

DrayTek

VigorNIC 132 Series VDSL2/ADSL2+ PCI-E Card

Your reliable networking solutions partner



User's Guide

V1.1

VigorNIC 132 Series VDSL2/ADSL2+ PCI-E Card

User's Guide

Version: 1.1

Firmware Version: V3.7.9

(For future update, please visit DrayTek web site)

Date: May 17, 2016

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 device via <http://www.DrayTek.com>.

Firmware & Tools Updates

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

<http://www.DrayTek.com>

European Community Declarations

Manufacturer: DrayTek Corp.

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

Product: VigorNIC 132 Series VDSL2/ADSL2+ PCI-E Card

DrayTek Corp. declares that VigorNIC 132 Series of VDSL2/ADSL2+ PCI-E Card are in compliance with the following essential requirements and other relevant provisions of R&TTE 1999/5/EC, ErP 2009/125/EC and RoHS 2011/65/EU.

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

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

This product is designed for the DSL network throughout the EC region.

Regulatory Information

Federal Communication Commission Interference Statement

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

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

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

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



More update, please visit www.draytek.com.

Table of Contents

Part I Installation	i
I-1 Introduction	1
I-1-1 Indicators and Connectors	1
I-2 Installing Your Network Card.....	2
I-3 Accessing Web Page	3
I-4 Changing Password.....	4
I-5 Dashboard.....	5
I-5-1 Virtual Panel	6
I-5-2 Name with a Link.....	6
I-5-3 Quick Access for Common Used Menu	7
I-5-4 GUI Map	8
I-5-5 Web Console	8
I-5-6 Config Backup	10
I-5-7 Logout.....	10
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-6-1 WAN1 (ADSL/VDSL2).....	15
Part II Connectivity	21
II-1 WAN.....	22
Web User Interface	23
II-1-1 General Setup	23
II-1-1-1 WAN1(ADSL/VDSL2).....	24
II-1-1-2 WAN2 (Fiber)	26
II-1-2 Internet Access.....	27
II-1-2-1 Details Page for PPPoE in WAN1 (Physical Mode: ADSL).....	29
II-1-2-2 Details Page for MPoA/Static or Dynamic IP in WAN1 (Physical Mode: ADSL) ..	32
II-1-2-3 Details Page for PPPoE/PPPoA in WAN1 (Physical Mode: VDSL).....	34
II-1-2-4 Details Page for Static or Dynamic IP in WAN1 (Physical Mode: VDSL).....	35
II-1-2-5 Details Page for PPPoE in WAN2 (Physical Mode: Fiber)	37
II-1-2-6 Details Page for Static or Dynamic IP in WAN2 (Physical Mode: Fiber)	38
II-1-2-7 Details Page for IPv6 - Offline in WAN1/WAN2	41
II-1-2-8 Details Page for IPv6 - PPP.....	41
II-1-2-9 Details Page for IPv6 - TSPC.....	42
II-1-2-10 Details Page for IPv6 - AICCU.....	43
II-1-2-11 Details Page for IPv6 - DHCPv6 Client.....	44
II-1-2-12 Details Page for IPv6 - Static IPv6	44
II-1-2-13 Details Page for IPv6 - 6in4 Static Tunnel.....	46
II-1-2-14 Details Page for IPv6 - 6rd	47
II-1-3 Multi-PVC/VLAN	49
Application Notes	53
A-1 How to configure settings for IPv6 Service in VigorNIC 132	53
II-2 LAN	65

Web User Interface	67
II-2-1 General Setup	67
<i>II-2-1-1 Details Page for LAN - Ethernet TCP/IP and DHCP Setup</i>	<i>67</i>
<i>II-2-1-2 Details Page for LAN IPv6 Setup</i>	<i>70</i>
II-2-2 Bind IP to MAC	73
II-3 NAT	75
Web User Interface	76
II-3-1 Port Redirection.....	76
II-3-2 DMZ Host	79
II-3-3 Open Ports	81
II-4 Applications	83
Web User Interface	84
II-4-1 Dynamic DNS	84
II-4-2 Schedule.....	88
II-4-3 UPnP	91
II-4-4 IGMP.....	92
II-5 Routing.....	93
Web User Interface	93
II-5-1 Static Route	93
Part III Security.....	99
III-1 Firewall.....	100
Web User Interface	102
III-1-1 General Setup	102
III-1-2 Filter Setup	106
III-1-3 DoS Defense	112
Application Notes	116
<i>A-1 How to Configure Certain Computers Accessing to Internet</i>	<i>116</i>
III-2 Central Security Management (CSM).....	120
Web User Interface	121
III-2-1 URL Content Filter Profile	121
Application Notes	125
<i>A-1 How to Create an Account for MyVigor</i>	<i>125</i>
<i>A-2 How to Block Facebook Service Accessed by the Users via URL Content Filter ..</i>	<i>128</i>
Part IV Management	131
IV-1 System Maintenance	132
Web User Interface	133
IV-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	140

IV-1-6 Time and Date.....	142
IV-1-7 Management	143
IV-1-8 Reboot System.....	146
IV-1-9 Firmware Upgrade	147
Part V Others.....	149
V-1 Objects Settings.....	150
Web User Interface	151
V-1-1 IP Object	151
V-1-2 IP Group.....	154
V-1-3 IPv6 Object.....	155
V-1-4 IPv6 Group	157
V-1-5 Service Type Object.....	158
V-1-6 Service Type Group	160
V-1-7 Keyword Object.....	162
V-1-8 Keyword Group	164
V-1-9 File Extension Object	165
Part VI Troubleshooting	167
VI-1Diagnostics	168
Web User Interface	169
VI-1-1 Dial-out Triggering.....	169
VI-1-2 Routing Table.....	170
VI-1-3 ARP Cache Table	171
VI-1-4 IPv6 Neighbour Table	172
VI-1-5 DHCP Table	173
VI-1-6 NAT Sessions Table	174
VI-1-7 DNS Cache Table	175
VI-1-8 Ping Diagnosis	176
VI-1-9 Data Flow Monitor	177
VI-1-10 Trace Route	179
VI-1-11 IPv6 TSPC Status	180
VI-1-12 DSL Status	181
VI-2 Checking If the Hardware Status Is OK or Not.....	182
VI-3 Checking If the Network Connection Settings on Your Computer Is OK or Not.....	183
VI-4 Pinging the Device from Your Computer	186
VI-5 Checking If the ISP Settings are OK or Not.....	188
VI-6 Backing to Factory Default Setting If Necessary	189
VI-7 Contacting DrayTek	190
Part VII Telnet Commands.....	192
Accessing Telnet of VigorNIC 132.....	193

Part I Installation



Installation

This part will introduce Vigor device 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.

I-1-1 Indicators and Connectors



VigorNIC 132F



VigorNIC 132

LED	Status	Explanation
WAN2	On	The Fiber WAN is connected (VigorNIC 132F). The Ethernet WAN connection is ready (VigorNIC 132).
	Blinking	It will blink while transmitting data.
DSL	On	DSL connection synchronized.
	Blinking	Quickly: DSL is handshaking. Slowly: DSL tries to synchronize.
ACT	Off	The system is not ready or is failed.
	Blinking	The system is ready and can work normally.

LED on Connector

Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
WAN2	SFP Port - Connector for accessing the Internet via fiber connection. (VigorNIC 132F) Ethernet Port - Connector for accessing the Internet via fiber connection. (VigorNIC 132)
DSL	Connector for accessing the Internet through VDSL2/ADSL2/2+. (VigorNIC 132)

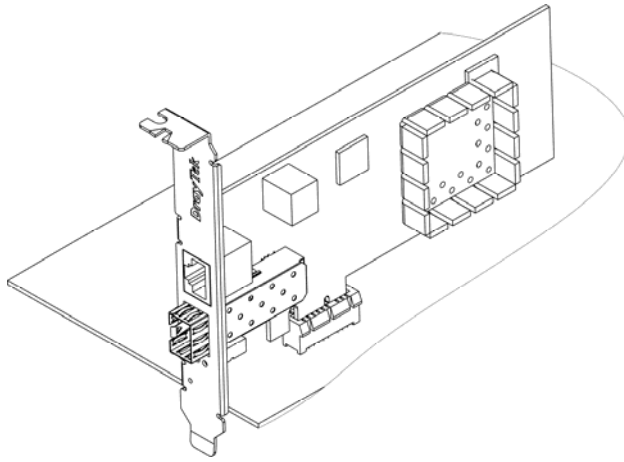
I-2 Installing Your Network Card



Info

VigorNIC 132 is being supported by the Windows 7 Generic Ethernet Driver. If you are required to install the driver manually, please download it from www.draytek.com.

1. Power off your computer.
2. Remove the cover of your computer.
3. Choose a spare card slot and insert VigorNIC 132 network card into the card slot.



4. Use RJ-11 cable (for AnnexA) or RJ-45 cable (for AnnexB) to connect DSL interface to the external VDSL splitter to establish DSL connection (VigorNIC 132). Or, insert the fiber cable into WAN2 interface to establish fiber WAN connection (VigorNIC 132F).



5. Install the cover of your computer and power on the computer.
6. Check the ACT, WAN2/DSL LEDs of VigorNIC 132 to assure WAN connections.

I-3 Accessing Web Page

1. 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.



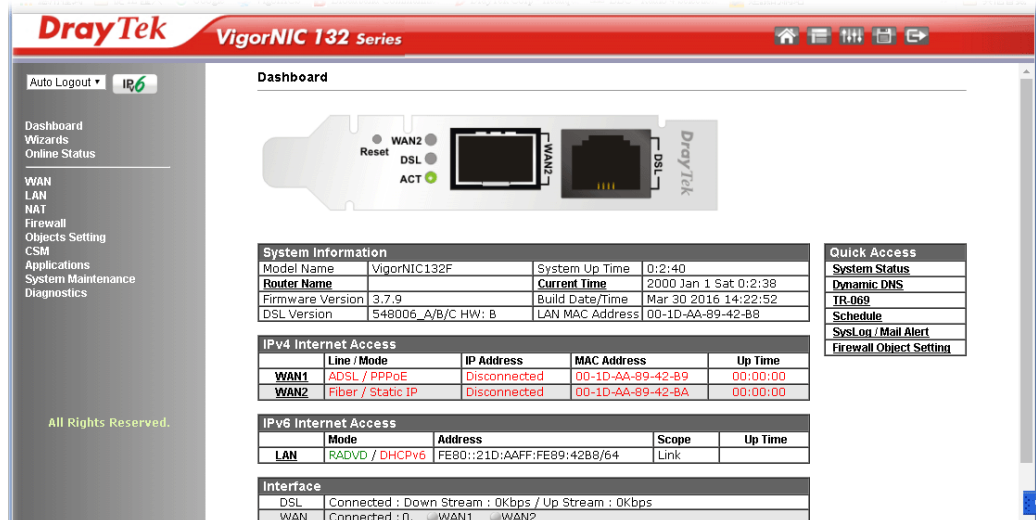
2. Please type "admin/admin" as the Username/Password and click Login.



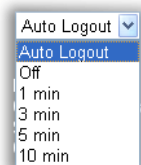
Info

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

3. Now, the Main Screen will appear.



4. 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 card.

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

System Maintenance >> Administrator Password Setup

Administrator Password

Old Password	<input type="text"/>	
New Password	<input type="text"/>	(Max. 23 characters allowed)
Confirm Password	<input type="text"/>	(Max. 23 characters allowed)

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 23 characters.

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

The screenshot shows the login page for a DrayTek VigorNIC 132 router. At the top, there is a red header with the DrayTek logo on the left and 'VigorNIC 132' on the right. Below the header is a black bar with the word 'Login' in white. The main content area is white and contains two input fields: 'Username' and 'Password'. Below the 'Password' field is a 'Login' button. At the bottom of the page, there is a copyright notice: 'Copyright © 2015 DrayTek Corp. All Rights Reserved.'



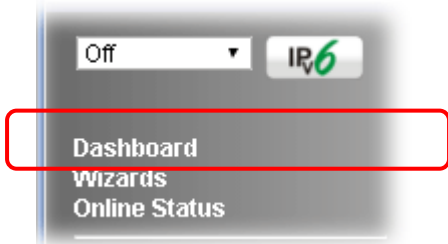
Info

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

I-5 Dashboard

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

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



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

Dashboard



System Information			
Model Name	VigorNIC132F	System Up Time	0:6:24
Router Name		Current Time	2000 Jan 1 Sat 0:6:22
Firmware Version	3.7.9	Build Date/Time	Mar 30 2016 14:22:52
DSL Version	548006_A/B/C HW: B	LAN MAC Address	00-1D-AA-89-42-B8

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	ADSL / PPPoE	Disconnected	00-1D-AA-89-42-B9	00:00:00
WAN2	Fiber / Static IP	Disconnected	00-1D-AA-89-42-BA	00:00:00

IPv6 Internet Access				
	Mode	Address	Scope	Up Time
LAN	RADVD / DHCPv6	FE80::21D:AFF:FE89:42B8/64	Link	

Interface	
DSL	Connected : Down Stream : 0Kbps / Up Stream : 0Kbps
WAN	Connected : 0, <input type="radio"/> WAN1 <input type="radio"/> WAN2
LAN	Connected : 0, <input checked="" type="radio"/> LAN1

I-5-1 Virtual Panel

On the top of the Dashboard, a virtual panel (simulating the physical panel of the router) displays the physical interface connection. It will be refreshed every five seconds. When you move and click the mouse cursor on LEDs (except ACT), WAN2, or DSL, related web setting page will be open for you to configure if required.



For detailed information about the LED display, refer to I-1-1 LED Indicators and Connectors.

I-5-2 Name with a Link

A name with a link (e.g., Router Name, Current Time, WAN1~2 and etc.) below means you can click it to open the configuration page for modification.

System Information			
Model Name	VigorNIC132F	System Up Time	21:6:0
Router Name		Current Time	2000 Jan 1 Sat 21:5:58
Firmware Version	3.7.9_RC3c	Build Date/Time	Jan 26 2016 09:51:59
DSL Version	544512_B HW: B	LAN MAC Address	00-1D-AA-89-42-B8

IPv4 Internet Access				
	Line / Mode	IP Address	MAC Address	Up Time
WAN1	ADSL / PPPoE	Disconnected	00-1D-AA-89-42-B9	00:00:00
WAN2	Fiber / Static IP	Disconnected	00-1D-AA-89-42-BA	00:00:00

IPv6 Internet Access				
	Mode	Address	Scope	Up Time
LAN	RADVD / DHCPv6	FE80::21D:AFF:FE89:42B8/64	Link	

Interface	
DSL	Connected : Down Stream : 0Kbps / Up Stream : 0Kbps
WAN	Connected : 0, <input type="radio"/> WAN1 <input type="radio"/> WAN2
<input checked="" type="checkbox"/> LAN	Connected : 0, <input checked="" type="radio"/> LAN1

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, 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.

Interface	
DSL	Connected : Down Stream : 0Kbps / Up Stream : 0Kbps
WAN	Connected : 0, <input type="radio"/> WAN1 <input type="radio"/> WAN2
<input checked="" type="checkbox"/> LAN	Connected : 0, <input checked="" type="radio"/> LAN1

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

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

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

I-5-4 GUI Map



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

GUI Map

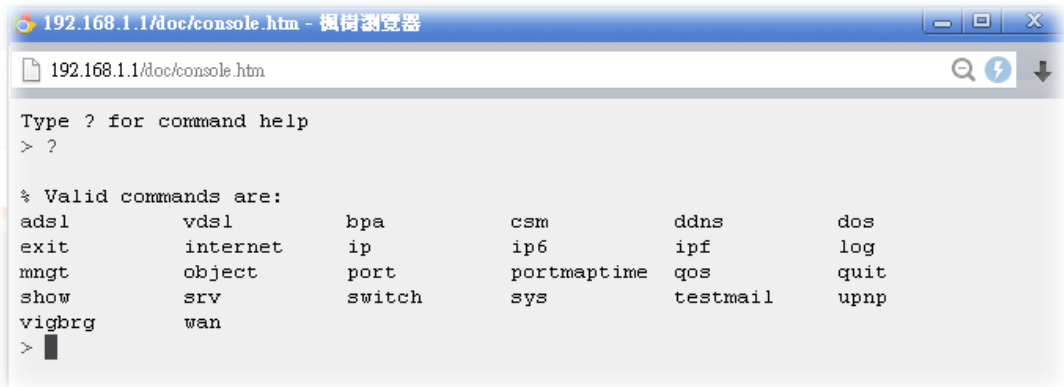
Dashboard		Applications	Dynamic DNS
Wizards	Quick Start Wizard		Schedule
Online Status	Physical Connection		UPnP
	Virtual WAN	System Maintenance	IGMP
WAN	General Setup		System Status
	Internet Access		TR-069
	Multi-PVC/LAN		Administrator Password
LAN	General Setup		Configuration Backup
	Static Route		SysLog / Mail Alert
	Bind IP to MAC		Time and Date
NAT			Management
	Port Redirection	Diagnostics	Reboot System
	DMZ Host		Firmware Upgrade
	Open Ports		Dial-out Triggering
Firewall	General Setup		Routing Table
	Filter Setup		ARP Cache Table
	DoS Defense		IPv6 Neighbour Table
Objects Setting			DHCP Table
	IP Object		NAT Sessions Table
	IP Group		Ping Diagnosis
	IPv6 Object		Data Flow Monitor
	IPv6 Group		Trace Route
			IPv6 TSPC Status
			DSL Status

I-5-5 Web Console



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

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

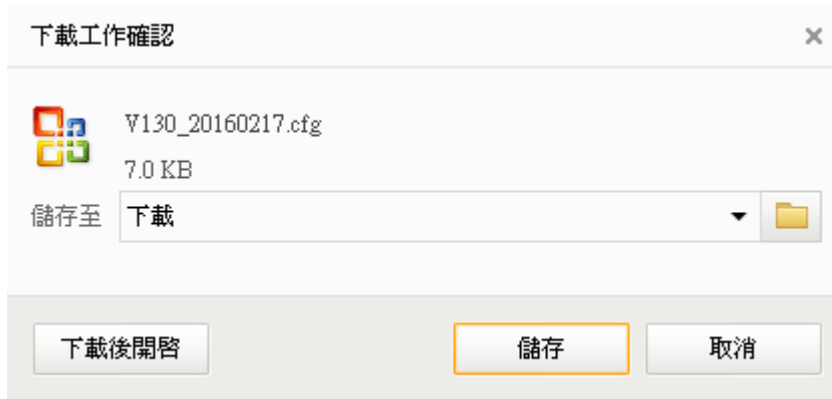


I-5-6 Config Backup



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

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



Click Save to store the setting.

I-5-7 Logout



Click this icon to exit the web user interface.

