmt, 4: Multi, 5: ADSL2, 7:ADSL2_AnnexM 8:ADSL2+ 14:ADSL2+_AnnexM.
acqIP	It means the way to acquire IP address. Type the number to determine the IP address by specifying or assigned dynamically by DHCP server. 0 : fix_ip, 1: dhcp_client/PPPoE/PPPoA.(acquire IP method)
idle	Type number to determine the network connection will be kept for always or idle after a certain time. 1: always on, else idle timeout secs. Only for PPPoE/PPPoA.
Username	This parameter is used only for PPPoE/PPPoA
Password	This parameter is used only for PPPoE/PPPoA

You have to reboot the system when you set it on Route mode.

Example

```
> adsl ppp o 35 8 1 1 4 1 -1 draytek draytek
pvc no.=0
vci=35
vpi=8
encap=LLC(1)
proto=PPPoE(1)
modu=MULTI(4)
AcquireIP: Dhcp_client(1)
```

```
Idle timeout:-1
Username=draytek
Password=draytek
```

Telnet Command: adsl bridge

This command can specify a LAN port (LAN1 to LAN4) for mapping to certain PVC, and the mapping port/PVC will be operated in bridge mode.

adsl bridge [*pvc_no/status/save/enable/disable*] [*on/off/clear/tag tag_no*] [*service type*] [*px ...*]

Syntax Description

Parameter	Description
<i>pvc_no</i>	It means <i>pvc</i> number and must be between 0(Channel 1) to 7(Channel 8).
<i>status</i>	It means to shown the whole bridge status.
<i>save</i>	It means to save the configuration to flash.
<i>enable</i>	It means to enable the Multi-VLAN function.
<i>disable</i>	It means to disable the Multi-VLAN function.
<i>on/off</i>	It means to turn on/off bridge mode for the specific channel.
<i>clear</i>	It means to turn off and clear all the PVC settings.
<i>tag tag_no</i>	No tag: -1 Available number for tag: 0-4095
<i>pri pri_no</i>	The number 0 to 7 can be set to indicate the priority. "7" is the highest.
<i>service type</i>	Two number can be set: 0: for Normal (all the applications will be processed with the same PVC). 1: for the IGMP with different PVC which is used for special ISP.
<i>px...</i>	It means the number of LAN port (x=2-4). Port 1 is locked for NAT.

Example

```
> adsl bridge 4 on p2 p3
PVC Bridge  p1  p2  p3  p4  Service Type  Tag  Pri
-----
  4   ON      0   0   1   0   Normal    -1(OFF)  0
PVC 0 & 1 can't set for bridge mode.
Please use 'save' to save config.
```

Telnet Command: adsl idle

This command can make the router accessing into the idle status. If you want to invoke the router again, you have to reboot the router by using "reboot" command.

Example

```
> adsl idle
%Idle Mode!
You has to use {adsl reboot} to restart booting.
```

Telnet Command: adsl drivemode

This command is useful for laboratory to measure largest power of data transmission. Please follow the steps below to set adsl drivermode.

1. Please connect dsl line to the DSLAM.
2. Waiting for dsl SHOWTIME.
3. Drop the dsl line.
4. Now, it is on continuous sending mode, and adsl2/2+ led is always ON.
5. Use 'adsl reboot' to restart dsl to normal mode.

Telnet Command: adsl reboot

This command can wake up the idle router.

Example

```
> adsl reboot
% Adsl is Rebooting...
```

Telnet Command: adsl oamlb

This command is used to test if the connection between CPE and CO is OK or not.

adsl oamlb [*n*][*type*]

adsl oamlb chklink [*on/off*]

adsl oamlb [*log_on/log_off*]

Syntax Description

Parameter	Description
<i>n</i>	It means the total number of transmitted packets.
<i>type</i>	It means the protocol that you can use. 1 - for F4 Seg-to-Seg (VP level) 2 - for F4 End-to-End (VP level) 4 - for F5 Seg-to-Seg (VC level) 5 - for F5 End-to-End (VC level)
<i>chklink</i>	Check the DSL connection.
<i>Log_on/log_off</i>	Enable or disable the OAM log for debug.

Example

```
> adsl oamlb chklink on
OAM checking dsl link is ON.
> adsl oamlb F5 4
Tx cnt=0
Rx Cnt=0
>
```

Telnet Command: adsl vcilimit

This command can cancel the limit for vci value.

Some ISP might set the vci value under 32. In such case, we can cancel such limit manually by using this command. Do not set the number greater than 254.

adsl vcilimit [*n*]

Syntax Description

Parameter	Description
<i>n</i>	The number shall be between 1 ~ 254.

Example

```
> adsl vcilimit 33
change VCI limitation from 32 to 33.
```

Telnet Command: adsl annex

This command can display the annex interface of this router.

Example

```
> adsl annex
% hardware is annex B.
% modem code is annex B; built at 01/15,07:34.
```

Telnet Command: adsl automode

This command is used to add or remove ADSL modes (such as ANNEXL, ANNEXM and ANNEXJ) supported by Multimode.

adsl automode [*add/remove/set/default/show*] [*adsl_mode*]

Syntax Description

Parameter	Description
<i>add</i>	It means to add ADSL mode.
<i>remove</i>	It means to remove ADSL mode.
<i>set</i>	It means to use default settings plus the new added ADSL mode.
<i>default</i>	It means to use default settings.
<i>show</i>	It means to display current setting.
<i>adsl_mode</i>	There are three modes to be choose, ANNEXL, ANNEXM and ANNEXJ.

Example

```
> Vigor> adsl automode set ANNEXJ
Automode supported : T1.413, G.DMT, ADSL2, ADSL2+, ANNEXJ,

Vigor> adsl automode default
Automode supported : T1.413, G.DMT, ADSL2, ADSL2+,
```

Telnet Command: adsl showbins

This command can display the allocation for each Bin (Tone) SNR, Gain, and Bits.

adsl showbins [*startbin endbin /up*]

Syntax Description

Parameter	Description
<i>startbin</i>	The number is between 0 ~ 517.
<i>endbin</i>	The number is between 4 ~ 511.

Example

```
> adsl showbins 2 30
```

```
-----
Bin  SNR  Gain Bi - Bin  SNR  Gain Bi - Bin  SNR  Gain Bi - Bin  SNR  Gain Bi
   dB   dB   ts        dB   dB   ts        dB   dB   ts        dB   dB   ts
-----
 0  0.0  0.0  0 * 1  0.0  0.0  0 * 2  0.0  0.0  0 * 3  0.0  0.0  0
 4  0.0  0.0  0 * 5  0.0  0.0  0 * 6  0.0  0.0  0 * 7  0.0  0.0  8
 8  0.0  0.0 10 * 9  0.0  0.0 10 * 10  0.0  0.0 11 * 11  0.0  0.0 11
12  0.0  0.0 11 * 13  0.0  0.0 11 * 14  0.0  0.0 12 * 15  0.0  0.0 12
16  0.0  0.0 12 * 17  0.0  0.0 12 * 18  0.0  0.0 12 * 19  0.0  0.0 12
20  0.0  0.0 12 * 21  0.0  0.0 12 * 22  0.0  0.0 12 * 23  0.0  0.0 12
24  0.0  0.0 11 * 25  0.0  0.0 11 * 26  0.0  0.0 11 * 27  0.0  0.0 10
28  0.0  0.0 10 * 29  0.0  0.0 10 * 30  0.0  0.0 9 * 31  0.0  0.0 9
32  0.0  0.0 0 * 33  0.0  0.0 0 * 34  0.0  0.0 0 * 35  0.0  0.0 0
-----
Bin  SNR  Gain Bi - Bin  SNR  Gain Bi - Bin  SNR  Gain Bi - Bin  SNR  Gain Bi
   dB   dB   ts        dB   dB   ts        dB   dB   ts        dB   dB   ts
```

Telnet Command: adsl optn

At present ,this command allows you to enable and disable dual-latency only.

adsl optn FUNC [*value/on/off*]

Syntax Description

Parameter	Description
<i>FUNC</i>	Available setting is "dual" only. It means dual-latency.
<i>value</i>	The value shall be hex digits.
<i>on/off</i>	Type "on" for enabling such function. Type "off" for disabling such function.

Example

```
> adsl optn dual on
dsl dual-latency is ON.
```


Telnet Command: adsl femec

This command allows you to set FDM or EC mode for wireless setting. It may cause sync problem when change this setting.

adsl fdmec [*mode*]

Syntax Description

Parameter	Description
<i>mode</i>	Type the value for enabling the specified mode. 0: default (EC) 1: EC 2: FDM

Example

```
> adsl fdmec 1
FDM/EC mode: = EC
> adsl fdmec 0
FDM/EC mode: = Default
```

Telnet Command: adsl savecfg

This command can save the configuration into FLASH with a file format of cfg.

Example

```
> adsl savecfg
% Xdsl Cfg Save OK!
```

Telnet Command: adsl vendorid

This command allows you to configure user-defined CPE vendor ID.

adsl vendorid [*status/on/off/ set vid0 vid1*]

Syntax Description

Parameter	Description
<i>status</i>	Display current status of user-defined vendor ID.
<i>on</i>	Enable the user-defined function.
<i>off</i>	Disable the user-defined function.
<i>set vid0 vid1</i>	It means to set user-defined vendor ID with vid0 and vid1. The vendor ID shall be set with HEX format, ex: 00fe7244:79612f21.

Example

```
> adsl vendorid status
% User define CPE Vendor ID is OFF
% vid0:vid1 = 0x00fe7244:79612f21
> adsl vendorid on set vid0 vid1
% User define CPE Vendor ID is ON
```

Telnet Command: adsl atm

This command can set QoS parameter for ATM.

adsl atm pcr [*pvc_no*][*PCR*][*max*][*status*]

adsl atm scr [*pvc_no*][*SCR*]

adsl atm mbs [*pvc_no*][*MBS*]

adsl atm status

Syntax Description

Parameter	Description
<i>pvc_no</i>	It means <i>pvc</i> number and must be between 0(Channel 1) to 7(Channel 8).
<i>PCR</i>	It means Peak Cell Rate for upstream. The range for the number is "1" to "2539".
<i>max</i>	It means to get the highest speed for the upstream.
<i>SCR</i>	It means Sustainable Cell Rate.
<i>MBS</i>	It means Maximum Burst Size.
<i>status</i>	It means to display PCR/SCR/MBS setting.

Example

```
> adsl atm pcr 1 200 max
```

```
% PCR is 200 for pvc 1.
```

```
> adsl atm pcr status
```

```
pvc   channel      PCR
```

```
-----
```

```
0      1           0
```

```
1      2          200
```

```
2      3           0
```

```
3      4           0
```

```
4      5           0
```

```
5      6           0
```

```
6      7           0
```

```
7      8           0
```

```
> adsl atm mbs 2 300 max
```

```
% MBS is 300 for pvc 2.
```

Telnet Command: adsl pvcbinding

This command can configure PVC to PVC binding. Such command is available only for PPPoE and MPoA 1483 Bridge mode.

adsl pvcbinding [*pvc_x pvc_y* / *status* / -1]

Syntax Description

Parameter	Description
-----------	-------------

<i>pvc_x</i>	It means the PVC number for the source.
<i>pvc_y</i>	It means the PVC number that the source PVC will be bound to.
<i>status</i>	Display a table for PVC binding group.
<i>-1</i>	It means to clear specific PVC binding.

Example

```
> adsl pvcbinding 3 5
set done. bind pvc3 to pvc5.
```

The above example means PVC3 has been bound to PVC5.

```
> adsl pvcbinding 3 -1
clear pvc-1 binding
```

The above example means the PVC3 binding group has been removed.

Telnet Command: vdsl status

This command is used for display VDSL status.

Example

```
> vdsl status

----- ATU-R Info (hw: annex A, f/w: annex A/B/C) -----
Running Mode           :                State           : TRAINING
DS Actual Rate         :          0 bps   US Actual Rate   :          0 bps
DS Attainable Rate     :          0 bps   US Attainable Rate :          0 bps
DS Path Mode          :          Fast   US Path Mode       :          Fast
DS Interleave Depth    :          0     US Interleave Depth :          0
NE Current Attenuation :          0 dB   Cur SNR Margin    :          0 dB
DS actual PSD          :          0. 0 dB   US actual PSD     :          0. 0 dB
NE CRC Count           :          0     FE CRC Count       :          0
NE ES Count            :          0     FE ES Count        :          0
Xdsl Reset Times       :          0     Xdsl Link Times    :          0
ITU Version[0]         : b5004946       ITU Version[1]     : 544e0000
VDSL Firmware Version  : 05-04-08-00-00-06
Power Management Mode  : DSL_G997_PMS_NA
Test Mode              : DISABLE

----- ATU-C Info -----
Far Current Attenuation :          0 dB   Far SNR Margin     :          0 dB
CO ITU Version[0]      : 00000000       CO ITU Version[1]  : 00000000
DSLAM CHIPSET VENDOR   : < unknown >
```

Telnet Command: vdsl idle

Note: We can provide prompt support (support@draytek.com) if you refer to the telnet command and have any queries.

adsl idle [on | tcpmessage | tcpmessage_off]

Syntax Description

Parameter	Description
<i>on</i>	
<i>tcpmessage</i>	
<i>Tcpmessage_off</i>	

Example

```
> vdsl idle ?
% Usage : adsl idle [on | tcpmessage | tcpmessage_off]
% DSL is under [DISABLE] test mode.
% DSL debug tool mode is off.

Vigor> vdsl idle on
% DSL is under [IDLE/QUIET] test mode.
% DSL debug tool mode is off.
```

Telnet Command: vdsl drivermode

Note: We can provide prompt support (support@draytek.com) if you refer to the telnet command and have any queries.

Example

```
> vdsl drivermode
%ADSL Enter Driver Mode!
% 1. please connect dsl line to the DSLAM.
% 2. Waiting for dsl SHOWTIME.
% 3. drop the dsl line.
% 4. now, it is on continuous sending mode.
% Use 'adsl reboot' to restart dsl to normal mode.
```

Telnet Command: vdsl reboot

Note: We can provide prompt support (support@draytek.com) if you refer to the telnet command and have any queries.

Example

```
> vdsl reboot ?
%ADSL is Rebooting....
```

Telnet Command: vdsl annex

Note: We can provide prompt support (support@draytek.com) if you refer to the telnet command and have any queries.

Example

```
> vdsl annex ?  
% hardware is annex A.  
% ADSL modem code is annex A
```

Telnet Command: vdsl showbins

This command is used to display each Bin(Tone) SNR, Gain, and Bits allocated.

Note: We can provide prompt support (support@draytek.com) if you refer to the telnet command and have any queries.

adsl showbins [*startbin endbin* | *up*]

Syntax Description

Parameter	Description
<i>startbin</i>	Available setting: 0 to 4092.
<i>endbin</i>	Available setting: 4 to 4092.
<i>up</i>	It is used to display upstream information. The default is downstream.

Example

```
> vdsl showbins 0 30
DOWNSTREAM :
-----
Bin   SNR   Gain Bi - Bin   SNR   Gain Bi - Bin   SNR   Gain Bi - Bin   SNR   Gain Bi
      dB   .1dB ts       dB   .1dB ts       dB   .1dB ts       dB   .1dB ts
-----
Bin   SNR   Gain Bi - Bin   SNR   Gain Bi - Bin   SNR   Gain Bi - Bin   SNR   Gain Bi
      dB   .1dB ts       dB   .1dB ts       dB   .1dB ts       dB   .1dB ts
```

Telnet Command: vdsl optn

This command is used to enable or disable the parameters related to VDSL.

Note: We can provide prompt support (support@draytek.com) if you refer to the telnet command and have any queries.

adsl optn FUNC [*us/ds/bi* [*value/on/off*]]

Syntax Description

Parameter	Description
FUNC	Available settings: trellis', 'bitswap', 'sra', 'retx', 'aelem', 'status', 'g.vector' 'default'.
<i>us/ds/bi</i>	us - upstream ds - downstream bi - birection.

<i>value</i>	bitswap=0~2, sra=0~4
<i>on/off</i>	On - Enable the function. Off - Disable the function.

Example

```
>
```

Telnet Command: vdsl savecfg

This command is used to save the configuration.

Note: We can provide prompt support (support@draytek.com) if you refer to the telnet command and have any queries.

Example

```
> Vigor> vdsl savecfg ?
% Xdsl Cfg Save OK!
```

Telnet Command: vdsl vendorid

This command is used to set user defined CPE vendor ID.

Note: We can provide prompt support (support@draytek.com) if you refer to the telnet command and have any queries.

adsl vendorid [?/status/on/off/ set vid0 vid1]

Syntax Description

Parameter	Description
<i>status</i>	Display current setting of vendor ID.
<i>On/off</i>	Enable/Disable the user defined setting.
<i>set</i>	It is used to set user define vendor ID by "vid0" & "vid1".
<i>vid0 vid1</i>	Set vendor ID number with the format of HEX, ex: 00fe7244 79612f21.

Example

```
> vdsl vendorid on set 00fe7244 79612f21
% User define CPE Vendor ID is ON
```

Telnet Command: vdsl snr

This command is used to .