I-5-8 Online Status

Online Status
 Physical Connection
 Virtual WAN

I-5-8-1 Physical Connection

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

Physical Connection for IPv4 Protocol

Online Status

Physical Connection		System Uptime: 21:15:50				
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		12781	3648			
WAN 1 Status		>> Dial PPPoE				
Enable	Line	Name	Mode	Up Time		
Yes	ADSL		PPPoE	00:00:00		
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)	
---	---	0	0	0	0	
WAN 2 Status						
Enable	Line	Name	Mode	Up Time		
Yes	Fiber		Static IP	00:00:00		
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)	
0.0.0.0	0.0.0.0	0	0	0	0	
ADSL Information		(ADSL Firmware Version: 544512_B)				
ATM Statistics	TX Cells	RX Cells	TX CRC errs	RX CRC errs		
	0	0	0	0		
ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
		TRAINING	0	0	0	0

Physical Connection for IPv6 Protocol

Online Status

Physical Connection		System Uptime: 21:16:27	
IPv4	IPv6		
LAN Status			
IP Address FE80::21D:AAFF:FE89:42B8/64 (Link)			
TX Packets 303	RX Packets 0	TX Bytes 23634	RX Bytes 0
WAN IPv6 Status			
Enable No	Mode Offline	Up Time ---	Gateway IP ---

Detailed explanation (for IPv4) is shown below:

Item	Description
LAN Status	<p>Primary DNS-Displays the primary DNS server address for WAN interface.</p> <p>Secondary DNS -Displays the secondary DNS server address for WAN interface.</p> <p>IP Address-Displays the IP address of the LAN interface.</p> <p>TX Packets-Displays the total transmitted packets at the LAN interface.</p> <p>RX Packets-Displays the total received packets at the LAN interface.</p>
WAN1/WAN2 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, or Fiber) of this interface.</p> <p>Name - Display the name of the router.</p> <p>Mode - Displays the type of WAN connection (e.g., PPPoE).</p> <p>Up Time - Displays the total uptime of the interface.</p> <p>IP - Displays the IP address of the WAN interface.</p> <p>GW IP - Displays the IP address of the default gateway.</p> <p>TX Packets - Displays the total transmitted packets at the WAN interface.</p> <p>TX Rate - Displays the speed of transmitted octets at the WAN interface.</p> <p>RX Packets - Displays the total number of received packets at the WAN interface.</p> <p>RX Rate - Displays the speed of received octets at the WAN interface.</p>

Detailed explanation (for IPv6) is shown below:

Item	Description
LAN Status	<p>IP Address- Displays the IPv6 address of the LAN interface..</p> <p>TX Packets-Displays the total transmitted packets at the LAN interface.</p>

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



Info

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

I-5-8-2 Virtual WAN

Such page displays the virtual WAN connection information.

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

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

I-6 Quick Start Wizard

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

Quick Start Wizard

Enter login password

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

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

On the next page as shown below, please select the WAN interface that you use. If DSL interface is used, please choose WAN1; if fiber interface is used, please choose WAN2. At present, only WAN1 is available. Then click **Next** for next step.

Quick Start Wizard

WAN Interface

WAN Interface:	<input type="text" value="WAN1"/>
Display Name:	<input type="text"/>
Physical Mode:	<input type="text" value="ADSL / VDSL2"/>
DSL Mode:	<input type="text" value="ADSL only"/>
Physical Type:	<input type="text" value="Auto negotiation"/>

I-6-1 WAN1 (ADSL/VDSL2)

WAN1 is specified for ADSL or VDSL2 connection.

Quick Start Wizard

WAN Interface

WAN Interface:	WAN1 ▾
Display Name:	<input type="text"/>
Physical Mode:	ADSL / VDSL2
DSL Mode:	ADSL only ▾
Physical Type:	Auto negotiation ▾

Available settings are explained as follows:

Item	Description
Display Name	Type a name to identify such WAN.
DSL Mode	Specify the physical mode (Auto, VDSL2 only or ADSL only) for such router manually.

You have to select the appropriate Internet access type according to the information from your ISP. For example, you should select PPPoE mode if the ISP provides you PPPoE interface. In addition, the field of For ADSL Only will be available only when ADSL is detected. Then click Next for next step.

I-6-1-1 PPPoE/PPPoA

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

Quick Start Wizard

Connect to Internet

WAN 1

Protocol PPPoE / PPPoA ▼

For ADSL Only:

Encapsulation PPPoE LLC/SNAP ▼

VPI Auto detect

VCI

Fixed IP Yes No(Dynamic IP)

IP Address

Subnet Mask

Default Gateway

Primary DNS

Second DNS

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

Tag value (0~4095)

Priority (0~7)

< Back
Next >
Finish
Cancel

Available settings are explained as follows:

Item	Description
Protocol	<p>There are two modes offered for you to choose for WAN1 interface.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> ▼ PPPoE / PPPoA MPoA / Static or Dynamic IP </div> <p>Choose PPPoE/PPPoA as the protocol.</p>
For ADSL Only	<p>Such field is provided for ADSL only. You have to choose encapsulation and type the values for VPI and VCI. Or, click Auto detect to find out the best values.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> ▼ PPPoE LLC/SNAP PPPoE VC MUX PPPoA LLC/SNAP PPPoA VC MUX </div>
Fixed IP	Click Yes to enable Fixed IP feature.
IP Address	Type the IP address if Fixed IP is enabled.
Subnet Mask	Type the subnet mask.
Default Gateway	Type the IP address as the default gateway.

Primary DNS	Type in the primary IP address for the router.
Second DNS	Type in secondary IP address for necessity in the future.
VLAN Tag insertion (VDSL2)/(ADSL)	The settings configured in this field are available for WAN1 and WAN2. Enable - Enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the WAN while sending them out. Please type the tag value and specify the priority for the packets sending by WAN1. Disable - Disable the function of VLAN with tag. Tag value - Type the value as the VLAN ID number. The range is from 0 to 4095. Priority - Type the packet priority number for such VLAN. The range is from 0 to 7.
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**. Manually enter the Username/Password provided by your ISP

Quick Start Wizard

Set PPPoE / PPPoA

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

Available settings are explained as follows:

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

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

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

Quick Start Wizard

Please confirm your settings:

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

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

Quick Start Wizard Setup OK!

- Now, you can enjoy surfing on the Internet.

I-6-1-2 MPoA / Static or Dynamic IP

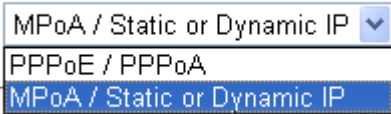
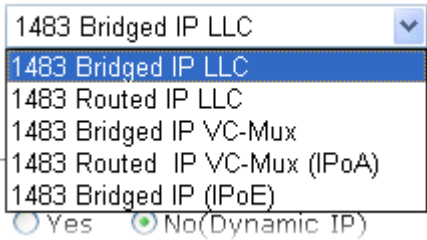
1. Choose **WAN1** as WAN Interface and click the **Next** button; you will get the following page.

Quick Start Wizard

Connect to Internet

WAN 1	
Protocol	MPoA / Static or Dynamic IP ▼
For ADSL Only:	
Encapsulation	1483 Bridged IP LLC ▼
VPI	0 <input type="button" value="Auto detect"/>
VCI	33
Fixed IP	<input type="radio"/> Yes <input checked="" type="radio"/> No(Dynamic IP)
IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Default Gateway	<input type="text"/>
Primary DNS	8.8.8.8
Second DNS	8.8.4.4
VLAN Tag insertion (ADSL):	Disable ▼

Available settings are explained as follows:

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

Second DNS	Type in secondary IP address for necessity in the future.
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. Please type in the IP address/mask/gateway information originally provided by your ISP. Then click **Next** for viewing summary of such connection.

Quick Start Wizard

Please confirm your settings:

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

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

Quick Start Wizard Setup OK!

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

Part II Connectivity



WAN

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



LAN

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



NAT

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



Applications

DNS, IGMP, UpnP



Routing

Static Route

II-1 WAN

It allows users to access Internet.

Basics of Internet Protocol (IP) Network

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

From 10.0.0.0 to 10.255.255.255
From 172.16.0.0 to 172.31.255.255
From 192.168.0.0 to 192.168.255.255

What are Public IP Address and Private IP Address

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

Get Your Public IP Address from ISP

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

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

Web User Interface

II-1-1 General Setup

This section will introduce some general settings of Internet and explain the connection modes for WAN1, WAN2 and WAN3/WAN4 in details.

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

This webpage allows you to set general setup for WAN1, WAN2, WAN3 and WAN4 respectively. In default, WAN2 is disabled. If you want to enable it, simply click the WAN2 link and select Yes in the field of Enable.

For VigorNIC 132 Series except VigorNIC 132L and VigorNIC 132Ln

WAN >> General Setup

Setup	Index	Enable	Physical Mode/Type
	WAN1	V	ADSL/-
	WAN2	v	Fiber/Auto negotiation

OK

Available settings are explained as follows:

Item	Description
Index	Click the WAN interface link under Index to access into the WAN configuration page.
Enable	V means such WAN interface is enabled and ready to be used.
Physical Mode / Type	Display the physical mode and physical type of such WAN interface.



Info In default, each WAN port is enabled.

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

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

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

WAN >> General Setup

WAN 1

Enable:	Yes ▾
Display Name:	<input type="text"/>
Physical Mode:	ADSL
DSL Mode:	VDSL2 only ▾
Physical Type:	Auto ▾
VLAN Tag insertion (ADSL):	VDSL2 only channel 1
Tag value:	<input type="text"/> (0~4095)
Priority:	<input type="text"/> (0~7)
VLAN Tag insertion (VDSL2):	Disable ▾
Tag value:	<input type="text"/> (0~4095)
Priority:	<input type="text"/> (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
Enable	Choose Yes to invoke the settings for this WAN interface. Choose No to disable the settings for this WAN interface.
Display Name	Type the description for such interface.
Physical Mode	Display the physical mode of such interface. If VDSL2 is detected, this field will display "VDSL2"; if ADSL is detected, it will display "ADSL".
DSL Mode	Specify the physical mode (VDSL2 or ADSL) for such router manually.
Physical Type	For such interface, no type can be selected.
VLAN Tag insertion (ADSL)	The settings configured in this field are available for ADSL. Enable - Enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the WAN while sending them out. Please type the tag value and specify the priority for the packets sending by WAN1. Disable - Disable the function of VLAN with tag. Tag value - Type the value as the VLAN ID number. The range is form 0 to 4095. Priority - Type the packet priority number for such VLAN. The range is from 0 to 7.

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

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

II-1-1-2 WAN2 (Fiber)

WAN2 can be configured for general setting for fiber connection.

WAN >> General Setup

WAN 2

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

Available settings are explained as follows:

Item	Description
Enable	Choose Yes to invoke the settings for this WAN interface. Choose No to disable the settings for this WAN interface.
Display Name	Type the description for such WAN interface.
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 WAN1.</p> <p>Disable - Disable the function of VLAN with tag.</p> <p>Tag value - Type the value as the VLAN ID number. The range is form 0 to 4095.</p> <p>Priority - Type the packet priority number for such VLAN. The range is from 0 to 7.</p>

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

II-1-2 Internet Access

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

Access Mode for ADSL/VDSL2,

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode		
WAN1		ADSL	PPPoE / PPPoA	▼	Details Page IPv6
WAN2		Fiber	None		Details Page IPv6
			PPPoE / PPPoA		
			MPOA (RFC1483/2684)		

Note: Only one WAN can support IPv6.

Advanced You can configure DHCP client options here.

Access Mode for Fiber,

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode		
WAN1		ADSL	PPPoE / PPPoA	▼	Details Page IPv6
WAN2		Fiber	Static or Dynamic IP	▼	Details Page IPv6
			None		
			PPPoE		
			Static or Dynamic IP		

Note: Only one WAN can support IPv6.

Advanced You can configure DHCP client options here.

Available settings are explained as follows:

Item	Description
Index	Display the WAN interface.
Display Name	It shows the name of the WAN1/WAN2 that entered in general setup.
Physical Mode	It shows the physical connection for WAN1(ADSL/VDSL2)/WAN2 (Fiber) according to the real network connection.
Access Mode	Use the drop down list to choose a proper access mode. The details page of that mode will be popped up. If not, click Details Page for accessing the page to configure the settings.
Details Page	This button will open different web page (based on IPv4) according to the access mode that you choose in WAN interface. Note that Details Page will be changed slightly based on ADSL/VDSL2 physical mode specified on WAN>>General Setup.
IPv6	This button will open different web page (based on Physical Mode) to setup IPv6 Internet Access Mode for WAN

	interface.															
Advanced	<p>This button allows you to configure DHCP client options. DHCP packets can be processed by adding option number and data information when such function is enabled and configured.</p> <p>WAN >> Internet Access</p> <div data-bbox="708 427 1402 790" style="border: 1px solid black; padding: 5px;"> <p>DHCP Client Options Status</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="5">Options List</th> </tr> <tr> <th style="width: 10%;">Enable</th> <th style="width: 20%;">Interface</th> <th style="width: 15%;">Option</th> <th style="width: 15%;">Type</th> <th style="width: 40%;">Data</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"> </td> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table> <p>Enable: <input checked="" type="checkbox"/></p> <p>Interface: <input type="checkbox"/> All <input checked="" type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3 <input type="checkbox"/> WAN4 <input type="checkbox"/> WAN5</p> <p>Option Number: <input type="text"/></p> <p>Data Type: <input checked="" type="radio"/> ASCII Character (EX: Option:18, Data:/path) <input type="radio"/> Hexadecimal Digit (EX: Option:18, Data:2F70617468) <input type="radio"/> Address List (EX: Option:44, Data:172.16.2.10,172.16.2.20...)</p> <p>Data: <input type="text"/></p> <p style="text-align: right;"> <input type="button" value="Add"/> <input type="button" value="Update"/> <input type="button" value="Delete"/> </p> </div> <p>Enable/Disable - Enable/Disable the function of DHCP Option. Each DHCP option is composed by an option number with data. For example, Option number: 100 Data: abcd</p> <p>When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets.</p> <p>Interface - Specify the WAN interface(s) that will be overwritten by such function. WAN5 ~ WAN7 can be located under WAN>>Multi-PVC/VLAN.</p> <p>Option Number - Type a number for such function.</p> <p>Data Type - Choose the type (ASCII or Hex) for the data to be stored.</p> <p>Data - Type the content of the data to be processed by the function of DHCP option.</p>	Options List					Enable	Interface	Option	Type	Data					
Options List																
Enable	Interface	Option	Type	Data												



Info

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

	<p>network can use another set of PPPoE session (different with the Host PC) to access into Internet.</p> <p>Note: To have PPPoA Pass-through, please choose PPPoA protocol and check the box(es) here. The router will behave like a modem which only serves the PPPoE client on the LAN. That's, the router will offer PPPoA dial-up connection.</p>
WAN Connection Detection	<p>Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.</p> <p>Mode - Choose ARP Detect or Ping Detect for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items.</p> <ul style="list-style-type: none"> ● Ping 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 device can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation.
MTU	<p>It means Max Transmit Unit for packet. Click Detect to open the following dialog.</p>
ISP Access Setup	<p>Enter your allocated username, password and authentication parameters according to the information provided by your ISP.</p> <p>Username - Type in the username provided by ISP in this field.</p> <p>Password - Type in the password provided by ISP in this field.</p> <p>Separate Account for ADSL - In default, WAN1 supports VDSL2/ADSL and uses the same PPPoE account and password for connection. If required, you can configure another account and password for ADSL connection by checking this box. If it is checked, the system will ask you to type another group of account and password additionally.</p> <p>PPP Authentication - Select PAP only or PAP or CHAP for PPP.</p>
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 would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.</p>

WAN1 IP Alias (Multi-NAT)

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

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

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

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

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

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

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

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

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

WAN >> Internet Access

WAN 1

PPPoE / PPPoA	MPoA / Static or Dynamic IP	IPv6
<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Modem Settings (for ADSL only) Multi-PVC channel: Channel 2 Encapsulation: 1483 Bridged IP LLC VPI: 0 VCI: 88 Modulation: Multimode		
WAN Connection Detection Mode: ARP Detect Ping IP: <input type="text"/> TTL: <input type="text"/>		
MTU : 1492 (Max: 1500)		
RIP Protocol <input type="checkbox"/> Enable RIP		
Bridge Mode <input type="checkbox"/> Enable Bridge Mode		
WAN IP Network Settings WAN IP Alias		<input checked="" type="radio"/> Obtain an IP address automatically Router Name: Vigor* Domain Name: <input type="text"/> * <input checked="" type="radio"/> Specify an IP address IP Address: <input type="text"/> Subnet Mask: <input type="text"/> Gateway IP Address: <input type="text"/>
		<input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: 00 · 1D · AA · 89 · 42 · B9
		DNS Server IP Address Primary IP Address: 8.8.8.8 Secondary IP Address: 8.8.4.4

*: Required for some ISPs

OK Cancel

Available settings are explained as follows:

Item	Description
Enable/Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
Modem Settings (for ADSL only)	Set up the DSL parameters required by your ISP. These settings configured here are specified for ADSL only. Multi-PVC channel - The selections displayed here are determined by the page of Internet Access >> Multi-PVC/VLAN . Select M-PVCs Channel means no selection will be chosen. Encapsulating Type - Drop down the list to choose the type provided by ISP. VPI - Type in the value provided by ISP. VCI - Type in the value provided by ISP. Modulation -Default setting is Multimode. Choose the one that fits the requirement of your router.

Modem Setting (for ADSL only)	It is not necessary to configure settings in these fields for modem settings are prepared for ADSL only.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode - Choose ARP Detect , Ping Detect or Always On for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items. <ul style="list-style-type: none"> ● Ping 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 device can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation.
MTU	It means Max Transmit Unit for packet.
RIP Protocol	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.
Bridge Mode	Enable Bridge Mode - If the function is enabled, the router will work as a bridge modem.
WAN IP Network Settings	This group allows you to obtain an IP address automatically and allows you type in IP address manually. WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 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. Obtain an IP address automatically - Click this button to obtain the IP address automatically. <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. Specify an IP address - Click this radio button to specify some data. <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. Default MAC Address - Type in MAC address for the router. You can use Default MAC Address or specify another MAC address for your necessity. Specify a MAC Address - Type in the MAC address for the router manually.
DNS Server IP Address	Type in the primary IP address for the router. If necessary, type in secondary IP address for necessity in the future.

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

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

WAN >> Internet Access

WAN 1

PPPoE	Static or Dynamic IP	IPv6
<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
ISP Access Setup Service Name (Optional) <input type="text"/> Username <input type="text"/> Password <input type="text"/> Index(1-15) in Schedule Setup: => <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>		PPP/MP Setup PPP Authentication <input type="text" value="PAP or CHAP"/> Idle Timeout <input type="text" value="-1"/> second(s)
WAN Connection Detection Mode <input type="text" value="ARP Detect"/> Ping IP <input type="text"/> TTL: <input type="text"/>		IP Address Assignment Method (IPCP) <input type="text" value="WAN IP Alias"/> Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address <input type="text"/> <input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: <input type="text" value="00"/> <input type="text" value="1D"/> <input type="text" value="AA"/> <input type="text" value="89"/> <input type="text" value="42"/> <input type="text" value="B9"/>
MTU <input type="text" value="1492"/> (Max:1492)		

Available settings are explained as follows:

Item	Description
Enable/Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
ISP Access Setup	<p>Enter your allocated username, password and authentication parameters according to the information provided by your ISP.</p> <p>Service Name (Optional) - Enter the description of the specific network service.</p> <p>Username - Type in the username provided by ISP in this field.</p> <p>Password - Type in the password provided by ISP in this field.</p> <p>Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Applications >> Schedule web page and you can use the number that you have set in that web page.</p>
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"> ● Ping 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 device can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation.
MTU	It means Max Transmit Unit for packet.