Note: We can provide prompt support (support@draytek.com) if you refer to the telnet command and have any queries.

adsl srn [delta]

Syntax Description

Parameter	Description
-----------	-------------

<i>delta</i>	It means SNR margin delta. The range is from -50 to 50. Current ADSL SNR Margin is 0 dB.
--------------	--

Example

```
> vdsl snr 25
ADSL SNR update successfully !
Restarting ADSL modem ...
```

Telnet Command: bpa

This command allows to configure a network setting specified for Australia's ISP.

bpa m [*-<command>* *<parameter>* / ...]

Syntax Description

Parameter	Description
<i>m</i>	Available settings are 1 and 2.
-a <i><enable></i>	1/0 to enable/disable this entry
-n <i><UserName></i>	contact UserName(max. 24 characters)
-p <i><PassWord></i>	contact PassWord (max. 24 characters)
-s <i><select></i>	It means to specify an IP address for Server. 0 : no selection. 1 : NSW(61.9.192.13) 2 : QLD(61.9.208.13), 3 : VIC(61.9.128.13) 4 : SA(61.9.224.13), 5 : WA(61.9.240.13)
-l <i><List></i>	List all settings configured.

Example

```
> bpa 1 -a 1 -n testUser -p testPassword -s 4
> bpa -l
-----index: 1 active-----
UserName[1]: testUser
PassWord[1]: testPassword
ServerIP[1]:4

-----index: 2 inactive-----
UserName[2]:
PassWord[2]:
ServerIP[2]:0

>
```


Telnet Command: csm appe prof

Commands under CSM allow you to set CSM profile to define policy profiles for different policy of IM (Instant Messenger)/P2P (Peer to Peer) application.

“csm appe prof ” is used to configure the APP Enforcement Profile name. Such profile will be applied in Default Rule of Firewall>>General Setup for filtering.

Syntax

csm appe prof -i INDEX [-v / -n NAME/setdefault]

Syntax Description

Parameter	Description
INDEX	It means to specify the index number of CSM profile, from 1 to 32.
- v	It means to view the configuration of the CSM profile.
- n	It means to set a name for the CSM profile.
NAME	It means to specify a name for the CSM profile, less than 15 characters.
setdefault	Reset to default settings.

Example

```
> csm appe prof -i 1 -n games
The name of APPE Profile 1 was setted.
```

Telnet Command: csm appe set

It is used to configure group settings for IM/P2P/Protocol and Others in APP Enforcement Profile.

csm appe set -i INDEX [-v GROUP/ -e AP_IDX / -d AP_IDX]

Syntax Description

Parameter	Description
INDEX	Specify the index number of CSM profile, from 1 to 32.
- v	View the IM/P2P/Protocol and Others configuration of the CSM profile.
-e	Enable to block specific application.
-d	Disable to block specific application.
GROUP	Specify the category of the application. Available options are: IM, P2P, Protocol and Others.
AP_IDX	Each application has independent index number for identification in CLI command. Specify the index number of the application here. If you have no idea of the 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
show	It means to display all of the profiles.
setdefault	It means to return to default settings for all of the profile.
msg MSG	It means to set the administration message. MSG means the content (less than 255 characters) of the message itself.
obj	It means to specify the object for the profile.
INDEX	It means to specify the index number of CSM profile, from 1 to 8.
-n	It means to set the profile name.
PROFILE_NAME	It means to specify the name of the profile (less than 16 characters)
-p	Set the priority (defined by the number specified in VALUE) for the profile.

<i>VALUE</i>	Number 0 to 3 represent different conditions. 0: It means Bundle: Pass. 1: It means Bundle: Block. 2: It means Either: URL Access Control First. 3: It means Either: Web Feature First.
<i>-l</i>	It means the log type of the profile. They are: P: Pass, B: Block, A: All, N: None
<i>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>-l N P B A</i>	Specify the log type of the profile. P: Pass. B: Block. A: All. N: None.
<i>-w WCF_PROFILE</i>	WCF_PROFILE: Type the index number of the WCF profile.
<i>-u UCF_PROFILE</i>	UCF_PROFILE: Type the index number of the UCF profile.
<i>-c CACHE_TIME</i>	-c means to set the cache time for DNS filter. CACHE_TIME: It means to set the time for cache to live (available values are 1 to 24; 1 is one hour, 2 is two hours, and so on ...) for DNS filter.
<i>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
<code>-V</code>	It means to view the configuration of DoS defense system.
<code>-D</code>	It means to deactivate the DoS defense system.
<code>-A</code>	It means to activate the DoS defense system.
<code>-s</code>	It means to enable the defense function for a specific attack and set its parameter(s).
<code>ATTACK_F</code>	It means to specify the name of flooding attack(s) or portscan, e.g., synflood, udpflood, icmpflood, or postscan.
<code>THRESHOLD</code>	It means the packet rate (packet/second) that a flooding attack will be detected. Set a value larger than 20.
<code>TIMEOUT</code>	It means the time (seconds) that a flooding attack will be blocked. Set a value larger than 5.
<code>-a</code>	It means to enable the defense function for all attacks listed in <code>ATTACK_0</code> .
<code>-e</code>	It means to enable defense function for a specific attack(s).
<code>ATTACK_0</code>	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.
<code>-d</code>	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
<code><command><parameter>[...]</code>	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
<code>-M n</code>	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 unnumber] -c [option number] -v [option value]

ip dhcpc option -e [1 or 0] -w [wan unnumber] -c [option number] -x [option value]

ip dhcpc option -e [1 or 0] -w [wan unnumber] -c [option number] -a [option value]

ip dhcpc option -u [idx unnumber]

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<1ms
Receive reply from 192.168.1.1, time<1ms
Receive reply from 192.168.1.1, time<1ms
Receive reply from 192.168.1.1, time<1msReceive reply from 192.168.1.1,
time<1ms

Packets: Sent = 5, Received = 5, Lost = 0 (0% loss)
```

Telnet Command: ip tracet

This command allows users to trace the routes from the router to the host.

Syntax

`ip tracer [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 tracer 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
<i><command><parameter>[...]</i>	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>-i [value]</i>	Specify an index number for setting policy route profile. Value: 1 to 60. "-1" means to get a free policy index automatically.
<i>-e [0/1]</i>	0: Disable the selected policy route profile. 1: Enable the selected policy route profile.
<i>-o [value]</i>	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.
<i>-1 [any/range]</i>	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.
<i>-2 [any/ip_range/ip_subnet/domain]</i>	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.
<i>-3 [any/range]</i>	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>-l [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 [value]	It means "source IP". Value: Available settings include: Any: It indicates any IP address can be used as source IP address. "xxx.xxx.xxx.xxx": The type format (e.g, 192.168.1.0).
-d [value]	It means "destination IP". Value : Available settings include: Any: It indicates any IP address can be used as destination IP address. "xxx.xxx.xxx.xxx": Specify an IP address.
-p [value]	It means "destination port". Value: Specify a number or type Any (indicating any number).
-t [value]	It means "protocol". Value: Available settings include "ICMP", "TCP", "UDP" and "Any".

Example

```
> ip policy_rt diagnose -s 192.168.1.100 -d any -p any -t ICMP

-----
      Matched Route  (Priority)
-----
* No_Match

-----
      Matched Policy (Priority)
-----
* Policy_1 (200)

* Conclusion:The packet was dropped because the send-to interface of the
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. [...] means that you can type in several commands in one line.
<i>-a <IP Address></i>	Set forwarded DNS server IP Address.
<i>-d <DNS server mapping index number></i>	Delete the selected LAN DNS profile.
<i>-e <0/1></i>	0: disable such function. 1: enable such function.
<i>-i <profile setting index number></i>	Type the index number of the profile.
<i>-l</i>	List the content of LAN DNS profile (including domain name, IP address and message).
<i>-n <domain name></i>	Set domain name.

<i>-p</i> <profile name>	Set profile name for LAN DNS.
<i>-r</i>	Reset the settings for selected profile.

Example

```
> ip dnsforward -i 1 -n ftp.drayTek.com
% Configure Set1's DomainName:ftp.drayTek.com
> ip dnsforward -i 1 -a 172.16.1.1
% Configure Set1's IP:172.16.1.1
> ip dnsforward -i 1 -l
% Idx: 1
% State: Disable
% Profile: test
% Domain Name: ftp.drayTek.com
% DNS Server IP: 172.16.1.1
>
```

Telnet Command: ip6 addr

This command allows users to set the IPv6 address for your router.