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

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

II-1-2-4 Details Page for Static or Dynamic IP in WAN1 (Physical Mode: VDSL)

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

WAN >> Internet Access

WAN 1

PPPoE	Static or Dynamic IP	IPv6
<input type="radio"/> Enable <input checked="" type="radio"/> Disable	WAN IP Network Settings WAN IP Alias	
Keep WAN Connection <input type="checkbox"/> Enable PING to keep alive PING to the IP: <input type="text"/> PING Interval: <input type="text"/> minute(s)	<input type="radio"/> Obtain an IP address automatically Router Name: <input type="text" value="Vigor"/> * Domain Name: <input type="text"/> * <input checked="" type="radio"/> Specify an IP address IP Address: <input type="text"/> Subnet Mask: <input type="text"/> Gateway IP Address: <input type="text"/>	
WAN Connection Detection Mode: <input type="text" value="ARP Detect"/> Ping IP: <input type="text"/> TTL: <input type="text"/>	<input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: <input type="text" value="00"/> <input type="text" value="1D"/> <input type="text" value="AA"/> <input type="text" value="89"/> <input type="text" value="42"/> <input type="text" value="B9"/>	
MTU <input type="text" value="1492"/> (Max:1500)	DNS Server IP Address Primary IP Address: <input type="text" value="8.8.8.8"/> Secondary IP Address: <input type="text" value="8.8.4.4"/>	
RIP Protocol <input type="checkbox"/> Enable RIP		

*: Required for some ISPs

OK Cancel

Available settings are explained as follows:

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

Enable/Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
Keep WAN Connection	Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time. Check Enable PING to keep alive box to activate this function. PING to the IP - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive. PING Interval - Enter the interval for the system to execute the PING operation.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode - Choose ARP Detect 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. ● Ping 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 device can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation.
MTU	It means Max Transmit Unit for packet.
RIP Protocol	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.
WAN IP Network Settings	This group allows you to obtain an IP address automatically and allows you type in IP address manually. WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 32 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog. Obtain an IP address automatically - Click this button to obtain the IP address automatically. ● Router Name - Type in the router name provided by ISP. ● Domain Name - Type in the domain name that you have assigned. Specify an IP address - Click this radio button to specify some data. ● IP Address - Type in the private IP address. ● Subnet Mask - Type in the subnet mask. ● Gateway IP Address - Type in gateway IP address. Default MAC Address - Type in MAC address for the router. You can use Default MAC Address or specify another MAC address for your necessity. Specify a MAC Address - Type in the MAC address for the router manually.

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

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

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

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

WAN >> Internet Access

WAN 2

PPPoE	Static or Dynamic IP	IPv6
<input type="radio"/> Enable <input checked="" type="radio"/> Disable	PPP/MP Setup PPP Authentication: PAP or CHAP ▾ Idle Timeout: 180 second(s)	IP Address Assignment Method (IPCP) <input type="button" value="WAN IP Alias"/> Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address: <input type="text"/>
ISP Access Setup Service Name (Optional): <input type="text"/> Username: <input type="text"/> Password: <input type="text"/> Index(1-15) in Schedule Setup: => <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>	IP Address Assignment Method (IPCP) <input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: <input type="text" value="00"/> · <input type="text" value="1D"/> · <input type="text" value="AA"/> · <input type="text" value="89"/> · <input type="text" value="42"/> · <input type="text" value="BA"/>	
WAN Connection Detection Mode: ARP Detect ▾ Ping IP: <input type="text"/> TTL: <input type="text"/>		
MTU : 1500 (Max:1492)		

Available settings are explained as follows:

Item	Description
Enable/Disable	Click Enable for activating this function. If you click Disable, this function will be closed and all the settings that you adjusted in this page will be invalid.
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP. Service Name (Optional) - Enter the description of the specific network service. Username - Type in the username provided by ISP in this field. The maximum length of the user name you can set is 63 characters. Password - Type in the password provided by ISP in this field. The maximum length of the password you can set is 62 characters. Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode - Choose ARP Detect or Ping Detect for the system to

	<p>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"> ● Ping 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 device can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation.
MTU	It means Max Transmit Unit for packet.
PPP/MP Setup	<p>PPP Authentication - Select PAP only or PAP or CHAP for PPP.</p> <p>Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action.</p>
IP Address Assignment Method (IPCP)	<p>Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function.</p> <p>WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 32 public IP addresses other than the current one you are using. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.</p> <p>Fixed IP - Click Yes to use this function and type in a fixed IP address in the box of Fixed IP Address.</p> <p>Default MAC Address - You can use Default MAC Address or specify another MAC address by typing on the boxes of MAC Address for the router.</p> <p>Specify a MAC Address - Type the MAC address for the router manually.</p>

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

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

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

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

WAN >> Internet Access

WAN 2

PPPoE	Static or Dynamic IP	IPv6
<input checked="" type="radio"/> Enable <input type="radio"/> Disable Keep WAN Connection <input type="checkbox"/> Enable PING to keep alive PING to the IP: <input type="text"/> PING Interval: <input type="text"/> minute(s) WAN Connection Detection Mode: <input type="text" value="ARP Detect"/> Ping IP: <input type="text"/> TTL: <input type="text"/> MTU : <input type="text" value="1500"/> (Max:1500) RIP Protocol <input type="checkbox"/> Enable RIP	WAN IP Network Settings <input type="text" value="WAN IP Alias"/> <input type="radio"/> Obtain an IP address automatically Router Name: <input type="text"/> * Domain Name: <input type="text"/> * <input checked="" type="radio"/> Specify an IP address IP Address: <input type="text"/> Subnet Mask: <input type="text"/> Gateway IP Address: <input type="text"/> <input type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: <input type="text" value="00"/> <input type="text" value="1D"/> <input type="text" value="AA"/> <input type="text" value="89"/> <input type="text" value="42"/> <input type="text" value="BA"/> DNS Server IP Address Primary IP Address: <input type="text" value="8.8.8.8"/> Secondary IP Address: <input type="text" value="8.8.4.4"/>	

*: Required for some ISPs

OK Cancel

Available settings are explained as follows:

Item	Description
Enable / Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
Keep WAN Connection	Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time. Check Enable PING to keep alive box to activate this function. PING to the IP - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive. PING Interval - Enter the interval for the system to execute the PING operation.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode - Choose ARP Detect , Ping Detect or Always On for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items. <ul style="list-style-type: none"> ● Ping 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 device can check if the WAN connection is on or off. ● TTL (Time to Live) - Set TTL value of PING operation.
MTU	It means Max Transmit Unit for packet.
RIP Protocol	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.

WAN IP Network Settings	<p>This group allows you to obtain an IP address automatically and allows you type in IP address manually.</p> <p>WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 32 public IP addresses other than the current one you are using.</p> <p>Obtain an IP address automatically - Click this button to obtain the IP address automatically if you want to use Dynamic IP mode.</p> <ul style="list-style-type: none"> ● Router Name: Type in the router name provided by ISP. ● Domain Name: Type in the domain name that you have assigned. <p>Specify an IP address - Click this radio button to specify some data if you want to use Static IP mode.</p> <ul style="list-style-type: none"> ● IP Address: Type the IP address. ● Subnet Mask: Type the subnet mask. ● Gateway IP Address: Type the gateway IP address. <p>Default MAC Address: Click this radio button to use default MAC address for the router.</p> <p>Specify a MAC Address: Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the Specify a MAC Address and enter the MAC address in the MAC Address field.</p>
DNS Server IP Address	<p>Type in the primary IP address for the router if you want to use Static IP mode. If necessary, type in secondary IP address for necessity in the future.</p>

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

II-1-2-7 Details Page for IPv6 – Offline in WAN1/WAN2

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

Internet Access >> IPv6

WAN 2

Internet Access Mode	
Connection Type	Offline ▾
OK	

II-1-2-8 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 device 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	
Connection Type	PPP ▾
<input type="radio"/> Auto <input checked="" type="radio"/> Manual	
Prefix Configuration	
Subnet Prefix	<input type="text"/> / <input type="text"/> (default:64)
Note : IPv4 WAN setting should be PPPoE client.	
OK	

Available settings are explained as follows:

Item	Description
Prefix Configuration	Type the IPv6 address with the value of subnet. If you choose Auto, there is no need to configure such setting.

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

Online Status

Physical Connection System Uptime: 0:2:32

IPv4		IPv6	
LAN Status			
IP Address			
2001:B010:7300:201:21D:AFF:FEA6:2568/64 (Global)			
FE80::21D:AFF:FEA6:2568/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
7	4	690	328
WAN2 IPv6 Status >> Drop PPP			
Enable	Mode	Up Time	
Yes	PPP	0:02:08	
IP		Gateway IP	
2001:B010:7300:201:21D:AFF:FEA6:256A/128 (Global)		FE80::9D:1A00:242:AD52	
FE80::1D:AFF:FEA6:256A/128 (Link)			
DNS IP			
2001:8000:168::1			
2001:8000:168::2			
TX Packets	RX Packets	TX Bytes	RX Bytes
7	9	544	1126



Info

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

II-1-2-9 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.

Internet Access >> IPv6

WAN 1

Internet Access Mode	
Connection Type	<input type="text" value="TSPC"/>
TSPC Configuration	
Username	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>
Tunnel Broker	<input type="text"/>
<input type="button" value="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 /Confirm 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.

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

II-1-2-10 Details Page for IPv6 – AICCU

Internet Access >> IPv6

WAN 1

Internet Access Mode
Connection Type AICCU ▼

AICCU Configuration

Always On

Username

Password

Confirm Password

Tunnel Broker

Subnet Prefix /

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

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 / Confirm 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.
Subnet Prefix	Type the subnet prefix address obtained from service provider. The maximum length of the prefix you can set is 128 characters.

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

II-1-2-11 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
 Identity Association: Prefix Delegation Non-temporary Address
 IAID (Identity Association ID):

OK

Available settings are explained as follows:

Item	Description
Identify Association	Choose Prefix Delegation or Non-temporary Address as the identify association.
IAID	Type a number as IAID.

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

II-1-2-12 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:

Current IPv6 Address Table

Index	IPv6 Address/Prefix Length	Scope

Static IPv6 Gateway Configuration
 IPv6 Gateway Address:

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. 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.

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

II-1-2-13 Details Page for IPv6 – 6in4 Static Tunnel

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

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

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

Internet Access >> IPv6

WAN 1

Internet Access Mode	
Connection Type	6in4 Static Tunnel ▾
6in4 Static Tunnel	
Remote Endpoint IPv4 Address	<input type="text"/>
6in4 IPv6 Address	<input type="text"/> / <input type="text" value="64"/> (default:64)
LAN Routed Prefix	<input type="text"/> / <input type="text" value="64"/> (default:64)
Tunnel TTL	<input type="text" value="255"/> (default:255)
<input type="button" value="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.

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

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

Online Status

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

II-1-2-14 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 Settings
 6rd Mode: Auto 6rd Static 6rd

Static 6rd Settings

IPv4 Border Relay:

IPv4 Mask Length:

6rd Prefix:

6rd Prefix Length:

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.

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

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

Online Status

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

II-1-3 Multi-PVC/VLAN

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

II-1-3-1 General

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

WAN >> Multi-PVC/VLAN

Multi-PVC/VLAN

General		Advanced		
Channel	Enable	WAN Type	VPI/VCI	VLAN Tag
1	Yes	ADSL	0/33	None
2	Yes	Fiber(WAN2)		None
3. WAN3	No	VDSL		None
4. WAN4	No	VDSL		None
5. WAN5	No	VDSL		None

OK Cancel

Available settings are explained as follows:

Item	Description
Channel	Display the number of each channel. Channels 1 and 2 are used by the Internet Access web user interface and can not be configured here. Channels 3 ~ 5 are configurable.
Enable	Display whether the settings in this channel are enabled (Yes) or not (No).
WAN Type	Displays the physical medium that the channel will use.
VPI/VCI	Display the value for VPI and VCI.
VLAN Tag	Displays the VLAN tag value that will be used for the packets traveling on this channel.

Click any index (3-5) to get the following web page:

WAN >> Multi-PVC/VLAN >> Channel 3

Multi-PVC/VLAN Channel 3: Enable Disable

WAN Type :

General Settings

VLAN Header

VLAN Tag:

Priority:

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

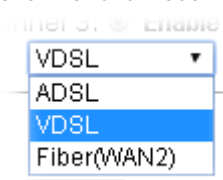
Open WAN Interface for this Channel

WAN Application:

WAN Setup:

<p>ISP Access Setup</p> <p>ISP Name <input type="text"/></p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>PPP Authentication <input type="text" value="PAP or CHAP"/></p> <p><input type="checkbox"/> Always On</p> <p>Idle Timeout <input type="text" value="86400"/> second(s)</p> <p>IP Address From ISP</p> <p>Fixed IP <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP)</p> <p>Fixed IP Address <input type="text"/></p>	<p>WAN IP Network Settings</p> <p><input type="radio"/> Obtain an IP address automatically</p> <p>Router Name <input type="text" value="Vigor"/>*</p> <p>Domain Name <input type="text"/>*</p> <p>*: Required for some ISPs</p> <p><input checked="" type="radio"/> Specify an IP address</p> <p>IP Address <input type="text"/></p> <p>Subnet Mask <input type="text"/></p> <p>Gateway IP Address <input type="text"/></p> <p>DNS Server IP Address</p> <p>Primary IP Address <input type="text" value="8.8.8.8"/></p> <p>Secondary IP Address <input type="text" value="8.8.4.4"/></p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Available settings are explained as follows:

Item	Description
Multi-VLAN Channel 3~5	Enable - Click it to enable the configuration of this channel. Disable - Click it to disable the configuration of this channel.
WAN Type	The connections and interfaces created in every channel may select a specific WAN type to be built upon. In the Multi-PVC application, only the Ethernet WAN type is available. The user will be able to select the physical WAN interface the channel shall use here. 
General Settings	VLAN Header - Check the box to enable the following two options. VLAN Tag - Type the value as the VLAN ID number. Valid settings are in the range from 1 to 4095. The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value. Priority - Choose the number to determine the packet

	priority for such VLAN. The range is from 0 to 7.
<p>Open WAN Interface for this Channel</p>	<p>Check the box to enable relating function.</p> <p>WAN Application -</p> <ul style="list-style-type: none"> ● Management - It can be specified for general management (Web configuration/telnet/TR069). If you choose Management, the configuration for this VLAN will be effective for Web configuration/telnet/TR069. ● IPTV - The IPTV configuration will allow the WAN interface to send IGMP packets to IPTV servers. <p>WAN Setup -</p> <p>It is available only when VDSL or Ethernet (WAN2) is selected as WAN Type. Choose PPPoE/PPPoA Client or Static or Dynamic IP as the WAN mode for such channel.</p> <ul style="list-style-type: none"> ● If PPPoE/PPPoA Client is selected as WAN Setup, you have to configure the settings listed under ISP Access Setup. Enter your allocated username, password and authentication parameters according to the information provided by your ISP. <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. <p>PPP Authentication - Select PAP only or PAP or CHAP for PPP.</p> <ul style="list-style-type: none"> ➤ Always On - Check it to keep the network connection always. ➤ Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action. <p>Fixed IP - Click Yes to use this function and type in a fixed IP address in the box of Fixed IP Address.</p> <ul style="list-style-type: none"> ● If Static or Dynamic IP is selected as WAN Setup, you have to configure the settings listed under WAN IP Network Settings. <ul style="list-style-type: none"> Obtain an IP address automatically - Click this button to obtain the IP address automatically. <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. Specify an IP address - Click this radio button to specify some data. <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.

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.

WAN >> Multi-PVC/LAN

Multi-PVC/LAN

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 ▼

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.

OK Cancel

Available settings are explained as follows:

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

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

Application Notes

A-1 How to configure settings for IPv6 Service in VigorNIC 132

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

- **Dual Stack**

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

- **Tunnel**

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

- **Translation**

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

Before configuring the settings on VigorNIC 132, you need to know which connection type that your IPv6 service used.



Info

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

I. Configuring the WAN Settings

For the IPv6 WAN settings for VigorNIC 132, there are five connection types to be chosen: PPP, TSPC, AICCU, DHCPv6 Client and Static IPv6.

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

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode		
WAN1		ADSL	PPPoE / PPPoA	Details Page	IPv6
WAN2		Fiber	Static or Dynamic IP	Details Page	IPv6

Note: Only one WAN can support IPv6.

Advanced You can configure DHCP client options here.



Info

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

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

Internet Access >> IPv6

WAN 2

Internet Access Mode

Connection Type

Offline

Offline

PPP

TSPC

AICCU

DHCPv6 Client

Static IPv6

6in4 Static Tunnel

6rd

OK

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

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

WAN >> Internet Access

WAN 2

PPPoE

Enable Disable

ISP Access Setup

Service Name (Optional):

Username: 73768635@hinet.net

Password: *****

Index(1-15) in Schedule Setup: => [] [] [] []

WAN Connection Detection

Mode: ARP Detect

Ping IP: []

TTL: []

MTU: 1500 (Max:1492)

Static or Dynamic IP

IPv6

PPP/MP Setup

PPP Authentication: PAP or CHAP

Idle Timeout: 180 second(s)

IP Address Assignment Method (ICP)

WAN IP Alias

Fixed IP: Yes No (Dynamic IP)

Fixed IP Address: []

Default MAC Address Specify a MAC Address

MAC Address: 00 · 1D · AA · 89 · 42 · BA

OK Cancel

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

Internet Access >> IPv6

WAN 2

Internet Access Mode

Connection Type: PPP

Auto Manual

Note: IPv4 WAN setting should be PPPoE client.

OK

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

Online Status

Physical Connection						System Uptime: 0:1:17
IPv4			IPv6			
LAN Status		Primary DNS: 168.95.192.1		Secondary DNS: 168.95.1.1		
IP Address	TX Packets	RX Packets				
192.168.1.1	0	3085				
WAN 1 Status >> Dial PPPoE						
Enable	Line	Name	Mode	Up Time		
Yes	ADSL		PPPoE	00:00:00		
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)	
---	---	0	0	0	0	
WAN 2 Status >> Drop PPPoE						
Enable	Line	Name	Mode	Up Time		
Yes	Ethernet		PPPoE	0:00:54		
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)	
114.44.49.54	168.95.98.254	800	4761	821	6617	
WAN 3 Status						
Enable	Line	Name	Mode	Up Time	Signal	
Yes	USB		---	00:00:00	-	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)	
---	---	0	0	0	0	
ADSL Information (ADSL Firmware Version: 05-04-04-04-00-01)						
ATM Statistics	TX Cells	RX Cells	TX CRC errs	RX CRC errs		
	0	0	0	0		
ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
		READY	0	0	0	0

Online Status

Physical Connection						System Uptime: 0:2:32
IPv4			IPv6			
LAN Status						
IP Address						
2001:B010:7300:201:21D:AFF:FEA6:2568/64 (Global)						
FE80::21D:AFF:FEA6:2568/64 (Link)						
TX Packets	RX Packets	TX Bytes		RX Bytes		
7	4	690		328		
WAN2 IPv6 Status >> Drop PPP						
Enable	Mode	Up Time				
Yes	PPP	0:02:08				
IP	Gateway IP					
2001:B010:7300:201:21D:AFF:FEA6:256A/128 (Global)	FE80::90:1A00:242:AD52					
FE80::1D:AFF:FEA6:256A/128 (Link)						
DNS IP						
2001:8000:168::1						
2001:8000:168::2						
TX Packets	RX Packets	TX Bytes		RX Bytes		
7	9	544		1126		

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



Info

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

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

Internet Access >> IPv6

WAN 2

Internet Access Mode
Connection Type: TSPC

TSPC Configuration
Username: cacahsu
Password: *****
Confirm Password: *****
Tunnel Broker: broker.freenet6.net

OK

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

Online Status

Physical Connection System Uptime: 0:2:3

IPv4		IPv6	
LAN Status			
IP Address			
2001:5C0:1502:D00:21D:AFF:FEA6:2568/64 (Global)			
FE80::21D:AFF:FEA6:2568/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
88	121	15596	10249
WAN2 IPv6 Status			
Enable	Mode	Up Time	
Yes	TSPC	0:01:40	
IP			Gateway IP
2001:5C0:1400:B::10B9/128 (Global)			---
FE80::722C:3559/128 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
127	89	9219	15866

- **AICCU - Tunnel application**

Choose AICCU and type the information for AICCU of IPv6.



Info

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

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

Internet Access >> IPv6

WAN 2

Internet Access Mode
 Connection Type: AICCU

AICCU Configuration
 Always On
 Username: JCR3-SIXXS
 Password: *****
 Confirm Password: *****
 Tunnel Broker: tic.sixxs.net
 Subnet Prefix: 2001:4DD0:FF00:8805::2 / 64

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

OK

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

Online Status

System Uptime: 0:1:18

Physical Connection		IPv4	IPv6
LAN Status			
IP Address			
2001:4DD0:FF00:83E4:21D:AFF:FEA6:2568/64 (Global)			
FE80::21D:AFF:FEA6:2568/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
147	187	34205	19176
WAN2 IPv6 Status			
Enable	Mode	Up Time	
Yes	AICCU	0:00:48	
IP		Gateway IP	
2001:4DD0:FF00:3E4::2/64 (Global)		---	
FE80::4CD0:FF00:3E4:2/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
186	137	16438	33093

- DHCPv6 Client

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

Internet Access >> IPv6

WAN 2

Internet Access Mode
 Connection Type DHCPv6 Client

DHCPv6 Client Configuration
 Identity Association Prefix Delegation Non-temporary Address
 IAID (Identity Association ID) 4173039447

OK

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

Online Status

Physical Connection		System Uptime: 0:0:50	
IPv4	IPv6		
LAN Status			
IP Address			
FE80::21D:AFF:FEA6:2568/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
6	2	588	156
WAN2 IPv6 Status			
Enable	Mode	Up Time	
Yes	DHCPv6 Client	0:00:40	
IP			Gateway IP
2001:8010:7300:201:21D:AFF:FEA6:256A/64 (Global)			---
2001:1111:2222:5555:21D:AFF:FEA6:256A/64 (Global)			
2001:1111:2222:3333::1111/128 (Global)			
FE80::21D:AFF:FEA6:256A/64 (Link)			
DNS IP			
2001:4860:4860::8888			
2001:4860:4860::8844			
TX Packets	RX Packets	TX Bytes	RX Bytes
14	5	1174	694

- Static IPv6

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

Internet Access >> IPv6

WAN 2

Internet Access Mode
 Connection Type: Static IPv6

Static IPv6 Address Configuration
 IPv6 Address: 2001:B010:7300:201:21D:AFF:FEA6:256A / Prefix Length: /64 Add Delete

Current IPv6 Address Table

Index	IPv6 Address/Prefix Length	Scope
1	2001:B010:7300:201:21D:AFF:FEA6:256A/64	Global

Static IPv6 Gateway Configuration
 IPv6 Gateway Address: ::

OK

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

Online Status

Physical Connection System Uptime: 0:4:2

IPv4		IPv6	
LAN Status			
IP Address			
FE80::21D:AFF:FEA6:2568/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
4	0	312	0
WAN2 IPv6 Status			
Enable	Mode	Up Time	
Yes	Static IPv6	0:03:56	
IP		Gateway IP	
2001:B010:7300:201:21D:AFF:FEA6:256A/64 (Global)		---	
2001:1111:2222:3333:21D:AFF:FEA6:256A/64 (Global)			
FE80::21D:AFF:FEA6:256A/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
8	2	608	364

- **6in4 Static Tunnel**

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

Internet Access >> IPv6

WAN 2

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)

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

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

- 6rd

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

Internet Access >> IPv6

WAN 2

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:

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

Online Status

System Uptime: 0day 0:9:15

Physical Connection		IPv4	IPv6
LAN Status			
IP Address			
2001:F41:A865:1D00:21D:AAFF:FE83:11B4/64 (Global)			
FE80::21D:AAFF:FE83:11B4/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
15	113	1354	18040
WAN1 IPv6 Status			
Enable	Mode	Up Time	
Yes	6rd	0:09:06	
IP		Gateway IP	
2001:E41:A865:1D01:21D:AAFF:FE83:11B5/128 (Global)		---	
FE80::C0A8:651D/128 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
13	29	967	2620

II. Configuring the LAN Settings

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

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

LAN >> General Setup

Ethernet TCP / IP and DHCP Setup
LAN 1 IPv6 Setup

Router Advertisement Server

Enable Disable

Advertisement Lifetime Seconds (Range : 600 - 9000)

DHCPv6 Server

Enable Server Disable Server

Start IPv6 Address

End IPv6 Address

DNS Server IPv6 Address

Primary DNS Server

Secondary DNS Server

Static IPv6 Address

IPv6 Address / Prefix Length

Current IPv6 Address Table

Index	IPv6 Address/Prefix Length	Scope
1	FE80::21D:AFF:FE89:42B8/64	Link

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

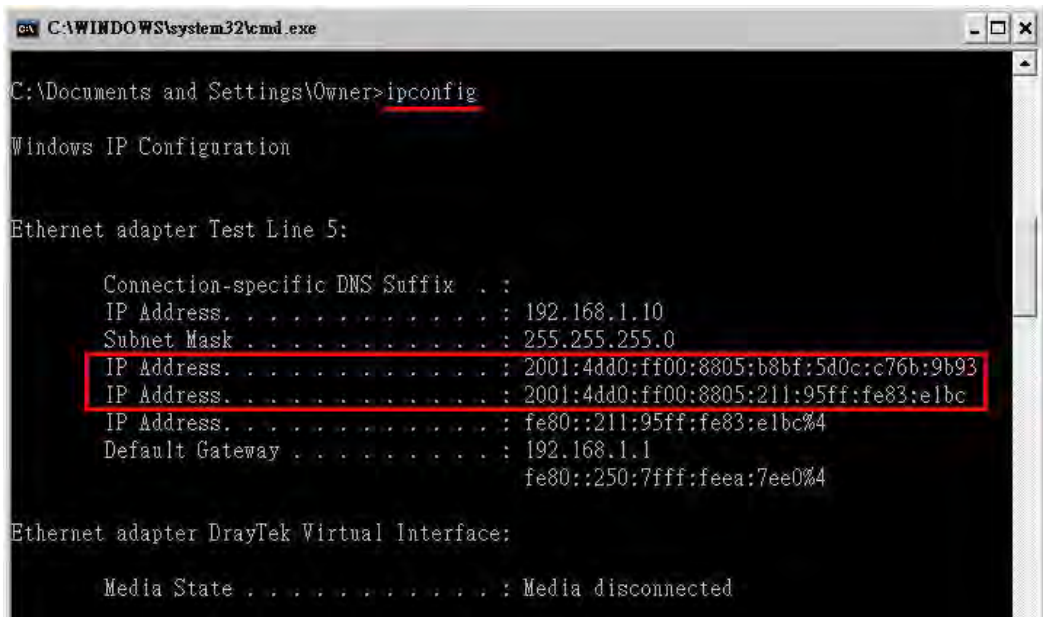


Info

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

III. Confirming IPv6 Service Run Successfully

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



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Owner>ipconfig

Windows IP Configuration

Ethernet adapter Test Line 5:

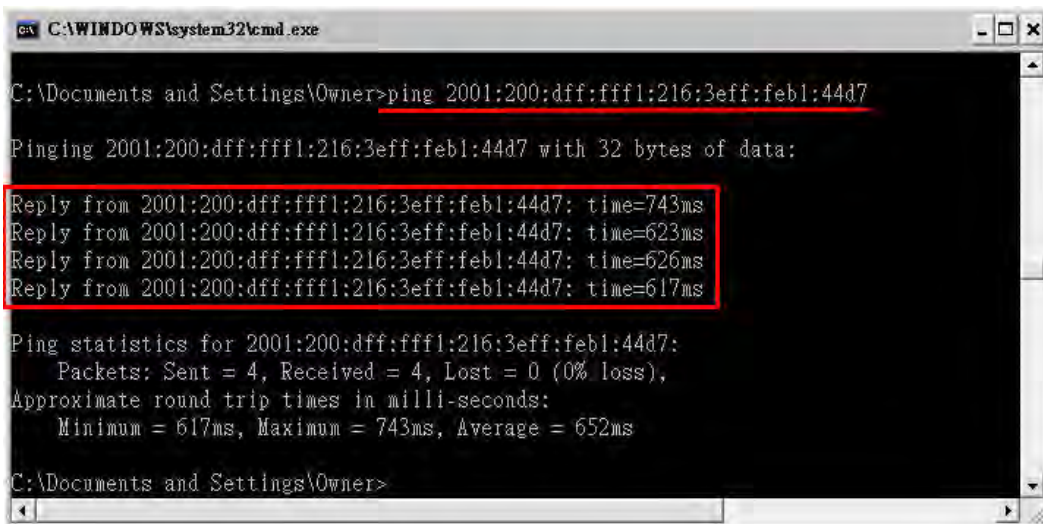
    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.10
    Subnet Mask . . . . . : 255.255.255.0
    IP Address. . . . . : 2001:4dd0:ff00:8805:b8bf:5d0c:c76b:9b93
    IP Address. . . . . : 2001:4dd0:ff00:8805:211:95ff:fe83:e1bc
    IP Address. . . . . : fe80::211:95ff:fe83:e1bc%4
    Default Gateway . . . . . : 192.168.1.1
                                     fe80::250:7fff:feea:7ee0%4

Ethernet adapter DrayTek Virtual Interface:

    Media State . . . . . : Media disconnected
```

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

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



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Owner>ping 2001:200:dff:fff1:216:3eff:febl:44d7

Pinging 2001:200:dff:fff1:216:3eff:febl:44d7 with 32 bytes of data:

Reply from 2001:200:dff:fff1:216:3eff:febl:44d7: time=743ms
Reply from 2001:200:dff:fff1:216:3eff:febl:44d7: time=623ms
Reply from 2001:200:dff:fff1:216:3eff:febl:44d7: time=626ms
Reply from 2001:200:dff:fff1:216:3eff:febl:44d7: time=617ms

Ping statistics for 2001:200:dff:fff1:216:3eff:febl:44d7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 617ms, Maximum = 743ms, Average = 652ms

C:\Documents and Settings\Owner>
```

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

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

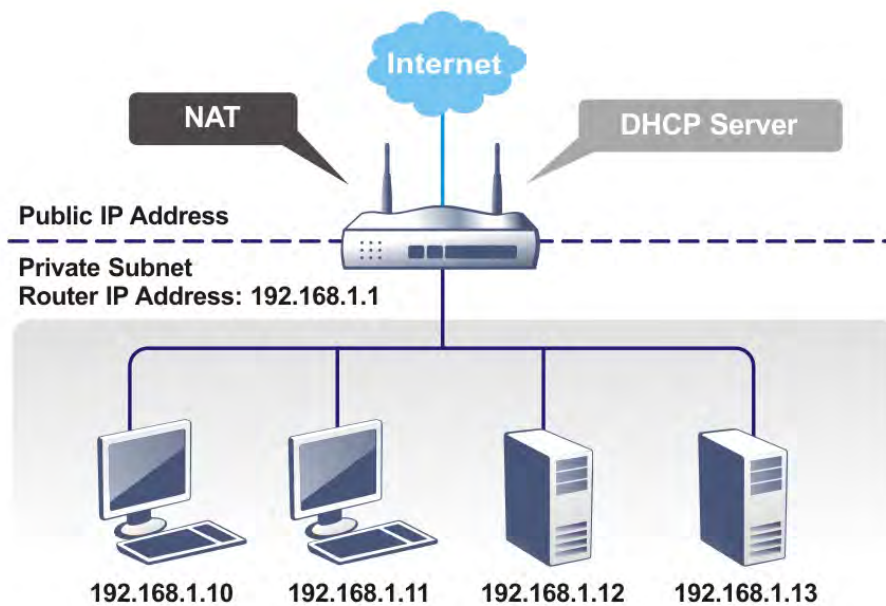


If you can see a turtle dancing on the screen, that means IPv6 service is ready for you to access and utilize.

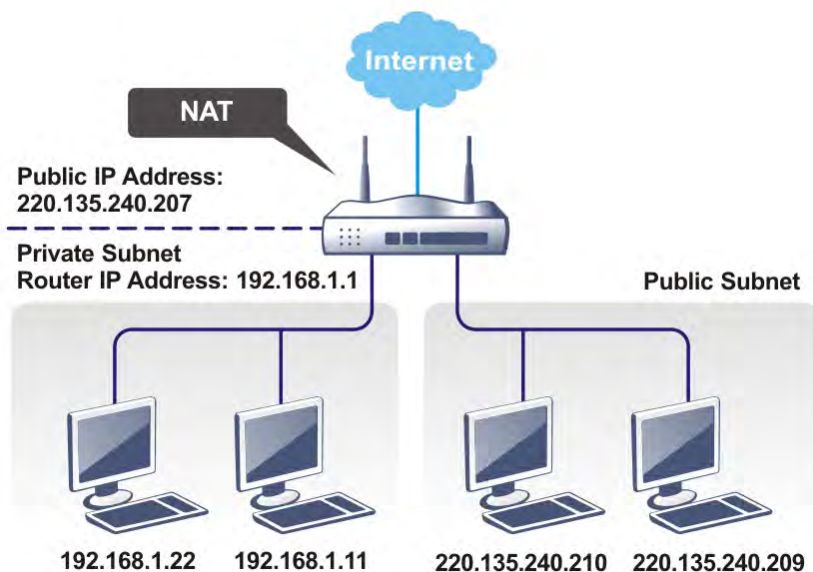
II-2 LAN

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

The most generic function of Vigor device 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 device 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 device 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)

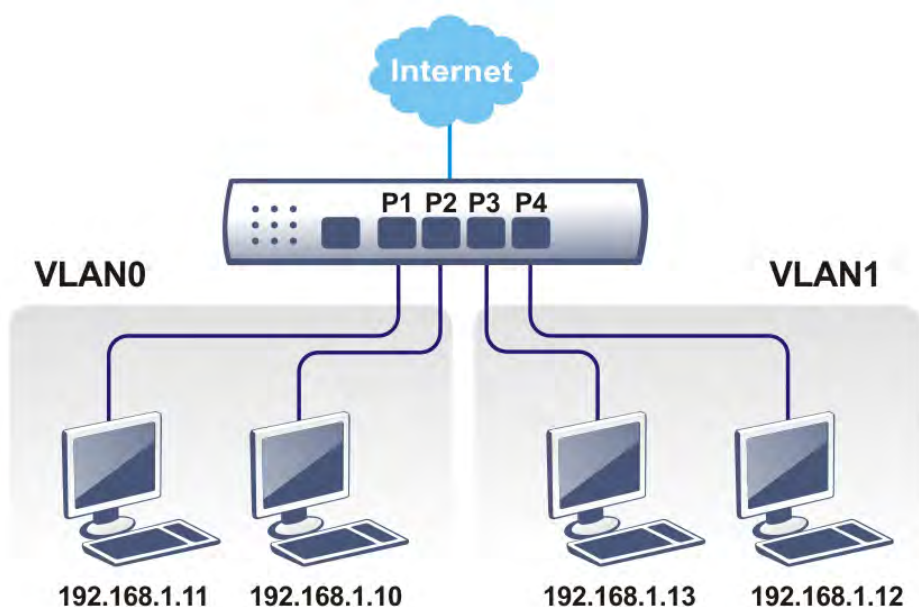
Vigor device will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

What is Static Route

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

What are Virtual LANs and Rate Control

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



Web User Interface

II-2-1 General Setup

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

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

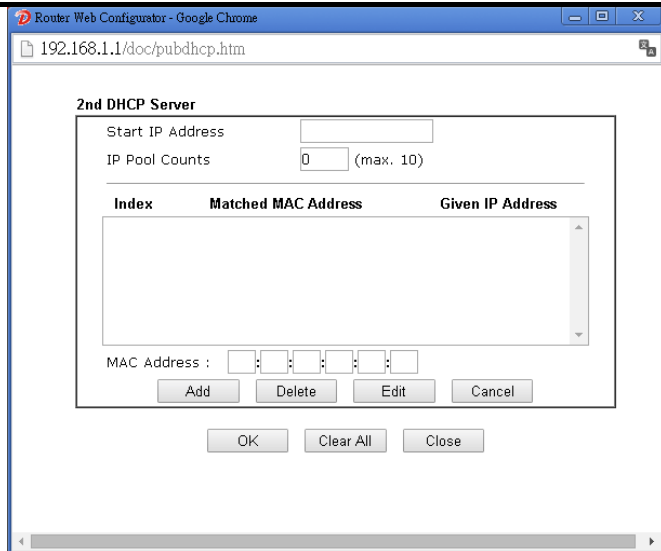
There are two configuration pages for LAN1, Ethernet TCP/IP and DHCP Setup (based on IPv4) and IPv6 Setup. Click the tab for each type and refer to the following explanations for detailed information.

LAN >> General Setup

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

Available settings are explained as follows:

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



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 router 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 router 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 router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2nd subnet won't get an IP address belonging to 1st subnet.

DHCP Server Configuration

DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatches related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.

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

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

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

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

Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP

address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.

IP Pool Counts - Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.

Gateway IP Address - Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway.

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

Advanced - Configure DHCP client option. DHCP packets can be processed by adding option number and data information when such function is enabled.

LAN >> General Setup

DHCP Server Options Status

Enable	Option	Type	Data
--------	--------	------	------

Enable:

Option Number:

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

Data:

Add Update Delete

Enable - Check the box to enable the function of DHCP Option. Each DHCP option is composed by an option number with data. For example,

Option number:100

Data: abcd

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

Option Number - Type a number for such option. If you choose to configure option 61 here, the detailed settings in WAN>>Interface Access will be overwritten.

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

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

Add - Create a new entry and display on the Option List table.

Update - Edit the existing entry.

Delete - Remove the existing entry.

DNS Server IP Address

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

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

address: 194.109.6.66 to this field.

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

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

Online Status

Physical Connection System Uptime: 22:22:45

IPv4		IPv6	
LAN Status	Primary DNS: 8.8.8.8	Secondary DNS: 8.8.4.4	
IP Address	TX Packets	RX Packets	
192.168.1.1	0	41533	

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

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

Force router to use address for DNS - Force Vigor router to use DNS servers configured in LAN1 instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).

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

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

There are two configuration pages for LAN, 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

Router Advertisement Server

Enable Disable

Advertisement Lifetime Seconds (Range : 600 - 9000)

DHCPv6 Server

Enable Server Disable Server

Start IPv6 Address

End IPv6 Address

DNS Server IPv6 Address

Primary DNS Server

Secondary DNS Server

Static IPv6 Address

IPv6 Address / Prefix Length

Current IPv6 Address Table

Index	IPv6 Address/Prefix Length	Scope
1	FE80::21D:AAFF:FE89:42B8/64	Link

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
Router Advertisement Server	<p>Enable - Click it to enable RADVD server. The router advertisement daemon (radvd) 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.</p> <p>Disable - Click it to disable RADVD server.</p> <p>Advertisement Lifetime - The lifetime associated with the default router in units of seconds. It's used to control the lifetime of the prefix. The maximum value corresponds to 18.2 hours. A lifetime of 0 indicates that the router is not a default router and should not appear on the default router list.</p>
DHCPv6 Server Configuration	<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>Start IPv6 Address / End IPv6 Address -Type the start and end address for IPv6 server.</p>
DNS Server IPv6 Address	<p>Primary DNS Sever - Type the IPv6 address for Primary DNS server.</p>

	Secondary DNS Server -Type another IPv6 address for DNS server if required.
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.
Current IPv6 Address Table	Display current used IPv6 addresses.