Syntax

```
ip6 addr -s [prefix] [prefix-length] [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
<i>-s</i>	It means to add a static ipv6 address.
<i>-d</i>	It means to delete an ipv6 address.
<i>-a</i>	It means to show current address(es) status.
<i>-u</i>	It means to show only unicast addresses.
<i>prefix</i>	It means to type the prefix number of IPv6 address.
<i>prefix-length</i>	It means to type a fixed value as the length of the prefix.
<i>LAN/WAN1/WAN2/iface#</i>	It means to specify LAN or WAN interface for such address.

Example

```
> ip6 addr -a
LAN
Unicast Address:
```

```
FE80::250:7FFF:FE00:0/64 (Link)
Multicast Address:
  FF02::2
  FF02::1:FF00:0
  FF02::1
```

Telnet Command: ip6 dhcp req_opt

This command is used to configure option-request settings for DHCPv6 client.

Syntax

`ip6 dhcp req_opt [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.
<i>[<command> <parameter> ...]</i>	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
<i>-a</i>	It means to show current DHCPv6 status.
<i>-s</i>	It means to ask the SIP.
<i>-S</i>	It means to ask the SIP name.
<i>-d</i>	It means to ask the DNS setting.
<i>-D</i>	It means to ask the DNS name.
<i>-n</i>	It means to ask NTP.
<i>-i</i>	It means to ask NIS.
<i>-I</i>	It means to ask NIS name.
<i>-p</i>	It means to ask NISP.
<i>-P</i>	It means to ask NISP name.
<i>-b</i>	It means to ask BCMCS.
<i>-B</i>	It means to ask BCMCS name.
<i>-r</i>	It means to ask refresh time.
<i>Parameter</i>	1: the parameter related to the request will be displayed. 0: the parameter related to the request will not be displayed.

Example

```
> ip6 dhcp req_opt WAN2 -S 1
> ip6 dhcp req_opt WAN2 -r 1
> ip6 dhcp req_opt WAN2 -a
% Interface WAN2 is set to request following DHCPv6 options:
%   sip name
>
```

Telnet Command: ip6 dhcp client

This command allows you to use DHCPv6 protocol to obtain IPv6 address from server.

Syntax

ip6 dhcp client [WAN1|WAN2|USB] [-<command> <parameter>| ...]

Syntax Description

Parameter	Description
<i>client</i>	It means the dhcp client settings.
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-a	It means to show current DHCPv6 status.
-p [IAID]	It means to request identity association ID for Prefix Delegation.
-n [IAID]	It means to request identity association ID for Non-temporary Address.
-t [time]	It means to set solicit interval. Time: 0 ~ seconds (default value is 0).
-c [parameter]	It means to send rapid commit to server.
-l [parameter]	It means to send information request to server.
-e[parameter]	It means to enable or disable the DHCPv6 client. 1: Enable 0: Disable
-m [parameter]	It means to enable/disable server DUID set by Link layer and time.
-d	It means to display the client DUID.
-A [parameter]	It means to set authentication protocol. 0: Undefine 2: delayed protocol
-R [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 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.
pdadd <suffix><prefix_len><client linklocal><client DUID>	It means to add PD node.
pddel <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
[<command> <parameter> / ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-W n	W means to set WAN interface and n means different selections. Default is WAN1. n=1: WAN1 n=2: WAN2 n=3: WAN3 . . n=X: WANx
-M n	M means to set Internet Access Mode (Mandatory) and n means different modes (represented by 0 - 5) n= 0: Offline, n=1: PPP, n=2: TSPC, n=3: AICCU, n=4: DHCPv6, n=5: Static n=6: 6in4-Static n=7: 6rd
-m n	It means to set IPv6 MTU. N = any value (0 means "unspecified").
6rd	
-C n	It means to set 6rd connection mode. n=0: Auto n=1: Static
-s <server>	It means to set 6rd IPv4 Border Relay.
-m n	It means to set 6rd IPv4 address mask length.
-p <prefix>	It means to set IPv6 prefix for 6rd connection.
-l n	It means to set the prefix length for 6rd connection.
6in4	
-s <server>	It means to set 6in4 remote endpoint IPv4 address.
-l <IPv6 Addr>	It means to set the IPv6 address for 6in4 connection.
-P n	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 neigh

This command allows you to add a proxy neighbour.

Syntax

```
ip6 neigh -s inet6_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 proxy neighbour.
-d	It means to delete a proxy neighbour.
-a	It means to show proxy neighbour status.
inet6_addr	Type an IPv6 address
LAN/WAN1/WAN2	Specify an interface for the proxy neighbor.

Example

```
> ip6 neigh -s FE80::250:7FFF:FE12:300 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 tspc

This command allows you to display TSPC status.

Syntax

`ip6 tspc [ifno]`

Syntax Description

Parameter	Description
<i>ifno</i>	It means the connection interface. Ifno=1 (means WAN1)

Example

```
> ip6 tspc 1
Local Endpoint v4 Address : 111.243.177.223
Local Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b9
Router DNS name : 8886666.broker.freenet6.net
Remote Endpoint v4 Address : 81.171.72.11
Remote Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b8
Tspc Prefixlen : 56
Tunnel Broker: Amsterdam.freenet.net
```

```
Status: Connected
```

```
>
```

Telnet Command: ip6 radvd

This command allows you to enable or disable RADVD server.

Syntax

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).
-I <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 (<i>"?"</i> 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.</p> <p>u - it means "user defined".</p> <p><protocol> - It means TCP(6),UDP(17), TCP/UDP(255).</p> <p><source_port__value> -</p> <p>1 - Port OP, range is 0-3. 0:=, 1:!=, 2:>, 3:<</p> <p>3 - Port range of the Start Port Number, range is 1-65535.</p> <p>5 - Port range of the End Port Number, range is 1-65535.</p> <p><destination_port_value>:</p> <p>2 - Port OP, range is 0-3, 0:=, 1:!=, 2:>, 3:<</p> <p>4 - Port range of the Start Port Number, range is 1-65535.</p> <p>6 - Port range of the End Port Number, range is 1-65535.</p>
-f <value>	<p>It means to set the gragment type.</p> <p>0 - Don't care</p> <p>1 - Unfragmented</p> <p>2 - Fragmented</p> <p>3 - Too Short</p>
-F	<p>It means the Filter action you can specify.</p> <p>0 -Pass Immediately,</p> <p>1 - Block Immediately,</p> <p>2 - Pass if no further match,</p> <p>3 - Block if no further match.</p>
-m <value>	<p>It means to set the MAC Bind IP type.</p> <p>0 - Non-Strict</p> <p>1 - Strict</p>
-L <value>	<p>It means to set number of sessions control.</p> <p>0 ~ 30000</p>
-q <value>	<p>It means the classification for QoS.</p> <p>1- Class 1,</p> <p>2 - Class 2,</p> <p>3 - Class 3,</p> <p>4 - Other</p>
-l <wan><log flag>	<p>It means load balance policy.</p> <p>Such function is used for "debug" only.</p>
-E <value>	<p>It means to enable APP Enforcement.</p> <p>1 - Enable</p> <p>0 - Disable</p>
-a<index><log flag>	<p>It means to specify which APP Enforcement profile will be applied.</p> <p><index> - Available settings range from 0 ~ 32. "0" means no profile will be applied.</p> <p><log flag> - Enable (1) the syslog; disable (0) the syslog.</p>
-u<index><log flag>	<p>It means to specify which URL 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>
-w<index><log flag>	<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>
<i>-n<index><log flag></i>	<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>
<i>-N <value></i>	<p>It means to set number of the next filter set.</p> <p>0 - 12</p>
<i>-c <0-20></i>	<p>It means to set code page. Different number represents different code page.</p> <ul style="list-style-type: none"> 0. None 1. ANSI(1250)-Central Europe 2. ANSI(1251)-Cyrillic 3. ANSI(1252)-Latin I 4. ANSI(1253)-Greek 5. ANSI(1254)-Turkish 6. ANSI(1255)-Hebrew 7. ANSI(1256)-Arabic 8. ANSI(1257)-Baltic 9. ANSI(1258)-Viet Nam 10. OEM(437)-United States 11. OEM(850)-Multilingual Latin I 12. OEM(860)-Portuguese 13. OEM(861)-Icelandic 14. OEM(863)-Canadian French 15. OEM(865)-Nordic 16. ANSI/OEM(874)-Thai 17. ANSI/OEM(932)-Japanese Shift-JIS 18. ANSI/OEM(936)-Simplified Chinese GBK 19. ANSI/OEM(949)-Korean 20. ANSI/OEM(950)-Traditional Chinese Big5
<i>-C <Windows Size> <Session_Timeout></i>	<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>
<i>-v</i>	It is used to show current filter/rule settings.
<i>-M <Your Comments></i>	It means to set comment for the set rule.
<i>-U <up or down></i>	<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
<i>-r</i>	It means to refresh the flowtrack.
<i>-e</i>	It means to enable or disable the flowtrack.
<i>-f</i>	It means to show the sessions state of flowtrack. If you do not specify any IP address, then all the session state of flowtrack will be displayed.
<i>-b</i>	It means to show all of IP sessions state.
<i>- i [IP address]</i>	It means to specify IP address (e.g., -i 192.168.2.55).
<i>-p[value]</i>	It means to type a port number (e.g., -p 1024). Available settings are 0 ~ 65535.
<i>-t [value]</i>	It means to specify a protocol (e.g., -t tcp).

	Available settings include: <i>tcp</i> <i>udp</i> <i>icmp</i>
--	--

Example