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

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. When this function is enabled, all the assigned IP and MAC address binding together cannot be changed. If you modified the binding IP or MAC address, it might cause you not access into the Internet.

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

LAN >> Bind IP to MAC

Bind IP to MAC

Enable
 Disable
 Strict Bind

ARP Table	Select All Sort Refresh	IP Bind List (Limit: 300 entries)	Select All Sort										
<table style="width: 100%; border-collapse: collapse;"> <tr> <th style="text-align: left;">IP Address</th> <th style="text-align: left;">Mac Address</th> </tr> <tr> <td>10.28.60.12</td> <td>00-50-7F-22-33-43</td> </tr> </table>	IP Address	Mac Address	10.28.60.12	00-50-7F-22-33-43		<table style="width: 100%; border-collapse: collapse;"> <tr> <th style="text-align: left;">Index</th> <th style="text-align: left;">IP Address</th> <th style="text-align: left;">Mac Address</th> </tr> <tr> <td> </td> <td> </td> <td> </td> </tr> </table>	Index	IP Address	Mac Address				
IP Address	Mac Address												
10.28.60.12	00-50-7F-22-33-43												
Index	IP Address	Mac Address											

Add or Update

IP Address:

Mac Address:

Comment:

Show Comment

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

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

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



Info

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

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

II-3 NAT

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

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

The benefit of the NAT includes:

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



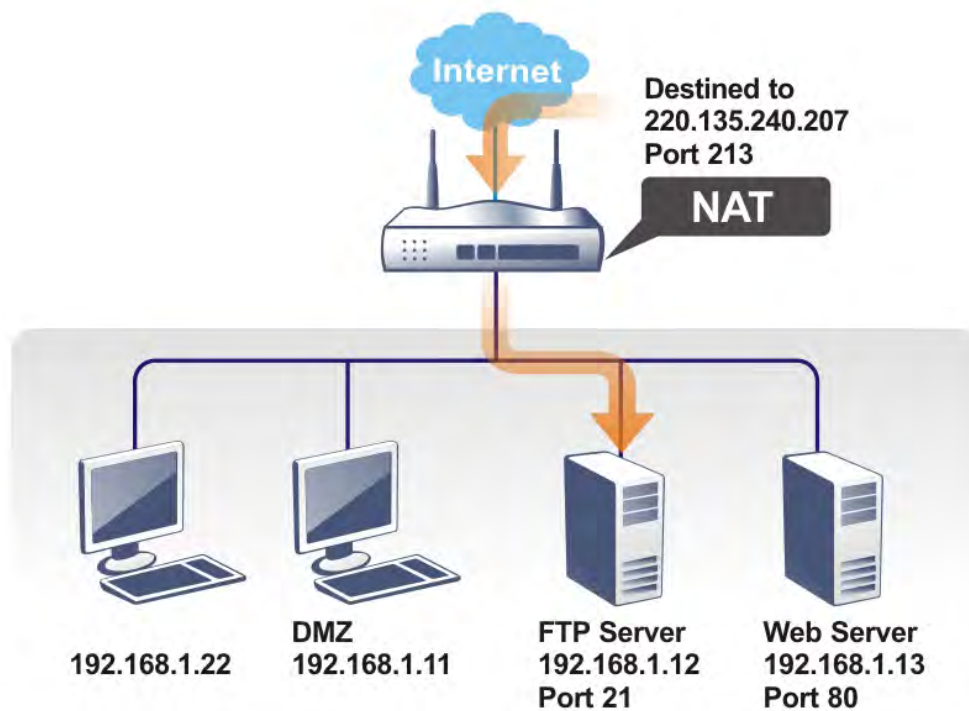
Info

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

Web User Interface

II-3-1 Port Redirection

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



The port redirection can only apply to incoming traffic.

To use this function, please go to NAT page and choose **Port Redirection** web page. The **Port Redirection Table** provides 20 port-mapping entries for the internal hosts.

NAT >> Port Redirection

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

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

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

Each item is explained as follows:

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

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

NAT >> Port Redirection

Index No. 1

Enable
 Mode Single ▾
 Service Name Single
 Protocol Range
 WAN IP 1.All ▾
 Public Port
 Private IP
 Private Port

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

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable such port redirection setting.

Mode	Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select Range . In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered, the system will calculate and display the ending IP of private IP automatically.
Service Name	Enter the description of the specific network service.
Protocol	Select the transport layer protocol (TCP or UDP).
WAN IP	Select the WAN IP used for port redirection. There are eight WAN IP alias that can be selected and used for port redirection. The default setting is All which means all the incoming data from any port will be redirected to specified range of IP address and port.
Public Port	Specify which port can be redirected to the specified Private IP and Port of the internal host. If you choose Range as the port redirection mode, you will see two boxes on this field. Type the required number on the first box (as the starting port) and the second box (as the ending port).
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.

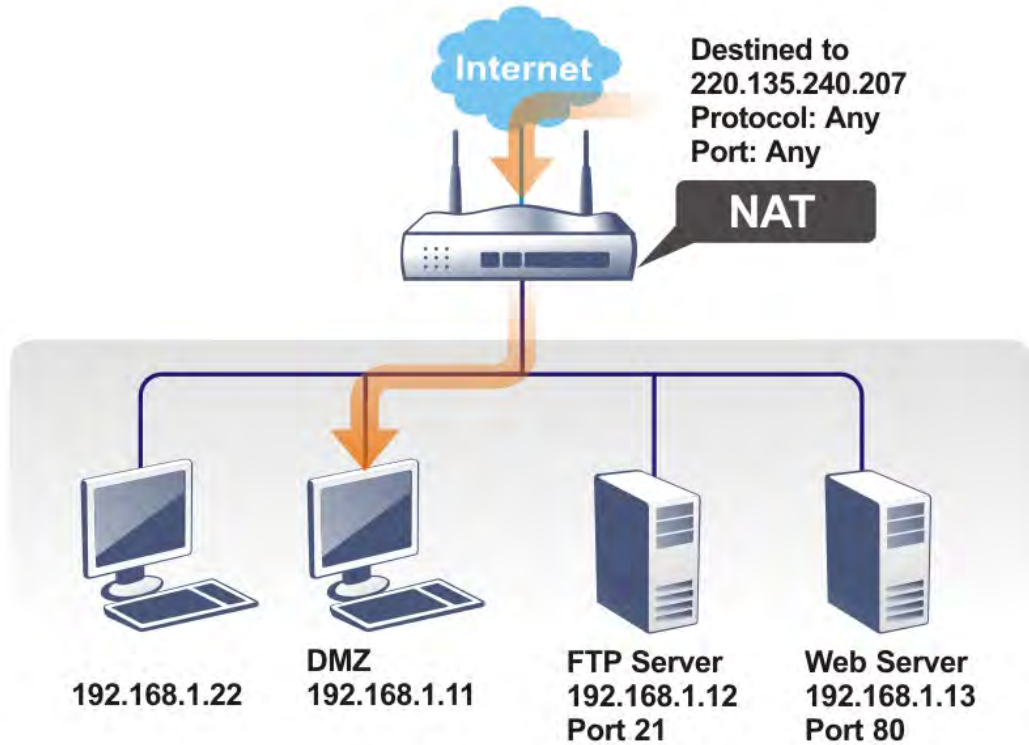
After finishing all the settings here, please click **OK** to save the configuration.

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.

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 device provides a facility **DMZ Host** that maps ALL unsolicited data on any protocol to a single host in the LAN. Regular web surfing and other such Internet activities from other clients will continue to work without inappropriate interruption. **DMZ Host** allows a defined internal user to be totally exposed to the Internet, which usually helps some special applications such as Netmeeting or Internet Games etc.



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

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

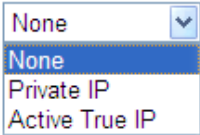

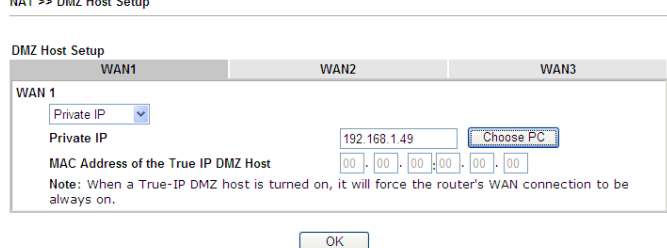
NAT >> DMZ Host Setup

DMZ Host Setup

WAN1	WAN2
WAN 1	
None	
Private IP	
MAC Address of the True IP DMZ Host	
Note: If True-IP DMZ is enabled the routers WAN connection will be forced to remain on.	


OK

Available settings are explained as follows:

Item	Description
<p>WAN 1</p> 	<p>Choose Private IP or Active True IP first. Active True IP selection is available for WAN1 only.</p>
Private IP	Enter the private IP address of the DMZ host, or click Choose PC to select one.
Choose IP	<p>Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.</p>  <p>When you have selected one private IP from the above dialog, the IP address will be shown on the following screen. Click OK to save the setting.</p> 

DMZ Host for WAN2 is slightly different with WAN1. **Active True IP** selection is available for WAN1 only. See the following figure.

NAT >> DMZ Host Setup



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

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	Comment	Local IP Address	Status
1.			X
2.			X
3.			X
4.			X
5.			X
6.			X
7.			X
8.			X
9.			X
10.			X

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

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

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

NAT >> Open Ports >> Edit Open Ports

Index No. 1

Enable Open Ports

Comment

Private IP

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

Available settings are explained as follows:

Item	Description
Enable Open Ports	Check to enable this entry.
Comment	Make a name for the defined network application/service.
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-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 devices 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 device 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) (1~14400)

Accounts:

Index	Domain Name	Active
<u>1.</u>		x
<u>2.</u>		x
<u>3.</u>		x
<u>4.</u>		x
<u>5.</u>		x
<u>6.</u>		x

Available settings are explained as follows:

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

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

Index : 1

Enable Dynamic DNS Account

Service Provider: ▼

Service Type: ▼

Domain Name: ▼

Login Name: (max. 64 characters)

Password: (max. 23 characters)

Wildcards

Backup MX

Mail Extender:

Determine Real WAN IP: ▼

OK Clear Cancel

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

Index : 1

Enable Dynamic DNS Account

Service Provider: ▼

Provider Host:

Service API:

Auth Type: ▼

Connection Type: ▼

Server Response:

Login Name: (max. 64 characters)

Password: (max. 23 characters)

Wildcards

Backup MX

Mail Extender:

Determine Real WAN IP: ▼

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 3).
Service Provider	Select the service provider for the DDNS account.
Service Type	Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field. Note that such option is not available when Customized is selected as Service Provider.
Domain Name	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.

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

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

Disable the Function and Clear all Dynamic DNS Accounts

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

Delete a Dynamic DNS Account

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

II-4-2 Schedule

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

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

Applications >> Schedule

Schedule:		Set to Factory Default	
Index	Status	Index	Status
1.	x	9.	x
2.	x	10.	x
3.	x	11.	x
4.	x	12.	x
5.	x	13.	x
6.	x	14.	x
7.	x	15.	x
8.	x		

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

Available settings are explained as follows:

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

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

To add a schedule:

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

Index No. 1

Enable Schedule Setup

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

Start Time (hh:mm) 0 : 0

Duration Time (hh:mm) 0 : 0

Action Force On

Idle Timeout 0 minute(s).(max. 255, 0 for default)

How Often

Once

Weekdays

Sun Mon Tue Wed Thu Fri Sat

OK Clear Cancel

Available settings are explained as follows:

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

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

Note: If you intend running UPnP service inside your LAN, you should check the appropriate service above.

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.

Applications >> IGMP

IGMP

Enable IGMP Proxy WAN1
 IGMP Proxy acts as a multicast proxy for hosts on the LAN side. Enable IGMP proxy to access any
 multicast group. This function is available in NAT mode. **Effect when Bridge Mode is enabled.**
WAN1
WAN2
PVC/VLAN
OK Cancel

[Refresh](#)

Working Multicast Groups		
Index	Group ID	P1

Available settings are explained as follows:

Item	Description
Enable IGMP Proxy	Check this box to enable this function. The application of multicast will be executed through WAN/LTE/PVC/VLAN port. In addition, such function is available in NAT mode.
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	It indicates the LAN port used for the multicast group.

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

II-5 Routing



Info

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

Web User Interface

II-5-1 Static Route

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

Static Route for IPv4

LAN >> Static Route Setup

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

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

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

Available settings are explained as follows:

Item	Description
Index	The number (1 to 30) under Index allows you to open next page to set up static route.
Destination Address	Displays the destination address of the static route.
Status	Displays the status of the static route.
Set to Factory Default	Clear all of the settings and return to factory default settings.

Viewing Routing Table

Displays the routing table for your reference.

```
Diagnostics >> View Routing Table

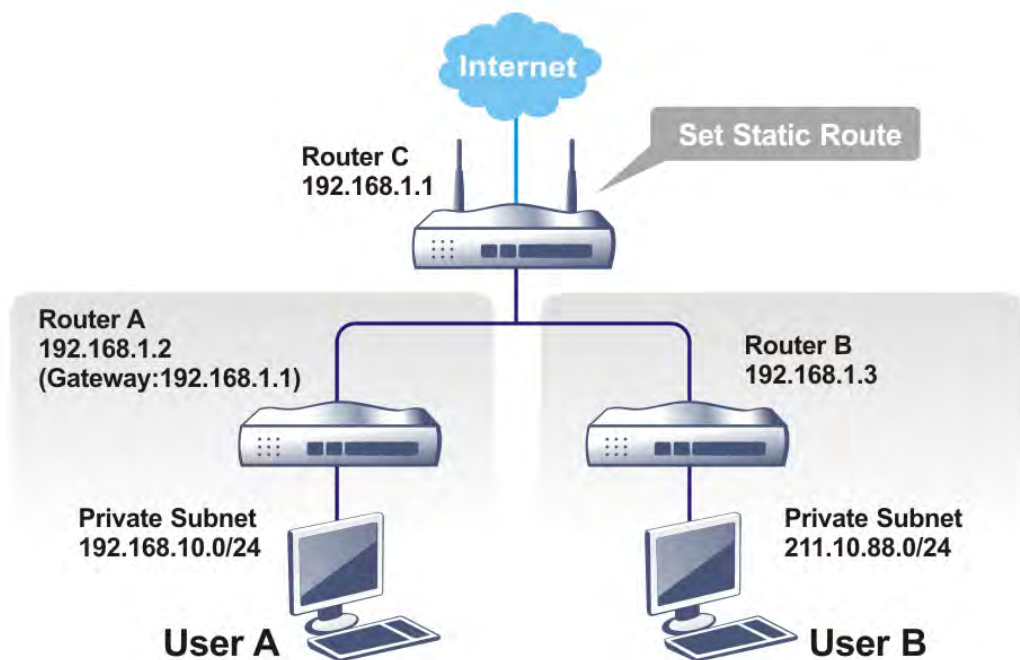
Current Running Routing Table | IPv6 Routing Table | Refresh |
Key: C - connected, S - static, R - RIP, * - default, ~ - private
C~ 192.168.1.0/255.255.255.0 directly connected LAN1
```

Add Static Routes to Private and Public Networks

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

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

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



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



Info

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

router, and continuously exchange of IP routing information with different subnets.

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

LAN >> Static Route Setup

Index No. 1

Enable

Destination IP Address	???
Subnet Mask	
Gateway IP Address	
Network Interface	LAN ▾

Note: WAN3, WAN4, WAN5 are router-borne WANs.

OK Cancel Delete

Available settings are explained as follows:

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

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

LAN >> Static Route Setup

Index No. 1

Enable

Destination IP Address	211.100.88.0
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.3
Network Interface	LAN1 ▾

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

Diagnostics >> View Routing Table

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

Static Route for IPv6

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

LAN >> Static Route Setup

IPv4			IPv6			Set to Factory Default	View IPv6 Routing Table
Index	Destination Address	Status	Index	Destination Address	Status		
1.	::/0	x	11.	::/0	x		
2.	::/0	x	12.	::/0	x		
3.	::/0	x	13.	::/0	x		
4.	::/0	x	14.	::/0	x		
5.	::/0	x	15.	::/0	x		
6.	::/0	x	16.	::/0	x		
7.	::/0	x	17.	::/0	x		
8.	::/0	x	18.	::/0	x		
9.	::/0	x	19.	::/0	x		
10.	::/0	x	20.	::/0	x		

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

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

Available settings are explained as follows:

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

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

LAN >> Static Route Setup

Index No. 1

Enable

Destination IPv6 Address / Prefix Len: /

Gateway IPv6 Address:

Network Interface: LAN

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.

This page is left blank.

Part III Security



Firewall



CSM

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

CSM is an abbreviation of Central Security Management which is used to filter 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 device 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:

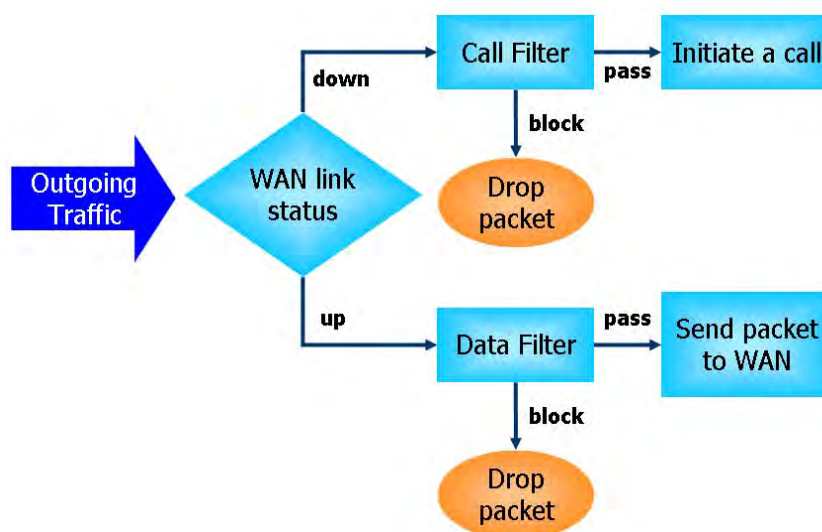
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

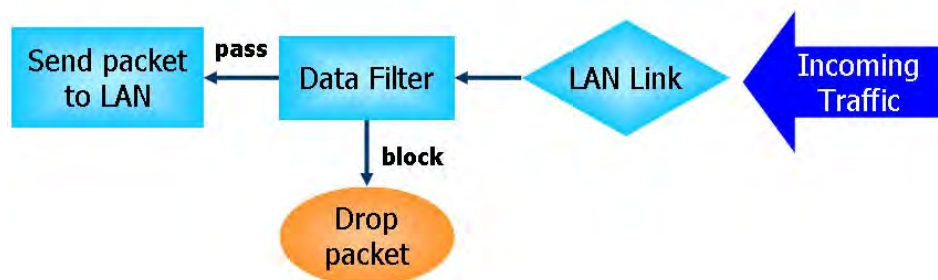
IP Filters

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 device 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 device 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.

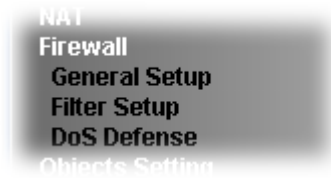
Also the Vigor device monitors the traffic. Any abnormal traffic flow violating the pre-defined parameter, such as the number of thresholds, is identified as an attack and the Vigor device will activate its defense mechanism to mitigate in a real-time manner.

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 to **Accept incoming fragmented UDP packets**.

Click **Firewall** and click **General Setup** to open the general setup page.