```
>ipf flowtrack set -r
Refresh the flowstate ok
> ipf flowtrack view -f
Start to show the flowtrack sessions state:

ORIGIN>> 192.168.1.11:59939 ->      8.8.8.8: 53 ,ifno=0
REPLY >>      8.8.8.8: 53 -> 192.168.1.11:59939 ,ifno=3
          proto=17, age=93023180(3920), flag=203
ORIGIN>> 192.168.1.11:15073 ->      8.8.8.8: 53 ,ifno=0
REPLY >>      8.8.8.8: 53 -> 192.168.1.11:15073 ,ifno=3
          proto=17, age=93025100(2000), flag=203
ORIGIN>> 192.168.1.11: 7247 ->      8.8.8.8: 53 ,ifno=0
REPLY >>      8.8.8.8: 53 -> 192.168.1.11: 7247 ,ifno=3
          proto=17, age=93020100(7000), flag=203
End to show the flowtrack sessions state
> 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`

mngr lanaccess -d
mngr lanaccess -v
mngr 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

```
> mngr lanaccess -e 1
> mngr lanaccess -s FTP,TELNET
> mngr lanaccess -i LAN3
> mngr 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
[<i><command></i> <i><parameter></i> /...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-e <i><1/2></i>	1: Enable the SNMP function. 2: Disable the SNMP function.
-g <i><Community name></i>	It means to set the name for getting community by typing a proper character. (max. 23 characters)
-s <i><Community name></i>	It means to set community by typing a proper name. (max. 23 characters)
-m <i><IP address></i>	It means to set one host as the manager to execute SNMP function. Please type in IPv4 address to specify certain host.
-t <i><Community name></i>	It means to set trap community by typing a proper name. (max. 23 characters)
-n <i><IP address></i>	It means to set the IPv4 address of the host that will receive the trap community.
-T <i><seconds></i>	It means to set the trap timeout <i><0-999></i> .
-V	It means to list SNMP setting.

Example

```
> mngt snmp -e 1 -g draytek -s DK -m  
192.168.1.20,192.168.5.192/26,10.20.3.40/24 -t trapcom -n  
192.168.1.20,10.20.3.40 -T 88  
SNMP Agent Turn on!!!  
Get Community set to draytek  
Set Community set to DK  
Manager Host IP set to 192.168.1.20,192.168.5.192/26,10.20.3.40/24  
Trap Community set to trapcom  
Notification Host IP set to 192.168.1.20,10.20.3.40  
Trap Timeout set to 88 seconds
```

Telnet Command: 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.
<i>-v</i>	It means to view the information of the specified object profile. Example: <i>object ip obj 1 -v</i>
<i>-n NAME</i>	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: <i>object ip obj 9 -n bruce</i>
<i>-i INTERFACE</i>	It means to define an interface for the IP object. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=3, means WAN Example: <i>object ip obj 8 -i 0</i>
<i>-s INVERT</i>	It means to set invert selection for the object profile. INVERT=0, means disableing the function. INVERT=1, means enabling the function. Example: <i>object ip obj 3 -s 1</i>
<i>-a TYPE</i>	It means to set the address type and IP for the IP object profile. TYPE=0, means Mask TYPE=1, means Single TYPE=2, means Any TYPE=3, means Rang 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 START_IP) 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.
-v	It means to view the information of the specified group profile. Example: <i>object ip grp 1 -v</i>
-n <i>NAME</i>	It means to define a name for the IP group. NAME: Type a name with less than 15 characters. Example: <i>object ip grp 8 -n bruce</i>
-i <i>INTERFACE</i>	It means to define an interface for the IP group. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=3, means WAN Example: <i>object ip grp 3 -i 0</i>
-a <i>IP_OBJ_INDEX</i>	It means to specify IP object profiles for the group profile. Example: <i>:object ip grp 3 -a 1 2 3 4 5</i> The IP object profiles with index number 1,2,3,4 and 5 will be group under such profile.

Example

```
> object ip grp 2 -n First
IP Group Profile 2
Name      :[First]
Interface:[Any]
Included ip object index:
[0:][0]
[1:][0]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]
[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.
<i>-v</i>	It means to view the information of the specified group profile. Example: <code>object ip grp 1 -v</code>
<i>-n 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>
<i>-a 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: <i>object service obj 3 -s 0 100 200</i></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: <i>object service obj 3 -d 1 100 200</i></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
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number of the specified group profile.
<i>-v</i>	It means to view the information of the specified group profile. Example: <i>object service grp 1 -v</i>
<i>-n NAME</i>	It means to define a name for the service group.

	NAME: Type a name with less than 15 characters. Example: <i>object service grp 8 -n bruce</i>
<i>-a SER_OBJ_INDEX</i>	It means to specify service object profiles for the group profile. Example: <i>:object service grp 3 -a 1 2 3 4 5</i> The service object profiles with index number 1,2,3,4 and 5 will be group under such profile.

Example

```
>object service grp 1 -n Grope_1
Service Group Profile 1
Name      :[Grope_1]
Included service object index:
[0:][0]
[1:][0]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]

>object service grp 1 -a 1 2
Service Group Profile 1
Name      :[Grope_1]
Included service object index:
[0:][1]
[1:][2]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]
```

Telnet Command: object kw

This command is used to create keyword profile.

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", ".vrml", ".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
[ ].vrml
-----
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: portmaptime

This command allows you to set a time of keeping the session connection for specified protocol.

Syntax

portmaptime [*-<command>* *<parameter>* / ...]

Syntax Description

Parameter	Description
[<i><command></i> <i><parameter></i> /...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-t <i><sec></i>	It means "TCP" protocol. <sec>: Type a number to set the TCP session timeout.
-u <i><sec></i>	It means "UDP" protocol. <sec>: Type a number to set the UDP session timeout.
-i <i><sec></i>	It means "IGMP" protocol. <sec>: Type a number to set the IGMP session timeout.
-w <i><sec></i>	It means "TCP WWW" protocol. <sec>: Type a number to set the TCP WWW session timeout.
-s <i><sec></i>	It means "TCP SYN" protocol. <sec>: Type a number to set the TCP SYN session timeout.
-f	It means to flush all portmaps (useful for diagnostics).
-l <i><List></i>	List all settings.

Example

```
> portmaptime -t 86400 -u 300 -i 10
> portmaptime -l
----- Current setting -----
TCP Timeout   : 86400 sec.
UDP Timeout   : 300 sec.
IGMP Timeout  : 10 sec.
```

```
TCP WWW Timeout: 60 sec.
TCP SYN Timeout: 60 sec.
```

Telnet Command: qos setup

This command allows user to set general settings for QoS.

Syntax

qos setup [*-<command> <parameter> | ...*]

Syntax Description

Parameter	Description
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-h	Type it to display the usage of this command.
-m <mode>	It means to define which traffic the QoS control settings will apply to and enable QoS control. 0: disable. 1: in, apply to incoming traffic only. 2: out, apply to outgoing traffic only. 3: both, apply to both incoming and outgoing traffic. Default is enable (for outgoing traffic).
-i <bandwidth>	It means to set inbound bandwidth in kbps (Ethernet WAN only). The available setting is from 1 to 100000.
-o <bandwidth>	It means to set outbound bandwidth in kbps (Ethernet WAN only). The available setting is from 1 to 100000.
-r <index:ratio>	It means to set ratio for class index, in %.
-u <mode>	It means to enable bandwidth control for UDP. 0: disable 1: enable Default is disable.
-p <ratio>	It means to enable bandwidth limit ratio for UDP.
-t <mode>	It means to enable/disable Outbound TCP ACK Prioritize. 0: disable 1: enable
-V	Show all the settings.
-I <bandwidth>	Minimum available non-VoIP Inbound Bandwidth when VoIP is detected (Kbps). Default value: half of WAN inbound bandwidth.
-O <bandwidth>	Minimum available non-VoIP Outbound Bandwidth when VoIP is detected (Kbps). Default value: half of WAN outbound bandwidth.
-v 0	It means Auto bandwidth adjustment. Adjust to minimum In/Out bandwidth setting (or half QoS bandwidth).
-v 1	When VoIP detected, QoS In/Out bandwidth adjusted to minimum values.
-D	Set all to factory default (for all WANs).
[...]	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
[<i><command></i> <i><parameter></i> /...]	The available commands with parameters are listed below. [...] <i>means that you can type in several commands in one line.</i>
<i>-h</i>	Type it to display the usage of this command.
<i>-c <no></i>	Specify the inde number for the class. Available value for <i><no></i> contains 1, 2 and 3. The default setting is class 1.
<i>-n <name></i>	It means to type a name for the class.
<i>-a</i>	It means to add rule for specified class.
<i>-e <no></i>	It means to edit specified rule. <i><no></i> : type the index number for the rule.
<i>-d <no></i>	It means to delete specified rule. <i><no></i> : type the index number for the rule.
<i>-m <mode></i>	It means to enable or disable the specified rule. 0: disable, 1: enable
<i>-l <addr></i>	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.
<i>-r <addr></i>	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> ".

	<p><i>addr1:subnet</i> - It means the subnet address with start IP address. Please type the subnet and the IP address, for example, "<i>-/172.16.3.9:255.255.0.0</i>".</p> <p><i>any</i> - It means Any address. Simple type "<i>-/</i>" to specify any address for this command.</p>
<i>-p <DSCP id></i>	Specify the ID.
<i>-s <Service type></i>	<p>Specify the service type by typing the number. The available types are listed as below:</p> <p>1:ANY 2:DNS 3:FTP 4:GRE 5:H.323 6:HTTP 7:HTTPS 8:IKE 9:IPSEC-AH 10:IPSEC-ESP 11:IRC 12:L2TP 13:NEWS 14:NFS 15:NNTTP 16:PING 17:POP3 18:PPTP 19:REAL-AUDIO 20:RTSP 21:SFTP 22:SIP 23:SMTP 24:SNMP 25:SNMP-TRAPS 26:SQL-NET 27:SSH 28:SYSLOG 29:TELNET 30:TFTP</p>
<i>-S <d/s></i>	Show the content for specified DSCP ID/Service type.
<i>-V <1/2/3></i>	Show the rule in the specified class.
<i>[...]</i>	It means that you can type in several commands in one line.

Example

```
> qos class -c 2 -n draytek -a -m 1 -l 192.168.1.50:192.168.1.80
```

Following setting will set in the class2
 class 2 name set to draytek
 Add a rule in class2
 Class2 the 1 rule enabled
 Set local address type to Range, 192.168.1.50:192.168.1.80

Telnet Command: qos type

This command allows user to configure protocol type and port number for QoS.

Syntax

`qos type [-a <service name> / -e <no> / -d <no>].`

Syntax Description

Parameter	Description
-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
on/off	On - Enable the QoS for VoIP. Off - Disable th QoS for VoIP.

Example

```
> qos voip off
QoS for VoIP: Disable; SIP Port: 5060
```

Telnet Command: quit

This command can exit the telnet command screen.

Telnet Command: show lan

This command displays current status of LAN IP address settings.

Example

```
> show lan
The LAN settings:
Status IP          Mask          DHCP Start IP    Pool Gateway
-----
[V]LAN1 192.168.1.1  255.255.255.0 V 192.168.1.10 200 192.168.1.1
[X]LAN2 192.168.2.1  255.255.255.0 V 192.168.2.10 100 192.168.2.1
[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: show traffic

This command can display traffic graph for WAN1, transmitted bytes, received bytes and sessions.

Syntax

```
show traffic [wan1] [tx/rx] [weekly]
```

show traffic session *[weekly]*

Example

[illegible]

Telnet Command: show statistic

This command displays statistics for WAN interface.

Syntax

show statistic

show statistic reset *[interface]*

Syntax Description

Parameter	Description
<i>reset</i>	It means to reset the transmitted/received bytes to Zero.
<i>interface</i>	It means to specify WAN1 interface for displaying related statistics.

Example

```
> show statistic
WAN1 total TX: 0 Bytes ,RX: 0 Bytes

>
```


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
<i>?</i>	It means to display current gateway that you can use.
<i>Gateway IP</i>	It means to specify a gateway address used for DHCP server.

Example

```
> srv dhcp gateway 192.168.2.1
This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

Telnet Command: `srv dhcp ipcnt`

This command allows users to specify IP counts for DHCP server.

Syntax

`srv dhcp ipcnt [?]`

`srv dhcp ipcnt [IP counts]`

Syntax Description

Parameter	Description
<i>?</i>	It means to display current used IP count number.
<i>IP counts</i>	It means the number that you have to specify for the DHCP server.

Example

```
> srv dhcp ipcnt ?
% srv dhcp ipcnt <IP counts>
% Now: 150
```

Telnet Command: `srv dhcp off`

This function allows users to turn off DHCP server. It needs rebooting router, please type "sys reboot" command to reboot router.

Telnet Command: `srv dhcp on`

This function allows users to turn on DHCP server. It needs rebooting router, please type "sys reboot" command to reboot router.

Telnet Command: `srv dhcp relay`

This command allows users to set DHCP relay setting.

Syntax

`srv dhcp relay servip [server ip]`

`srv dhcp relay subnet [index]`

Syntax Description

Parameter	Description
<i>server ip</i>	It means the IP address that you want to used as DHCP server.
<i>Index</i>	It means subnet 1 or 2. Please type 1 or 2. The router will invoke this function according to the subnet 1 or 2 specified here.

Example

```
> srv dhcp relay servip 192.168.1.46
> srv dhcp relay subnet 2
> srv dhcp relay servip ?
% srv dhcp relay servip <server ip>
% Now: 192.168.1.46
```

Telnet Command: srv dhcp startip

Syntax

srv dhcp startip [?]

srv dhcp startip [IP address]

Syntax Description

Parameter	Description
<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
<i>?</i>	It means to display current leasetime used for the DHCP server.
<i>Lease Time (sec)</i>	It means the lease time that DHCP server can use. The unit is second.

Example

```
> srv dhcp leasetime ?
% srv dhcp leasetime <Lease Time (sec.)>
% Now: 86400
>
```

Telnet Command: `srv dhcp nodetype`

This command can set the node type for the DHCP server.

Syntax

`srv dhcp nodetype <count>`

Syntax Description

Parameter	Description
<i>count</i>	It means to specify a type for node. 1. B-node 2. P-node 4. M-node 8. H-node

Example

```
> srv dhcp nodetype 1
> srv dhcp nodetype ?
%% srv dhcp nodetype <count>
%% 1. B-node 2. P-node 4. M-node 8. H-node
% Now: 1
```

Telnet Command: `srv dhcp primWINS`

This command can set the primary IP address for the DHCP server.

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 tftpdcl`

This command can remove the name defined for the TFTP server.

Syntax

`srv dhcp tftpdcl`

Example

```
> srv dhcp tftp TF123
> srv dhcp tftp ?
%% srv dhcp tftp <TFTP server name>
% Now: TF123
> srv dhcp tftpdcl
% The TFTP Server Name had been deleted !!!
```

Telnet Command: srv dhcp option

This command can set the custom option for the DHCP server.

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 -a, -c, -v and -x. -a: It means to set the option value by specifying the IP address. -c: It means to set option number. Available number ranges from 0 to 255. -v: It means to set option number by typing string. -x: 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. [...] 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. widx - means the WAN interface. In which, 1: WAN1 Default, 2: WAN1 Alias 1,..... 255: all WANs. ipidx - 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   Protocal      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.

<i>table</i>	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

D01    All    0.0.0.0            192.168.1.96        Y

R:Port Redirection, O:Open Ports, D:DMZ
```

Telnet Command: `switch -i`

This command is used to obtain the TX (transmitted) or RX (received) data for each connected switch.

Syntax

`switch -i [switch idx_no] [option]`

Syntax Description

Parameter	Description
<i>switch idx_no</i>	It means the index number of the switch profile.

<i>option</i>	The available commands with parameters are listed below. <i>cmd</i> <i>acc</i> <i>traffic [on/off/status/tx/rx]</i>
<i>cmd</i>	It means to send command to the client.
<i>acc</i>	It means to set the client authentication account and password.
<i>traffic [on/off/status/tx/rx]</i>	It means to turn on/off or display the data transmission from the client.

Example

```
> switch -i 1 traffic on
External Device NO. 1 traffic statistic function is enable
```

Telnet Command: switch status

This command is used to 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: 0xFFFFFFFF (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: Vigor160ac    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 signature = 0
# of lost by list = 0
```

Telnet Command: **sys pollbuf**

This command can turn on or turn off polling buffer for the router.