III-1-1-1 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 Start Filter Set:

Disable

Data Filter Enable Start Filter Set:

Disable

Accept large incoming fragmented UDP or ICMP packets (for some games, ex. CS)

Enable Strict Security Firewall
Block routing packet from WAN

IPv4 IPv6

Note: The packets will be filtered by the following firewall functions sequentially:

1. Data Filter Sets and Rules
2. Block routing packets from WAN
3. Default Rule

Available settings are explained as follows:

Item	Description
Call Filter	Check Enable to activate the Call Filter function. Assign a start filter set for the Call Filter.

Data Filter	Check Enable to activate the Data Filter function. Assign a start filter set for the Data Filter.
Accept large incoming...	Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor device will reject these fragmented packets to prevent attack unless you enable "Accept large incoming fragmented UDP or ICMP Packets" . By checking this box, you can play these kinds of on-line games. If security concern is in higher priority, you cannot enable "Accept large incoming fragmented UDP or ICMP Packets" .
Enable Strict Security Firewall	For the sake of security, the router will execute strict security checking for data transmission. Such feature is enabled in default. All the packets, while transmitting through Vigor device, will be filtered by firewall. If the firewall system (e.g., content filter server) does not make any response (pass or block) for these packets, then the router's firewall will block the packets directly.
Block routing packet from WAN	Usually, IPv6 network sessions/traffic from WAN to LAN will be accepted by IPv6 firewall in default. IPv6 - To prevent remote client accessing into the PCs on LAN, check the box to make the packets (routed from WAN to LAN) via IPv6 being blocked by such router. It is effective only for the packets routed but not for packets translated by NAT. IPv4 - To prevent remote client accessing into the PCs on LAN, check the box to make the incoming packets via IPv4 being blocked by such router. It is effective only for the packets routed but not for packets translated by NAT.

III-1-1-2 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 device.

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"/>

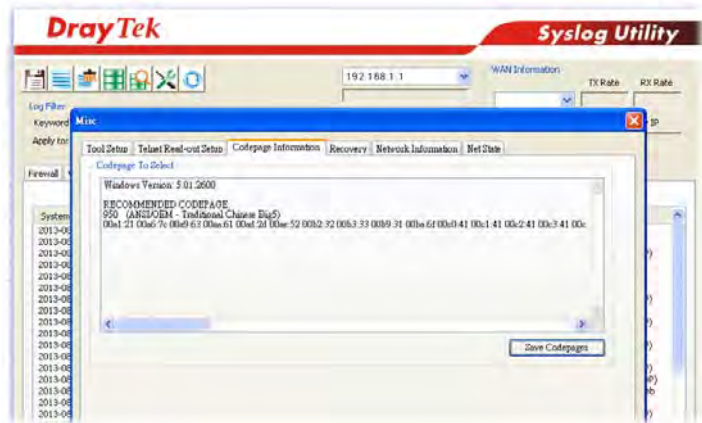
Advance Setting

Available settings are explained as follows:

Item	Description									
Filter	<p>Select Pass or Block for the packets that do not match with the filter rules.</p> <p>Filter <input type="button" value="Pass"/> ▾ Pass Block </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 10000.</p>									
URL Content Filter	<p>Select one of the URL Content Filter profile settings (created in CSM>> URL Content Filter) for applying with this router. Please set at least one profile for choosing in CSM>> URL Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for URL Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p>									
Advance Setting	<p>Click Edit to open the following window. However, it is strongly recommended to use the default settings here.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p style="text-align: center;">Firewall >> General Setup</p> <hr/> <p>Advance Setting</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Codepage</td> <td style="width: 40%;">ANSI(1252)-Latin I ▾</td> <td style="width: 30%;"></td> </tr> <tr> <td>Window size:</td> <td>65535</td> <td></td> </tr> <tr> <td>Session timeout:</td> <td>1440</td> <td>Minute</td> </tr> </table> <p style="text-align: center;"> <input type="button" value="OK"/> <input type="button" value="Close"/> </p> </div>	Codepage	ANSI(1252)-Latin I ▾		Window size:	65535		Session timeout:	1440	Minute
Codepage	ANSI(1252)-Latin I ▾									
Window size:	65535									
Session timeout:	1440	Minute								

Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtain correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage.

If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.



Window size - It determines the size of TCP protocol (0-65535). The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper.

Session timeout - Setting timeout for sessions can make the best utilization of network resources.

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 :

Filter Rule	Active	Comments	Move Up	Move Down
<input type="button" value="1"/>	<input checked="" type="checkbox"/>	Block NetBios		Down
<input type="button" value="2"/>	<input type="checkbox"/>		UP	Down
<input type="button" value="3"/>	<input type="checkbox"/>		UP	Down
<input type="button" value="4"/>	<input type="checkbox"/>		UP	Down
<input type="button" value="5"/>	<input type="checkbox"/>		UP	Down
<input type="button" value="6"/>	<input type="checkbox"/>		UP	Down
<input type="button" value="7"/>	<input type="checkbox"/>		UP	

Next Filter Set

Available settings are explained as follows:

Item	Description
Filter Rule	Click a button numbered (1 ~ 7) to edit the filter rule. Click the button will open Edit Filter Rule web page. For the detailed information, refer to the following page.
Active	Enable or disable the filter rule.
Comment	Enter filter set comments/description. Maximum length is 23-character long.
Move Up/Down	Use Up or Down link to move the order of the filter rules.
Next Filter Set	Set the link to the next filter set to be executed after the current filter run. Do not make a loop with many filter sets.

To edit Filter Rule, click the Filter Rule index button to enter the Filter Rule setup page.

Filter Set 1 Rule 1

Check to enable the Filter Rule

Comments:

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

Clear sessions when schedule ON: Enable

Direction:

Source IP:

Destination IP:

Service Type:

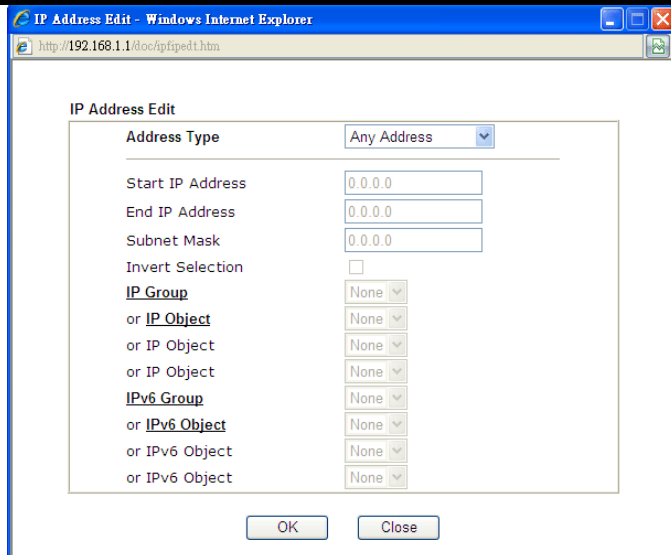
Fragments:

Application	Action/Profile	Syslog
Filter:	<input type="text" value="Block Immediately"/>	<input type="checkbox"/>
Branch to Other Filter Set:	<input type="text" value="None"/>	
Sessions Control	<input type="text" value="0 / 10000"/>	<input type="checkbox"/>
MAC Bind IP	<input type="text" value="Non-Strict"/>	<input type="checkbox"/>
Load-Balance policy	<input type="text" value="Auto-Select"/>	<input type="checkbox"/>
URL Content Filter:	<input type="text" value="None"/>	<input type="checkbox"/>

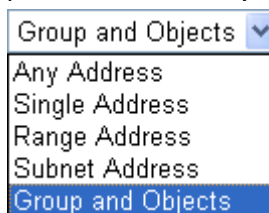
Advance Setting

Available settings are explained as follows:

Item	Description
Check to enable the Filter Rule	Check this box to enable the filter rule.
Comments	Enter filter set comments/description. Maximum length is 14-character long.
Index(1-15)	Set PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in Applications >> Schedule setup. The default setting of this field is blank and the function will always work.
Clear sessions when schedule ON	Check this box to clear the sessions when the above schedule profiles are applied.
Direction	Set the direction of packet flow. It is for Data Filter only. For the Call Filter , this setting is not available since Call Filter is only applied to outgoing traffic. <div style="border: 1px solid black; padding: 2px; width: fit-content;"> <input type="text" value="LAN/RT/VPN -> WAN"/> <ul style="list-style-type: none"> LAN/RT/VPN -> WAN WAN -> LAN/RT/VPN LAN/RT/VPN -> LAN/RT/VPN </div> <p>Note: RT means routing domain for 2nd subnet or other LAN.</p>
Source/Destination IP	Click Edit to access into the following dialog to choose the source/destination IP or IP ranges.



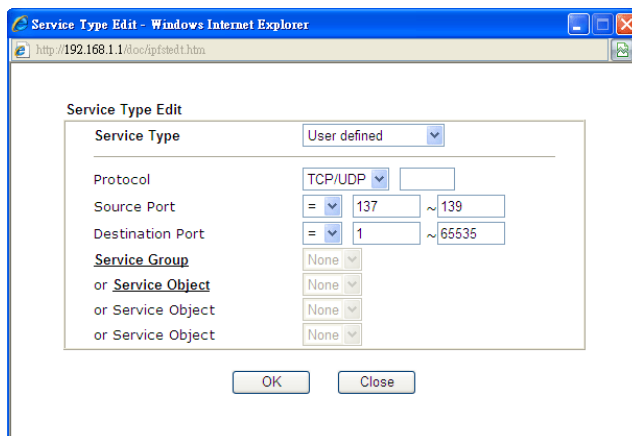
To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose **Group and Objects** as the Address Type.



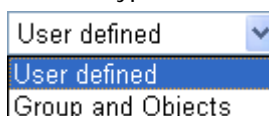
From the **IP Group** drop down list, choose the one that you want to apply. Or use the **IP Object** drop down list to choose the object that you want.

Service Type

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



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



Protocol - Specify the protocol(s) which this filter rule will

	<p>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 10000.</p>
MAC Bind IP	<p>Strict - Make the MAC address and IP address settings configured in IP Object for Source IP and Destination IP are bound for applying such filter rule.</p> <p>No-Strict - no limitation.</p>
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.</p>

	It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.
Advance Setting	<p>Click Edit to open the following window. However, it is strongly recommended to use the default settings here.</p> <p>Firewall >> Edit Filter Set >> Edit Filter Rule</p> <hr/> <p>Filter Set 1 Rule 1</p> <p>Advance Setting</p> <div data-bbox="715 450 1385 600" style="border: 1px solid black; padding: 5px;"> <p>Codepage: ANSI(1252)-Latin I</p> <p>Window size: 65535</p> <p>Session timeout: 1440 Minute</p> <p>DrayTek Banner: <input checked="" type="checkbox"/></p> </div> <p style="text-align: center;"> <input type="button" value="OK"/> <input type="button" value="Close"/> </p> <p>Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage.</p> <p>If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.</p> <div data-bbox="703 1077 1401 1496" style="border: 1px solid gray; padding: 5px;"> </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. However, Queue timeout is configured for TCP protocol only; session timeout is configured for the data flow which matched with the firewall rule.</p> <p>DrayTek Banner - Please uncheck this box and the following screen will not be shown for the unreachable web page. The default setting is Enabled.</p>

The requested Web page has been blocked by Web Content Filter.

Please contact your system administrator for further information.

[Powered by Draytek]

III-1-3 DoS Defense

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

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

Firewall >> DoS defense Setup

DoS defense Setup

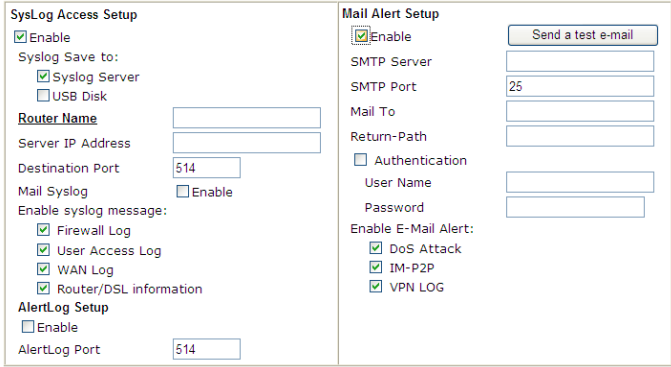
Enable DoS Defense

<input type="checkbox"/> Enable SYN flood defense	Threshold	<input type="text" value="2000"/>	packets / sec
	Timeout	<input type="text" value="10"/>	sec
<input type="checkbox"/> Enable UDP flood defense	Threshold	<input type="text" value="2000"/>	packets / sec
	Timeout	<input type="text" value="10"/>	sec
<input type="checkbox"/> Enable ICMP flood defense	Threshold	<input type="text" value="250"/>	packets / sec
	Timeout	<input type="text" value="10"/>	sec
<input type="checkbox"/> Enable Port Scan detection	Threshold	<input type="text" value="2000"/>	packets / sec
<input type="checkbox"/> Block IP options	<input type="checkbox"/> Block TCP flag scan		
<input type="checkbox"/> Block Land	<input type="checkbox"/> Block Tear Drop		
<input type="checkbox"/> Block Smurf	<input type="checkbox"/> Block Ping of Death		
<input type="checkbox"/> Block trace route	<input type="checkbox"/> Block ICMP fragment		
<input type="checkbox"/> Block SYN fragment	<input type="checkbox"/> Block Unassigned Numbers		
<input type="checkbox"/> Block Fraggle Attack			

Available settings are explained as follows:

Item	Description
Enable Dos Defense	Check the box to activate the DoS Defense Functionality.
Select All	Click this button to select all the items listed below.
Enable SYN flood defense	<p>Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor device 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 device.</p> <p>By default, the threshold and timeout values are set to 2000 packets per second and 10 seconds, respectively. That means, when 2000 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.</p>
Enable UDP flood defense	<p>Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor device will start to randomly discard the subsequent UDP packets for a period defined in Timeout.</p> <p>The default setting for threshold and timeout are 2000</p>

	packets per second and 10 seconds, respectively. That means, when 2000 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.
Enable ICMP flood defense	<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 PortScan detection	<p>Port Scan attacks the Vigor device 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 device will send out a warning.</p> <p>By default, the Vigor device 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 device 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 device 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 device will ignore any broadcasting ICMP echo request.</p>
Block trace route	<p>Check the box to enforce the Vigor device not to forward any trace route packets.</p>
Block SYN fragment	<p>Check the box to activate the Block SYN fragment function. The Vigor device will drop any packets having SYN flag and more fragment bit set.</p>
Block Fraggle Attack	<p>Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked.</p> <p>Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.</p>

Block TCP flag scan	Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include <i>no flag scan</i> , <i>FIN without ACK scan</i> , <i>SYN FINscan</i> , <i>Xmas scan</i> and <i>full Xmas scan</i> .
Block Tear Drop	Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor device is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.
Block Ping of Death	Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor devices will block any packets realizing this attacking activity.
Block ICMP Fragment	Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.
Block Unassigned Numbers	Check the box to activate the Block Unknown Protocol function. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and reject this kind of packets.
Warning Messages	<p>We provide Syslog function for user to retrieve message from Vigor device. The user, as a Syslog Server, shall receive the report sending from Vigor device which is a Syslog Client.</p> <p>All the warning messages related to DoS Defense will be sent to user and user can review it through Syslog daemon. Look for the keyword DoS in the message, followed by a name to indicate what kind of attacks is detected.</p> <p>System Maintenance >> SysLog / Mail Alert Setup</p>  <p>OK Clear</p>

The screenshot displays the DrayTek Syslog Utility web interface. At the top, the title bar reads "DrayTek Syslog 4.5.3" and the main header is "DrayTek Syslog Utility". Below the header, there are navigation icons and a search bar. The interface is divided into several sections:

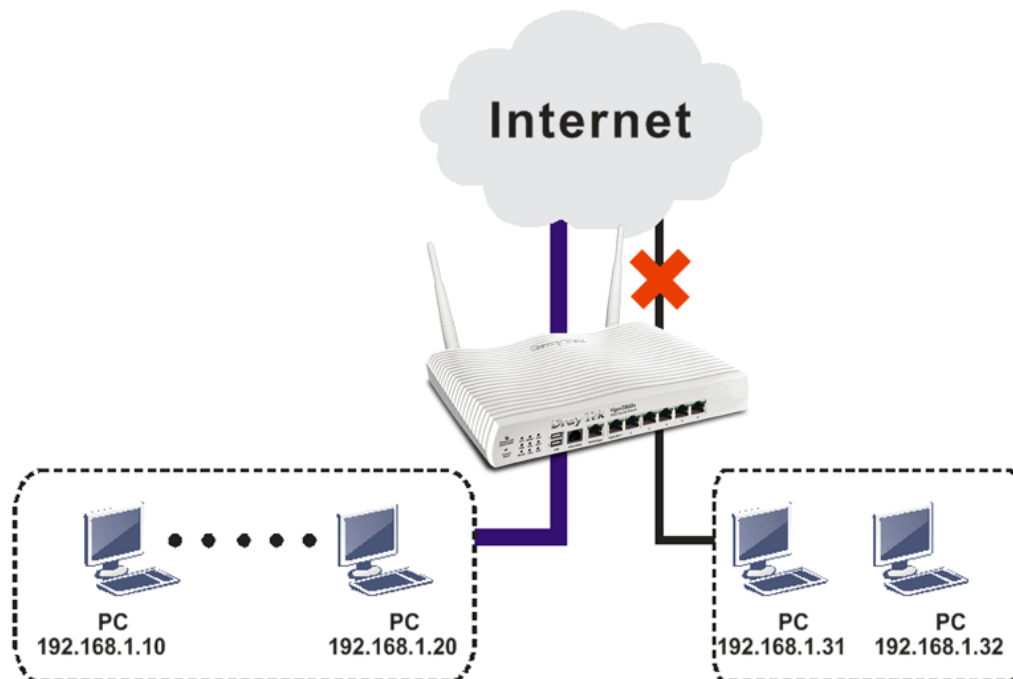
- Log Filter:** Includes a "Keyword:" field, an "Apply to:" dropdown menu (set to "All"), and a "Refresh" button.
- WAN Information:** Shows "172.16.3.130" and fields for "TX Rate" and "RX Rate".
- LAN Information:** Shows fields for "TX Packets" and "RX Packets".
- WAN IP:** Shows a field for "Gateway IP".
- Navigation:** Tabs for "Firewall", "VPN", "User Access", "Connection", "WAN", "PPPOE", and "Others".
- Log Selection:** Radio buttons for "Show Syslog List" (selected) and "Show Defense Alert TOP10".
- Log Table:** A table with columns for "System Time", "Router Time", "Host", and "Message". It contains five entries of "DOS[Block] [fraggle_attack]".
- Footer:** Small text at the bottom left reads "System Time: Time tag from the computer which runs the syslog application" and at the bottom right reads "Router Time: Time tag from router".

System Time	Router Time	Host	Message
2013-08-20 11:53:47	Aug 20 03:53:05	Vigor-router	[DOS][Block] [fraggle_attack] [0.0.0.0:68->255.255.255.255:67][UDP][Len=20, TLen=576]
2013-08-20 11:53:47	Aug 20 03:53:05	Vigor-router	[DOS][Block] [fraggle_attack] [0.0.0.0:68->255.255.255.255:67][UDP][Len=20, TLen=576]
2013-08-20 11:53:46	Aug 20 03:53:03	Vigor-router	[DOS][Block] [fraggle_attack] [192.168.1.10:4744->255.255.255.255:9999][UDP][Len=20, T
2013-08-20 11:53:14	Aug 20 03:53:02	Vigor-router	[DOS][Block] [fraggle_attack] [0.0.0.0:68->255.255.255.255:67][UDP][Len=20, TLen=576]
2013-08-20 11:53:14	Aug 20 03:53:02	Vigor-router	[DOS][Block] [fraggle_attack] [0.0.0.0:68->255.255.255.255:67][UDP][Len=20, TLen=576]

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 device. 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 device.
2. Open Firewall>>Filter Setup. Click the Set 2 link 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.	