Syntax

`sys pollbuf [on]`

`sys pollbuf [off]`

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on pulling buffer.
<i>off</i>	It means to turn off pulling buffer.

Example

```
> sys pollbuf on
% Buffer polling is on!

> sys pollbuf off
% Buffer polling is off!
```

Telnet Command: sys britask

This command can improve triple play quality.

Syntax

`sys britask [on]`

`sys britask [off]`

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on the bridge task for improving the triple play quality.
<i>off</i>	It means to turn off the bridge task.

Example

```
> sys britask on
% bridge task is ON, now
```

Telnet Command: sys tr069

This command can set CPE settings for applying in VigorACS.

Syntax

sys tr069 get *[parm]* *[option]*

sys tr069 set *[parm]* *[value]*

sys tr069 getnoti *[parm]*

sys tr069 setnoti *[parm]* *[value]*

sys tr069 log

sys tr069 debug *[on/off]*

sys tr069 save

sys tr069 inform *[event code]*

sys tr069 port *[port num]*

sys tr069 cert_auth *[on/off]*

Syntax Description

Parameter	Description
<i>get [parm] [option]</i>	It means to get parameters for tr-069. option=<nextlevel>: only gets nextlevel for GetParameterNames.
<i>set [parm] [value]</i>	It means to set parameters for tr-069.
<i>getnoti [parm]</i>	It means to get parameter notification value.
<i>setnoti [parm] [value]</i>	It means to set parameter notification value.
<i>log</i>	It means to display the TR-069 log.
<i>debug [on/off]</i>	on: turn on the function of sending debug message to syslog. off: turn off the function of sending debug message to syslog.
<i>save</i>	It means to save the parameters to the flash memory of the router.
<i>Inform [event code]</i>	It means to inform parameters for tr069 with different event codes. [event code] includes: 0-"0 BOOTSTRAP", 1-"1 BOOT", 2-"2 PERIODIC", 3-"3 SCHEDULED", 4-"4 VALUE CHANGE", 5-"5 KICKED", 6-"6 CONNECTION REQUEST", 7-"7 TRANSFER COMPLETE", 8-"8 DIAGNOSTICS COMPLETE", 9-"M Reboot"
<i>port [port num]</i>	It means to change tr069 listen port number.
<i>cert_auth [on/off]</i>	on: turn on certificate-based authentication. off: turn off certificate-based authentication.

Example

```
> sys tr069 get Int. nextlevel
Total number of parameter is 24
```

```

Total content length of parameter is 915
InternetGatewayDevice.LANDeviceNumberOfEntries
InternetGatewayDevice.WANDeviceNumberOfEntries
InternetGatewayDevice.DeviceInfo.
InternetGatewayDevice.ManagementServer.
InternetGatewayDevice.Time.
InternetGatewayDevice.Layer3Forwarding.
InternetGatewayDevice.LANDevice.
InternetGatewayDevice.WANDevice.
InternetGatewayDevice.Services.
InternetGatewayDevice.X_00507F_InternetAcc.
InternetGatewayDevice.X_00507F_LAN.
InternetGatewayDevice.X_00507F_NAT.
InternetGatewayDevice.X_00507F_Firewall.
InternetGatewayDevice.X_00507F_Bandwidth.
InternetGatewayDevice.X_00507F_Applications.
InternetGatewayDevice.X_00507F_VPN.
InternetGatewayDevice.X_00507F_VoIP.
InternetGatewayDevice.X_00507F_WirelessLAN.
InternetGatewayDevice.X_00507F_System.
InternetGatewayDevice.X_00507F_Status.

InternetGatewayDevice.X_00507F_Diagnostics.
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---

```

Telnet Command: sys 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> [-e/-d/-s]	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
[<i><command><parameter> ...]</i>	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-v	Display the daylight saving settings.
-r	Set to factory default setting.
-e [1/0]	Enable (1) / disable (0) daylight saving.
-t [0/1/2]	Specify the saving type for daylight setting. 0 - Default 1 - Time range 2 - Yearly
-s <year> <month> <day> <hour>	Set the detailed settings of the starting day for time range type. year - must be the year after 2013. month - 1 ~ 12 day - 1 ~ 31 hour - 0 ~ 23 e.g., sys daylightsave -s 2014 3 10 12
-d <year> <month> <day> <hour>	Set the detailed settings of the ending day for time range type. year - After 2013. month - 1 ~ 12 day - 1 ~ 31 hour - 0 ~ 23 e.g., sys daylightsave -d 2014 9 10 12
-y <month> <th weekday> <day in week> <hour>	Set the detailed settings of the starting day for yearly type. month - 1 ~ 12 th weekday - 1 ~ 5, 9: last week day in week - 0:Sun, 1:Mon, 2:Tue, 3:Wed, 4:Thu, 5: Fri, 6:Sat hour - 0 ~ 23 e.g., sys daylightsave -y 9 1 0 14
-z <month> <th weekday> <day in week> <hour>	Set the detailed settings of the ending day for yearly type. month - 1 ~ 12 th weekday - 1 ~ 5, 9: last week day in week - 0:Sun, 1:Mon, 2:Tue, 3:Wed, 4:Thu, 5: Fri, 6:Sat hour - 0 ~ 23 e.g., sys daylightsave -z 3 1 6 14

Example

```
> sys daylightsave -y 9 1 0 14
% Start: Yearly on Sep 1th Sun 14:00
```

Telnet Command: sys dnsCacheTbl

This command is used to configure TTL settings which will be displayed in DNS Cache table.

Syntax

sys dnsCacheTbl [*<command><parameter>|...*]

Syntax Description

Parameter	Description
[<i><command><parameter> ...</i>]]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-l	Display DNS IPv4 entry in the DNS cache table.
-s	Display DNS IPv6 entry in the DNS cache table.
-v	Display the TTL limit value in the DNS cache table.
-t <0/n>	Set the TTL limit value in the DNS cache table. 0- No limit N - Greater than or equal to 5.
-c	Clear the DNS cache table.

Example

```
> sys dnsCacheTbl -l
%DNS Cache Table List
> sys dnsCacheTbl -t 65
% Set TTL limit: 65 seconds.
% When TTL larger than 65s , delete the DNS entry in the router's DNS cache
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. [...] means that you can type in several commands in one line.
-a <1/0>	Enable (1) or disable (0) Syslog Access Setup.
-s <1/0>	Enable (1) or disable (0) Syslog Save to Syslog Server.
-i <IP address>	Define the IP address of the Syslog server.
-d <port number>	Define the port number (1 ~ 65535) as the destination port.
-u <1/0>	Enable (1) or disable (0) Syslog Save to USB Disk.

-m <1/0>	Enable (1) or disable (0) Mail Syslog.
-f <1/0>	Enable (1) or disable (0) Firewall Log.
-v <1/0>	Enable (1) or disable (0) VPN Log.
-e <1/0>	Enable (1) or disable (0) User Access Log.
-c <1/0>	Enable (1) or disable (0) Call Log.
-w <1/0>	Enable (1) or disable (0) WAN Log.
-r <1/0>	Enable (1) or disable (0) Router/DSL Information.
-t <1/0>	Enable (1) or disable (0) AlertLog Setup.
-o <port number>	Define the port number (1 ~ 65535) for AlertLog.
-p	Update the 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.
-e <0/1>	Enable (1) or disable (0) the mail alert function.
-i <SMTP Server IP>	Set the SMTP sever IP address.
-o <SMTP Server Port>	Set the port number (1~65535) for SMTP server.
-a <Mail Address>	Set Alert Mail Reciver E-maill Address.
-r <Mail Address>	Set Mail Return E-mail Address.
-s <0/1>	Enable/Disable Use SSL.
-h <0/1>	Enable/Disable SMTP Authentication.
-u <Username>	Set Username for SMTP Authentication.
-p <Password>	Set Password for SMTP Authentication.
-l <type> <0 /1 >	"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.
-f	Reset Mail Alert Setting to factory default.
-v	Show Current Mail Alert Setting.
-R <0/1>	Set Mail Alert Reboot Debug Log Mode. 0: Limited Mode, 1: Unlimited Mode.

Example

```
> sys mailalert -e 1
> 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
-v [<i>IP version</i>]	Indicate the IP version for the IP address. 4 - IPv4. 6 - IPv6.
-w [<i>WAN_idx</i>]	WAN_idx - Indicate the WAN interface. 1 - WAN1
-l [<i>LAN_idx</i>]	LAN_idx - Indicate the LAN interface. 1 - LAN1 2 - LAN2 3 - LAN3 4 - LAN4
e [<i>0/1</i>]	Enable (1) or disable (0) the Vigor Bridge for WAN or/and LAN.
f [<i>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: wan ppp_mru

This command allows users to adjust the size of PPP LCP MRU. It is used for specific network.