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 2

Comments:

Filter Rule	Active	Comments	Move Up	Move Down
1	<input checked="" type="checkbox"/>	xNetBios -> DNS		Down
2	<input type="checkbox"/>		UP	Down
3	<input type="checkbox"/>		UP	Down
4	<input type="checkbox"/>		UP	Down

3. Check the box of **Check to enable the Filter Rule**. Type the comments (e.g., `block_all`). Choose **Block If No Further Match** for the **Filter** setting. Then, click **OK**.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 2

Check to enable the Filter Rule

Comments:

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

Clear sessions when schedule ON: Enable

Direction: LAN/RT/WPN -> WAN

Source IP:

Destination IP:

Service Type:

Fragments:

Application

Filter:

Branch to Other Filter Set:

Sessions Control:

Syslog:



Info

In default, the router will check the packets starting with Set 2, Filter Rule 2 to Filter Rule 7. If Block If No Further Match for is selected for Filter, the firewall of the router would check the packets with the rules starting from Rule 3 to Rule 7. The packets not matching with the rules will be processed according to Rule 2.

4. Next, set another rule. Just open **Firewall>>Filter Setup**. Click the **Set 2** link and choose the **Filter Rule 3** button.
5. Check the box of **Check to enable the Filter Rule**. Type the comments (e.g., `open_ip`). Click the **Edit** button for **Source IP**.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 3

Check to enable the Filter Rule

Comments:

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

Clear sessions when schedule ON: Enable

Direction: LAN/RT/WPN -> WAN

Source IP:

Destination IP:

Service Type:

Fragments:

Application

Filter:

Branch to Other Filter Set:

Syslog:

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

IP Address Edit

Address Type	Range Address
Start IP Address	192.168.1.10
End IP Address	192.168.1.20
Subnet Mask	0.0.0.0
Invert Selection	<input type="checkbox"/>
IP Group	None
or IP Object	None
or IP Object	None
or IP Object	None
IPv6 Group	None
or IPv6 Object	None
or IPv6 Object	None
or IPv6 Object	None

OK Close

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

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 3

Check to enable the Filter Rule

Comments: open_ip

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

Clear sessions when schedule ON: Enable

Direction: LAN/RT/VPN -> WAN

Source IP: 192.168.1.10~192.168.1.20 Edit

Destination IP: Any Edit

Service Type: Any Edit

Fragments: Don't Care

Application

Filter: Action/Profile Pass Immediately Syslog

Branch to Other Filter Set: None

8. Both filter rules have been created. Click OK.

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 2

Comments :

Filter Rule	Active	Comments	Move Up	Move Down
<input type="button" value="1"/>	<input checked="" type="checkbox"/>	xNetBios -> DNS		<u>Down</u>
<input type="button" value="2"/>	<input checked="" type="checkbox"/>	block_all	<u>UP</u>	<u>Down</u>
<input type="button" value="3"/>	<input checked="" type="checkbox"/>	open_ip	<u>UP</u>	<u>Down</u>
<input type="button" value="4"/>	<input type="checkbox"/>		<u>UP</u>	<u>Down</u>
<input type="button" value="5"/>	<input type="checkbox"/>		<u>UP</u>	<u>Down</u>
<input type="button" value="6"/>	<input type="checkbox"/>		<u>UP</u>	<u>Down</u>
<input type="button" value="7"/>	<input type="checkbox"/>		<u>UP</u>	

Next Filter Set

Now, all the settings are configured well. Only the computers with the IP addresses within 192.168.1.10 ~ 192.168.1.20 can access to Internet.

III-2 Central Security Management (CSM)

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

URL Content Filter

To provide an appropriate cyberspace to users, Vigor device 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 device 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

III-2-1 URL Content Filter Profile

To provide an appropriate cyberspace to users, Vigor device 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 device 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 device 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 device will discard any request that tries to retrieve the malicious code.

Click CSM and click URL Content Filter Profile to open the profile setting page.

CSM >> URL Content Filter Profile



URL Content Filter Profile Table: | [Set to Factory Default](#) |

Profile	Name	Profile	Name
1.		5.	
2.		6.	
3.		7.	
4.		8.	

Administration Message (Max 255 characters) [Preview](#) | Default Message

```
<body><center><br><p>The requested Web page has been blocked by URL Content Filter.
<p>Please contact your system administrator for further information.</center></body>
```

OK

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Profile	Display the number of the profile which allows you to click to set different policy.
Name	Display the name of the URL Content Filter Profile.

Administration Message	You can type the message manually for your necessity. Default Message - You can type the message manually for your necessity or click this button to get the default message which will be displayed on the field of Administration Message .
-------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

You can set eight profiles as URL content filter. Simply click the index number under Profile to open the following web page.

CSM >> URL Content Filter Profile

Profile Index: 1

Profile Name:

Priority: **Log:**

1.URL Access Control

Enable URL Access Control Prevent web access from IP address

Action:

Exception List

2.Web Feature

Enable Restrict Web Feature

Action: Cookie Proxy Upload **File Extension Profile:**

Available settings are explained as follows:

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

	<div data-bbox="708 203 1150 376"> <p>Both : Pass</p> <p>Both : Pass</p> <p>Both : Block</p> <p>Either : URL Access Control First</p> <p>Either : Web Feature First</p> </div>
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> <div data-bbox="708 600 826 770"> <p>None</p> <p>None</p> <p>Pass</p> <p>Block</p> <p>All</p> </div>
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 device 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 device 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 device performs.</p>

Object/Group Edit	
<u>Keyword Object</u>	None ▾
or Keyword Object	None ▾
or Keyword Object	None ▾
or Keyword Object	None ▾
or Keyword Object	None ▾
or Keyword Object	None ▾
or Keyword Object	None ▾
or Keyword Object	None ▾
or <u>Keyword Group</u>	None ▾
or Keyword Group	None ▾
or Keyword Group	None ▾
or Keyword Group	None ▾
or Keyword Group	None ▾
or Keyword Group	None ▾
or Keyword Group	None ▾
or Keyword Group	None ▾

Web Feature

Enable Restrict Web Feature - Check this box to make the keyword being blocked or passed.

Action - This setting is available only when **Either: URL Access Control First** or **Either: Web Feature First** is selected.

Pass - Allow accessing into the corresponding webpage with the keywords listed on the box below.

Block - Restrict accessing into the corresponding webpage with the keywords listed on the box below.
If the web pages do not match with the specified feature set here, it will be processed with reverse action.

Cookie - Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy.

Proxy - Check the box to reject any proxy transmission. To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages.

Upload - Check the box to block the file upload by way of web page.

File Extension Profile - Choose one of the profiles that you configured in **Object Setting>> File Extension Objects** previously for passing or blocking the file downloading.

File Extension Profile:

None ▾
None
1-image

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

Application Notes

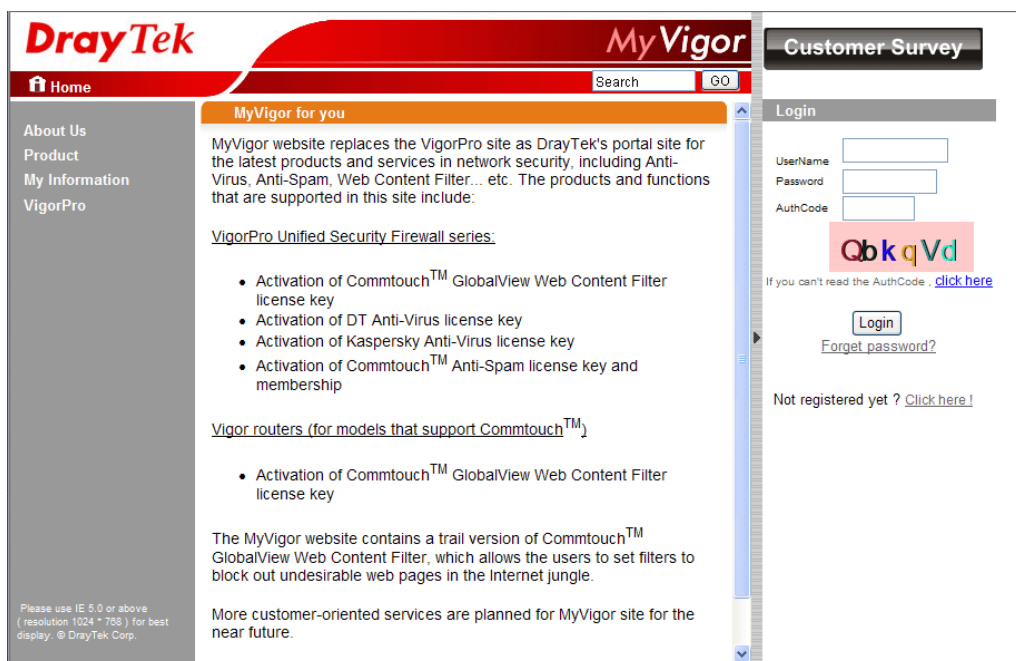
A-1 How to Create an Account for MyVigor

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

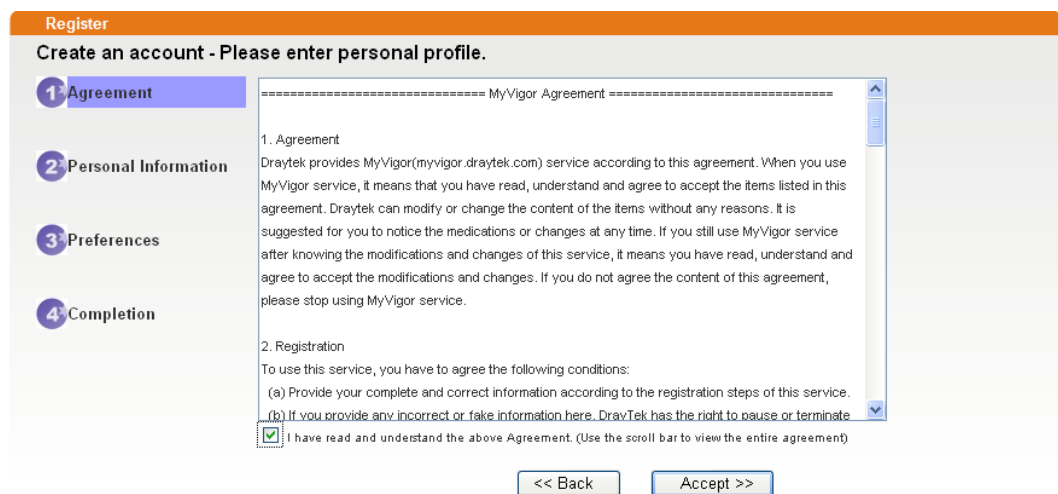
To access into MyVigor for getting more information, please create an account for MyVigor.

Create an Account via MyVigor Web Site

1. Access into <http://myvigor.draytek.com>. Find the line of **Not registered yet?**. Then, click the link **Click here!** to access into next page.



2. Check to confirm that you accept the Agreement and click **Accept**.



3. Type your personal information in this page and then click **Continue**.

The screenshot shows the 'Register' page with the 'Personal Information' step highlighted. The page title is 'Register' and the instruction is 'Create an account - Please enter personal profile. (Fields marked by (*) are required)'. The progress bar shows 4 steps: 1. Agreement, 2. Personal Information (highlighted), 3. Preferences, and 4. Completion. The 'Account Information' section includes: 'UserName:*' with the value 'Mary' and a 'Check Account' button; 'Password:*' with masked characters and a note '(3 - 20 characters)'; and 'Confirm Password:*' with masked characters and a note '(4 - 20 characters : Do not set the same as the username.)'. The 'Personal Information' section includes: 'First Name:*' with 'Mary'; 'Last Name:*' with 'Ted'; 'Company Name:' with 'Tech Ltd.'; 'Email Address:*' with 'mary_ted@tech.com' and a note 'Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.'; 'Tel:' with a field containing '0'; 'Country:*' with a dropdown menu set to 'SWITZERLAND'; and 'Career:*' with a dropdown menu set to 'Supervisor'. Navigation buttons '<< Back' and 'Continue >>' are at the bottom right.

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

The screenshot shows the 'Register' page with the 'Preferences' step highlighted. The page title is 'Register' and the instruction is 'Create an account - Please enter personal profile.'. The progress bar shows 4 steps: 1. Agreement, 2. Personal Information, 3. Preferences (highlighted), and 4. Completion. The 'Preferences' section includes: 'How did you find out about this website?' with a dropdown menu set to 'Internet'; 'What kind of anti-virus do you use?' with a dropdown menu set to 'AntiVir'; 'I would like to subscribe to the MyVigor e-letter.' with a checked checkbox; 'I would like to receive DrayTek product news.' with a checked checkbox; and 'Please select the mail server for receiving the verification mail.' with a dropdown menu set to 'Global Server'. Navigation buttons '<< Back' and 'Continue >>' are at the bottom right.

5. Now you have created an account successfully. Click **START**.

The screenshot shows the 'Register' page with the 'Completion' step highlighted. The page title is 'Register' and the instruction is 'Create an account - Please enter personal profile.'. The progress bar shows 4 steps: 1. Agreement, 2. Personal Information, 3. Preferences, and 4. Completion (highlighted). A grey box with the title 'Completion' contains the text: 'A confirmation email has been sent to mary_ted@tech.com. Please click on the activation link in the email to activate your account'. A large blue 'START' button is centered at the bottom of the page.

6. Check to see the confirmation *email* with the title of New Account Confirmation Letter from myvigor.draytek.com.

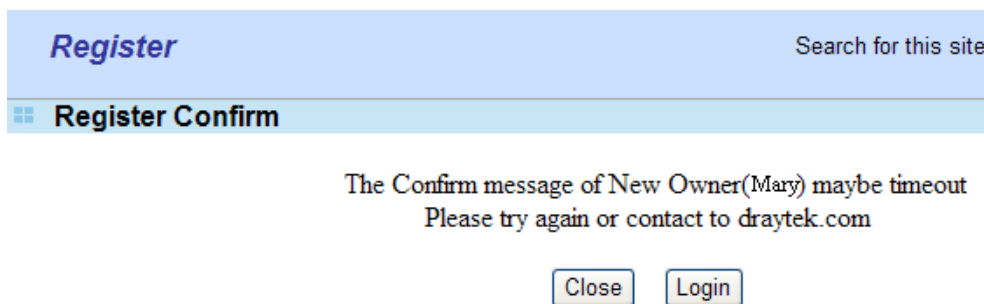
***** This is an automated message from myvigor.draytek.com.*****

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

Please click on the activation link below to activate your account

Link : [Activate my Account](#)

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



The screenshot shows a notification box with a blue header containing the word "Register" and a search bar. Below the header is a blue bar with the text "Register Confirm". The main content of the message reads: "The Confirm message of New Owner(Mary) maybe timeout Please try again or contact to draytek.com". At the bottom of the message are two buttons: "Close" and "Login".

8. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**. Then type the code in the box of **Auth Code** according to the value displayed on the right side of it.



Please take a moment to register.
Membership Registration entitles you to upgrade firmware for your purchased product and receive news about upcoming products and services!



The screenshot shows a login form with an orange header labeled "LOGIN". It contains three input fields: "UserName" with the value "Mary", "Password" with four dots, and "Auth Code" with the value "T4he1C". To the right of the "Auth Code" field is a red box containing the text "T4he1C". Below the input fields is a link "If you cannot read the word, [click here](#)". There is also a link "Forgotten password?" and a "Login" button. At the bottom of the form, there is a link "Don't have a MyVigor Account ? [Create an account now](#)".

If you are having difficulty logging in, contact our customer service.
Customer Service : (888) 3 597 2727 or

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

A-2 How to Block Facebook Service Accessed by the Users via URL Content Filter

A. Block the web page containing the word of “Facebook”

1. Open Object Settings>>Keyword Object. Click an index number to open the setting page.
2. In the field of Contents, please type *facebook*. Configure the settings as the following figure.

Objects Setting >> Keyword Object Setup

Profile Index : 1

Name	Facebook
Contents	facebook

Limit of Contents: Max 3 Words and 63 Characters.
Each word should be separated by a single space.

You can replace a character with %HEX.
Example:
Contents: backdoo%72 virus keep%20out

Result:
1. backdoor
2. virus
3. keep out

OK Clear Cancel

3. Open CSM>>URL Content Filter Profile. Click an index number to open the setting page.
4. Configure the settings as the following figure.

CSM >> URL Content Filter Profile

Profile Index: 1

Profile Name: Facebook

Priority: Either : URL Access Control First Log: None

1.URL Access Control

Enable URL Access Control Prevent web access from IP address

Action: Block Group/Object Selections: Facebook

2.Web Feature

Enable Restrict Web Feature

Action: Pass Cookie Proxy Upload File Extension Profile: None

OK Clear Cancel

5. When you finished the above steps, click OK. Then, open Firewall>>General Setup.

- Click the **Default Rule** tab. Choose the profile just configured from the drop down list in the field of **URL Content Filter**. Now, users cannot open any web page with the word "facebook" inside.

Firewall >> General Setup

General Setup

General Setup **Default Rule**

Actions for default rule:

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	None 1-Facebook	

OK Cancel

B. Disallow users to play games on Facebook

- Open **Object Settings>>Keyword Object**. Click an index number to open the setting page.
- In the field of **Contents**, please type *apps.facebook*. Configure the settings as the following figure.

Objects Setting >> Keyword Object Setup

Profile Index : 2

Name facebook-apps

Contents apps.facebook

Limit of Contents: Max 3 Words and 63 Characters.
Each word should be separated by a single space.

You can replace a character with %HEX.
Example:
Contents: backdoo%72 virus keep%20out

Result:

- backdoor
- virus
- keep out

OK Clear Cancel

- Open CSM>>URL Content Filter Profile. Click an index number to open the setting page.
- Configure the settings as the following figure.

CSM >> URL Content Filter Profile

Profile Index: 2

Profile Name:

Priority: Log:

1.URL Access Control

Enable URL Access Control Prevent web access from IP address

Action: Group/Object Selections:

2.Web Feature

Enable Restrict Web Feature

Action: Cookie Proxy Upload File Extension Profile:

- When you finished the above steps, please open Firewall>>General Setup.
- Click the **Default Rule** tab. Choose the profile just configured from the drop down list in the field of URL Content Filter. Now, users cannot open any web page with the word "facebook" inside.

Firewall >> General Setup

General Setup

General Setup **Default Rule**

Actions for default rule:

Application	Action/Profile	Syslog
Filter	<input type="text" value="Pass"/>	<input type="checkbox"/>
Sessions Control	<input type="text" value="0 / 10000"/>	<input type="checkbox"/>
URL Content Filter	<input type="text" value="None"/> (dropdown menu open showing: 1-Face, 2-face.apps)	<input type="checkbox"/>
Advance Setting		

Part IV Management



System
Maintenance

There are several items offered for the Vigor device system setup: System Status, TR-069, Administrator Password, Configuration Backup, Syslog /Mail Alert, Time and Date, Management, Reboot System, and Firmware Upgrade.

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, Reboot System, and Firmware Upgrade.

Below shows the menu items for System Maintenance.