Syntax

wan ppp_mru <WAN interface number> <MRU size >

Syntax Description

Parameter	Description
<WAN interface number>	Type a number to represent the physical interface. For Vigor130, the number is 1 (which means WAN1).
<MRU size >	It means the number of PPP LCP MRU. The available range is from 1400 to 1600.

Example

```
>wan ppp_mru 1 ?
% Now: 1492

> wan ppp_mru 1 1490
>
> wan ppp_mru 1 ?
% Now: 1490

> wan ppp_mru 1 1492
> wan ppp_mru 1 ?
% Now: 1492
```

Telnet Command: wan mtu

This command allows users to adjust the size of MTU for WAN1.

Syntax

wan mtu [value]

Syntax Description

Parameter	Description
value	It means the number of MTU for PPP. The available range is from 1000 to 1500. For Static IP/DHCP, the maximum number will be 1500. For PPPoE, the maximum number will be 1492. For PPTP/L2TP, the maximum number will be 1460.

Example

```
> wan mtu 1100
> wan mtu ?
Static IP/DHCP (Max MSS: 1500)
PPPoE(Max MSS: 1492)
PPTP/L2TP(Max MSS: 1460)
% wan ppp_mss <MSS size: 1000 ~ 1500>
% Now: 1100
```

Telnet Command: wan dns

This command allows 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>ttl <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
<i>wan [#]</i>	Specify which WAN interface will be tagged.
<i>tag [value]</i>	Type a number for tagging on WAN interface.
<i>enable/disable</i>	Enable: Specified WAN interface will be tagged. Disable: Disable the function of tagging on WAN interface.
<i>pri [value]</i>	It means the priority for such VLAN. The value shall be 0 ~ 7.
<i>stat</i>	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>-I [Host/IP address]</i>	Specify the IPv4 target to detect. It can be an IPv4 address or domain name.

	Host/IP address: Type the IP address/domain name of the target.
-s [mtu_size]	Set the MTU size base for Discovery. base_size: Available setting is 1000 ~ 1500.
-d [decrease size]	Set the MTU size to decrease between detections. decrease size: Available setting is 1 ~ 100.
-w	Specify the WAN interface to be detected.
-c [count]	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 [Host/IP address]	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 [mtu_size]	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
>
```

Index

6

6rd Mode, 39
6rd Prefix, 39
6rd Prefix Length, 39

A

Administrator Password, 137
Advance Mode, 105
Always On, 34, 35, 36, 37, 39
Applications, 72
ARP Cache Table, 177
ARP Detect, 26, 28
ARP Table, 59
Auth Type, 75
Auto Logout, 6
Auto-Update interval, 73
Aux. WAN IP, 70

B

Backup, 60
Backup MX, 75
Bind IP to MAC, 59
Bridge mode, 46
Bridge Mode, 29, 35, 37
Bridge Subnet, 29

C

Call Filter, 98
Channel, 41
Choose IP, 67
Codepage, 102
Comment, 60, 69
Config Backup, 11
Configuration Backup, 138
Connection Type, 75
Connectivity, 21
CSM, 121

CSV file, 158, 171
Current System Time, 76

D

Data Filter, 98
Data Flow Monitor, 183
Daylight Saving, 144
Days in a week, 77
Default Lifetime, 57
Default Preference, 57
Default Rule, 102
Details-IPv6-6in4 Static Tunnel, 37
Details-IPv6-6rd, 39
Details-Ipv6-AICCU, 34
Details-IPv6-DHCPv6 Client, 35
Details-IPv6-PPP, 31
Details-IPv6-Static IPv6, 36
Details-IPv6-TSPC, 32
Details-LAN-DMZ, 54
Details-LAN-Ethernet, 51
Determine Real WAN IP, 75
DHCP Table, 179
DHCPv6 (Stateful), 55
DHCPv6 Server, 56
Diagnostics, 174, 175
Dial-out Triggering, 175
Display Name, 23
DMZ Host, 66
DNS Cache Table, 181
DNS Server IP Address, 53
DNS Server IPv6 Address, 56
DoS Defense, 99, 113
DoS Flood Table, 187
DrayTek Banner, 111
Dynamic DNS, 72, 73
Dynamic DNS Account, 74

E

End IPv6 Address, 56
End Port, 71
Event Code, 135
Extension WAN, 57

F

File Extension Object, 169
Filter Setup, 104
Firewall, 98
Firmware Upgrade, 152
Force Update, 73

G

General Setup, 23
Group ID, 81
GUI Map, 9, 10

H

Hardware Installation, 3

I

IGMP, 80
IGMP Proxy, 80
IGMP Snooping, 80
Indicators and Connectors, 2
Installation, i
Internet Access, 25, 27, 31
IP (Internet Protocol), 22
IP Bind List, 60
IP Filters, 98
IP Object, 155
IPTV, 43
IPv4 Border Relay, 39
IPv4 Mask Length, 39
IPv6 Address, 36
IPv6 Gateway Address, 36
IPv6 Group, 161
IPv6 Neighbour Table, 178
IPv6 Object, 159
IPv6 TSPC Status, 186

ISP Access Setup, 26

K

Keep Alive Period, 136
Keyword Group, 168
Keyword Object, 166

L

LAN, 48
LAN- General Setup, 50
LAN Routed Prefix, 37
Local IP Address, 70
Log, 124
Login, 19
Login Name, 75
Logout, 11

M

Mail Extender, 75
Main Screen, 6
Management, 131, 145
Min/Max Interval Time, 57
MTU, 57
Multi-VLAN, 41

N

NAT, 61
NAT Sessions Table, 180
NAT Traversal, 79
Network Interface, 96
NS Detect, 35, 36, 37, 39

O

Objects Settings, 154
Open Ports, 69

P

Password, 26, 33, 34
Physical Connection, 11
Physical Members, 46

- Physical Mode, 23
- Ping Detect, 26, 28, 35, 36, 37, 39
- Ping Diagnosis, 182
- Ping Gateway IP, 26, 28
- Ping Interval, 26, 28
- Ping IP/Hostname, 35, 36, 37, 39
- Ping Retry, 26, 28
- Port Redirection, 62
- Port Triggering, 71
- PPPoE, 15
- PPPoE Pass-through, 26
- PPTP/L2TP, 18
- Prefix Len, 96
- Prefix Length, 36
- Primary DNS Sever**, 56
- Primary IP Address**, 53
- Primary/Secondary Ping IP, 26, 28
- Priority, 24
- Private IP, 64
- Private IP Address, 22
- Private Port, 64
- Production Registration, 19
- Provider Host, 75
- Public IP Addresss, 22
- Public Port, 64

Q

- Quick Access, 8
- Quick Start Wizard, 14

R

- Reboot System, 151
- Registering Vigor Router, 19
- Remote Endpoint IPv4 Address, 37
- Restore**, 60
- Router Advertisement Configuration, 57
- Router Name, 141
- Routing, 91
- Routing Information Protocol, 49
- Routing Table, 176

S

- Schedule, 72, 76
- Secondary DNS Server**, 56
- Secondary IP Address**, 53
- Security, 97
- Self-Signed Certificate, 148
- Server Response, 75
- Service API, 75
- Service Name, 64
- Service Provider, 74
- Service Type Group, 164
- Service Type Object, 162
- Sessions Control, 102
- Set to Factory Default, 73, 76, 92
- SLAAC(stateless), 55
- SMS/Mail Service Object, 171
- Source IP, 64, 70
- SPI, 99
- Start IPv6 Address, 56
- Start Port, 70
- Static Route, 91, 92
- Static Route for IPv6, 95
- Strict Bind**, 59
- Strict Security Firewall, 101
- STUN Settings, 136
- Subnet Prefix, 34
- Syslog/Mail Alert, 141
- System Maintenance, 132
- System Status, 133
- System time set, 76

T

- Tag value, 24
- Time and Date, 144
- Time Server, 144
- Time Zone, 144
- TR-069, 135
- Trace Route, 185
- Troubleshooting, 173
- TSPC, 32
- TTL (Time to Live), 26, 28, 35, 36, 37, 39
- Tunnel Broker, 33, 34

Tunnel ID, 34
Tunnel TTL, 37

U

Unique Local Address (ULA), 55
UPnP, 72, 79
URL Access Control, 124
URL Content Filter, 102, 121
URL Content Filter Profile, 122
Username, 26, 33, 34

V

Virtual WAN, 13

VLAN Tag, 41
VLAN Tag insertion, 24

W

WAN, 22
WAN Connection Detection, 26, 28, 35, 36, 37, 39
WAN Interface, 64, 70
WAN Type, 41
Web Console, 10
Web Feature, 125
Wildcard, 75
Wizard Mode, 105