A screenshot of a menu with a dark background and light text. The menu items are listed vertically. The 'System Maintenance' item is highlighted with a white background. The items are: Applications, System Maintenance, System Status, TR-069, Administrator Password, Configuration Backup, SysLog / Mail Alert, Time and Date, Management, Reboot System, Firmware Upgrade, and Diagnostics.

- Applications
- System Maintenance**
- System Status
- TR-069
- Administrator Password
- Configuration Backup
- SysLog / Mail Alert
- Time and Date
- Management
- Reboot System
- Firmware Upgrade
- Diagnostics

Web User Interface

IV-1-1 System Status

The System Status provides basic network settings of Vigor device. 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 : VigorNIC132F
Firmware Version : 3.7.9
Build Date/Time : Mar 30 2016 14:22:52

LAN				
MAC Address	1st IP Address	1st Subnet Mask	DHCP Server	DNS
LAN 00-1D-AA-89-42-B8	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-89-42-B9	PPPoE	---	---
WAN2 Disconnected	00-1D-AA-89-42-BA	Static IP	0.0.0.0	0.0.0.0

IPv6			
Address	Scope	Internet Access Mode	
LAN FE80::21D:AFF:FE89:42B8/64	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


	<ul style="list-style-type: none"> - Display the IP address of the WAN interface. <p>Default Gateway</p> <ul style="list-style-type: none"> - Display the assigned IP address of the default gateway.
IPv6	<p>Address - Display the IPv6 address for LAN.</p> <p>Scope - Display the scope of IPv6 address. For example, IPv6 Link Local could only be used for direct IPv6 link. It can't be used for IPv6 internet.</p> <p>Internet Access Mode - Display the connection mode chosen for accessing into Internet.</p>

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

ACS Server On	Internet
ACS Server	
URL	http://vigoracs.draytek.com/ACSServer/services/ACSServlet
Username	alpha
Password	*****
	Test With Inform
	Event Code
	PERIODIC
Last Inform Response Time	:Thu Aug 7 10:27:16 2014 
CPE Client	
	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
URL	http://111.251.216.33:8069/cwm/CRN.html
Port	8069
Username	vigor
Password	*****

Periodic Inform Settings

<input type="radio"/> Disable	
<input checked="" type="radio"/> Enable	
Interval Time	900 second(s)

STUN Settings

<input checked="" type="radio"/> Disable	
<input type="radio"/> Enable	
Server Address	
Server Port	3478
Minimum Keep Alive Period	60 second(s)
Maximum Keep Alive Period	-1 second(s)

Available settings are explained as follows:

Item	Description
ACS Server On	Choose the interface for the router connecting to ACS server.
ACS Server	<p>URL/Username/Password - Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information.</p> <p>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 IP - Type the IP address of the STUN server.</p> <p>Server Port - Type the port number of the STUN server.</p> <p>Minimum Keep Alive Period - If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds".</p> <p>Maximum Keep Alive Period - If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.</p>

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"/>	
New Password	<input type="text"/>	(Max. 23 characters allowed)
Confirm Password	<input type="text"/>	(Max. 23 characters allowed)

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>

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

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

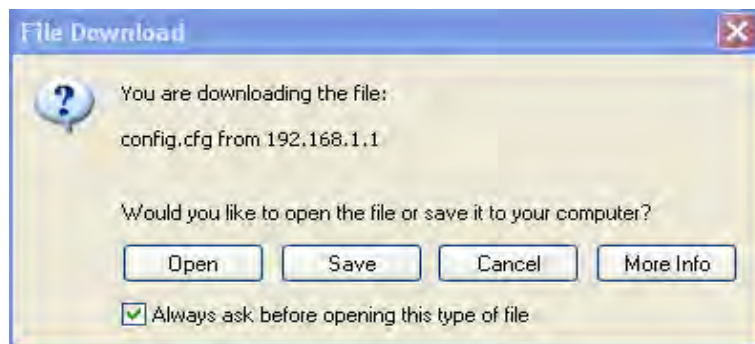
Configuration Backup / Restoration

Restore Restore settings from a configuration file. <input type="button" value="選擇檔案"/> 未選擇任何檔案 Click Restore to upload the file. <input type="button" value="Restore"/>
Backup Back up the current settings into a configuration file. <input type="button" value="Backup"/>

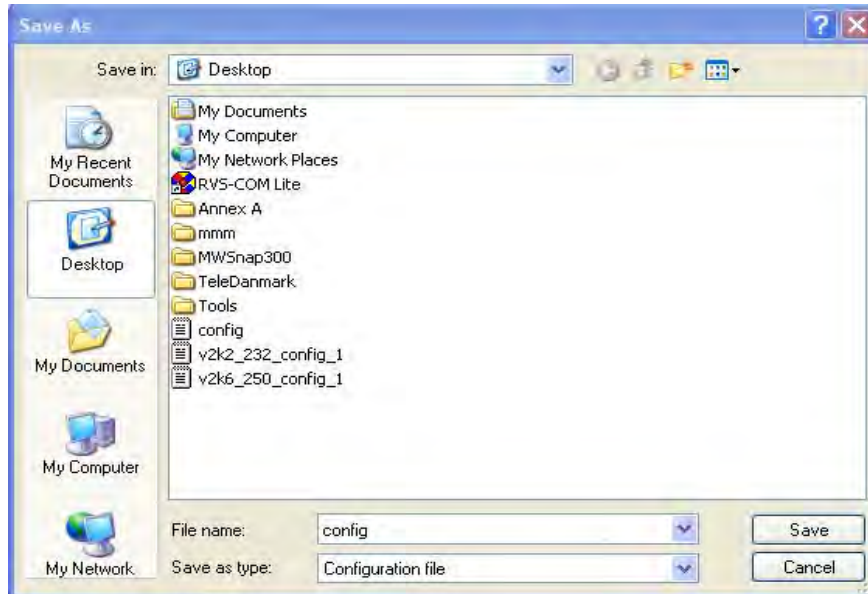
Available settings are explained as follows:

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 VigorNIC 132, 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	Click it to perform the configuration backup of this router.

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



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



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

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



Info

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

Restore Configuration

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

System Maintenance >> Configuration Backup

Configuration Backup / Restoration

<p>Restore</p> <p>Restore settings from a configuration file.</p> <p><input type="button" value="選擇檔案"/> 未選擇任何檔案</p> <p>Click Restore to upload the file.</p> <p><input type="button" value="Restore"/></p>
<p>Backup</p> <p>Back up the current settings into a configuration file.</p> <p><input type="button" value="Backup"/></p>

2. Click **Choose File** button to choose the correct configuration file for uploading to the router.
3. Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

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

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

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>
Router Name	<p>Display the name for such router configured in System Maintenance>>Management.</p> <p>If there is no name here, simply lick the link to access into System Maintenance>>Management to set the router name.</p> <p>Server IP Address -The IP address of the Syslog server.</p> <p>Destination Port - Assign a port for the Syslog protocol.</p> <p>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> <ul style="list-style-type: none"> ● Use SSL - Check this box to use port 465 for SMTP server for some e-mail server uses https as the transmission method. ● Authentication - Check this box to activate this

function while using e-mail application.

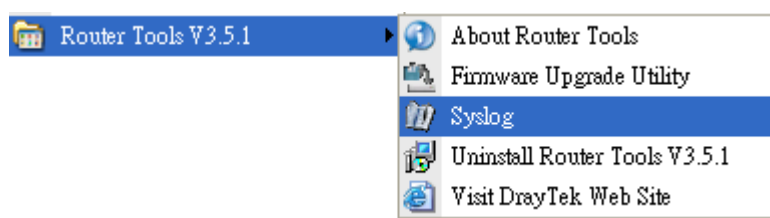
- **User Name** - Type the user name for authentication.
- **Password** - Type the password for authentication.

Enable E-mail Alert - Check the box to send alert message to the e-mail box while the router detecting the item(s) you specify here.

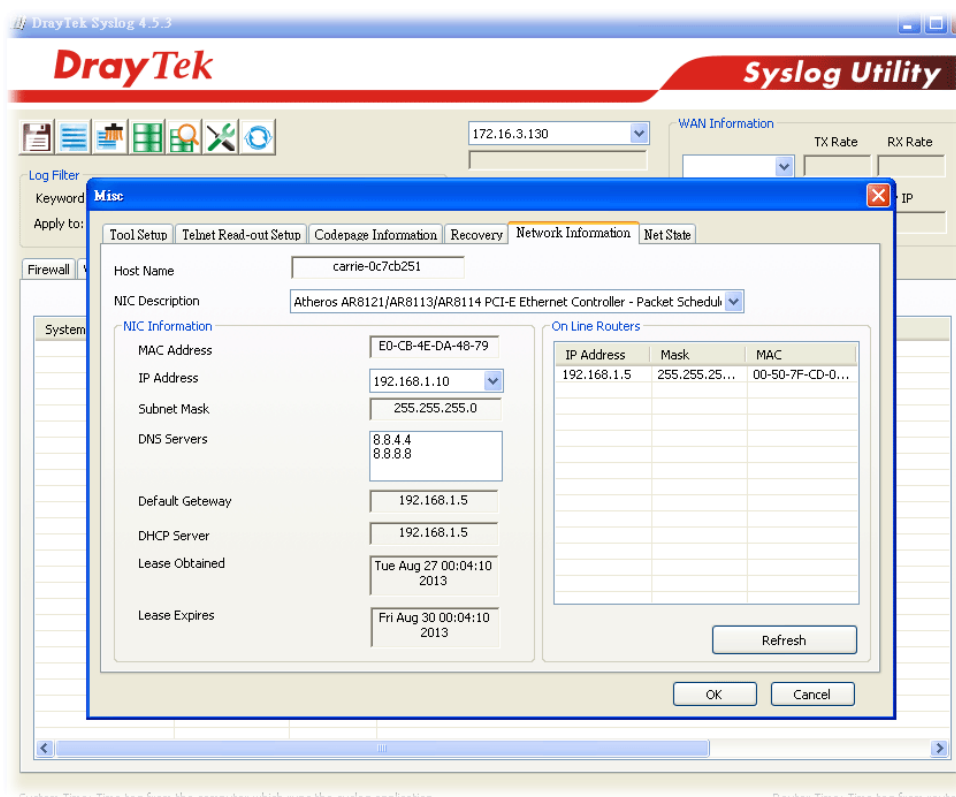
Click OK to save these settings.

For viewing the Syslog, please do the following:

1. Just set your monitor PC's IP address in the field of Server IP Address
2. Install the Router Tools in the **Utility** within provided CD. After installation, click on the **Router Tools>>Syslog** from program menu.



3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.



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: 2014 Aug 7 Thu 11 : 32 : 12 Inquire Time

Time Setup

Use Browser Time
 Use Internet Time

Time Server: pool.ntp.org

Priority: Auto

Time Zone: (GMT+08:00) Taipei

Enable Daylight Saving: Advanced

Automatically Update Interval: 1 day

OK Cancel

Available settings are explained as follows:

Item	Description
Current System Time	Click Inquire Time to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.
Time Server	Type the web site of the time server.
Priority	Choose Auto or IPv6 First as the priority.
Time Zone	Select the time zone where the router is located.
Enable Daylight Saving	Check the box to enable the daylight saving. Such feature is available for certain area. Advanced - Click it to open a pop up dialog.
Automatically Update Interval	<div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;"> <p>Daylight Saving Advanced</p> <p> <input checked="" type="radio"/> Default Start: No Daylight Saving End: No Daylight Saving </p> <p> <input type="radio"/> Date Range Start: Year Month Day 00:00 End: Year Month Day 00:00 </p> <p> <input type="radio"/> Yearly Start: Yearly On Januai First Sunda 00:00 End: Yearly On Januai First Sunda 00:00 </p> <p style="text-align: center;"> OK Close </p> </div> Use the default time setting or set user defined time for your requirement.

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"/> <input type="checkbox"/> Default:Disable Auto-Logout Internet Access Control <input type="checkbox"/> Allow management from the Internet Domain name allowed <input type="text"/> <input type="checkbox"/> FTP Server <input checked="" type="checkbox"/> HTTP Server <input checked="" type="checkbox"/> HTTPS Server <input checked="" type="checkbox"/> Telnet Server <input checked="" type="checkbox"/> TR069 Server <input type="checkbox"/> SSH Server <input checked="" type="checkbox"/> Disable PING from the Internet Access List from the Internet <table border="1"> <thead> <tr> <th>List</th> <th>IP</th> <th>Subnet Mask</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>2</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>3</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table>	List	IP	Subnet Mask	1	<input type="text"/>	<input type="text"/>	2	<input type="text"/>	<input type="text"/>	3	<input type="text"/>	<input type="text"/>	Management Port Setup <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports Telnet Port <input type="text" value="23"/> (Default: 23) HTTP Port <input type="text" value="80"/> (Default: 80) HTTPS Port <input type="text" value="443"/> (Default: 443) FTP Port <input type="text" value="21"/> (Default: 21) TR069 Port <input type="text" value="8069"/> (Default: 8069) SSH Port <input type="text" value="22"/> (Default: 22) 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 TLS/SSL Encryption Setup <input type="checkbox"/> Enable SSL 3.0 <input checked="" type="checkbox"/> Device Management <input type="checkbox"/> Respond to external device
List	IP	Subnet Mask											
1	<input type="text"/>	<input type="text"/>											
2	<input type="text"/>	<input type="text"/>											
3	<input type="text"/>	<input type="text"/>											

OK

Available settings are explained as follows:

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

Internet Access Control	<p>Allow management from the Internet - Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.</p> <p>Disable PING from the Internet - Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.</p>
Access List from the Internet	<p>You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.</p> <p>List IP - Indicate an IP address allowed to login to the router.</p> <p>Subnet Mask - Represent a subnet mask allowed to login to the router.</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. The maximum length of the text is limited to 23 characters.</p> <p>Set Community - Set community by typing a proper name. The default setting is private. The maximum length of the text is limited to 23 characters.</p> <p>Manager Host IP - Set one host as the manager to execute 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. The maximum length of the text is limited to 23 characters.</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 - Check the box to enable the function of SSL 3.0 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 VigorNIC 132.</p> <p>Respond to external device - If it is enabled, VigorNIC 132 will be regarded as slave device. When the external device (master device) sends request packet to VigorNIC 132, VigorNIC 132 would send back information to respond the request coming from the external device which is able to manage VigorNIC 132.</p>

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

For IPv6

System Maintenance >> Management



IPv4 Management Setup	IPv6 Management Setup
<p>Management Access Control</p> <p>Allow management from the Internet</p> <p><input type="checkbox"/> Telnet Server (Port : 23)</p> <p><input type="checkbox"/> HTTP Server (Port : 80)</p> <p><input type="checkbox"/> HTTPS Server (Port : 443)</p> <p><input type="checkbox"/> SSH Server (Port : 22)</p> <p><input type="checkbox"/> Enable PING from the Internet</p> <hr/> <p>Access List</p> <p>List IPv6 Address / Prefix Length</p> <p>1. <input type="text"/> / <input type="text" value="128"/></p> <p>2. <input type="text"/> / <input type="text" value="128"/></p> <p>3. <input type="text"/> / <input type="text" value="128"/></p> <p>Note : Telnet / Http server port is the same as IPv4.</p>	

OK

Available settings are explained as follows:

Item	Description
Management Access Control	<p>Allow management from the Internet - Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.</p> <p>Disable PING from the Internet - Check the checkbox to disable all PING packets from the Internet. For security issue, this function is enabled by default.</p>
Access List	<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>IPv6 Address /Prefix Length- Indicate the IP address(es) allowed to login to the router.</p>

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

IV-1-8 Reboot System

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

System Maintenance >> Reboot System

Reboot System

Do you want to reboot your router ?

Using current configuration
 Using factory default configuration

Auto Reboot Time Schedule

Index(1-15) in Schedule Setup: , , ,

Note: Action and Idle Timeout settings will be ignored.

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

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



Info

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

IV-1-9 Firmware Upgrade

Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is www.DrayTek.com (or local DrayTek's web site) and FTP site is ftp.DrayTek.com.

Click **System Maintenance**>> **Firmware Upgrade** to launch the Firmware Upgrade Utility.

System Maintenance >> Firmware Upgrade



Web Firmware Upgrade

Select a firmware file.

未選擇任何檔案

Click Upgrade to upload the file.

TFTP Firmware Upgrade from LAN

Current Firmware Version: 3.7.9

Firmware Upgrade Procedures:

1. Click "OK" to start the TFTP server.
2. Open the Firmware Upgrade Utility or other 3-party TFTP client software.
3. Check that the firmware filename is correct.
4. Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade.
5. After the upgrade is complete, the TFTP server will automatically stop running.

Do you want to upgrade firmware ?

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

Choose the right firmware by clicking **Select**. Then, click **Upgrade**. The system will upgrade the firmware of the router automatically.

Click **OK**. The following screen will appear. Please execute the firmware upgrade utility first.

System Maintenance >> Firmware Upgrade

TFTP server is running. Please execute a Firmware Upgrade Utility software to upgrade router's firmware. This server will be closed by itself when the firmware upgrading finished.

This page is left blank.

Part V Others



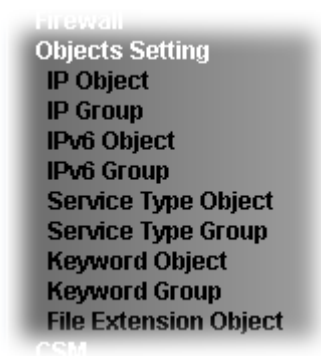
Objects Settings

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

For IPs in a range and service ports in a limited range usually will be applied in configuring router's settings, therefore we can define them with *objects* and bind them with *groups* for using conveniently. Later, we can select that object/group that can apply it. For example, all the IPs in the same department can be defined with an IP object (a range of IP address).

Web User Interface



V-1-1 IP Object

You can set up to 192 sets of IP Objects with different conditions.

Objects Setting >> IP Object

IP 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](#) >> [Next](#) >>

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.

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

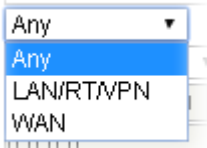
1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:

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:	0.0.0.0
Invert Selection:	<input type="checkbox"/>

OK Clear Cancel

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/VPN or any IP address. If you choose LAN/RT/VPN as the Interface here, and choose LAN/RT/VPN as the direction setting in Edit Filter Rule, then all the IP addresses specified with LAN/RT/VPN interface will be opened for you to choose in Edit Filter Rule page.</p>
Address Type	<p>Determine the address type for the IP address.</p> <p>Select Single Address if this object contains one IP address only.</p> <p>Select Range Address if this object contains several IPs within a range.</p> <p>Select Subnet Address if this object contains one subnet for IP address.</p> <p>Select Any Address if this object contains any IP address.</p> <p>Select Mac Address if this object contains Mac address.</p> 
MAC Address	Type the MAC address of the network card which will be controlled.
Start IP Address	Type the start IP address for Single Address type.
End IP Address	Type the end IP address if the Range Address type is

	selected.
Subnet Mask	Type the subnet mask if the Subnet Address type is selected.
Invert Selection	If it is checked, all the IP addresses except the ones listed above will be applied later while it is chosen.

- After finishing all the settings here, please click **OK** to save the configuration. Below is an example of IP objects settings.

Objects Setting >> IP Object

IP Object Profiles:

Index	Name	Index
<u>1.</u>	RD Department	<u>17.</u>
<u>2.</u>	Financial Dept	<u>18.</u>
<u>3.</u>	HR Department	<u>19.</u>
<u>4.</u>		<u>20.</u>
<u>5.</u>		<u>21.</u>
6.		22.

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

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.

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

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

Objects Setting >> IP Group

Profile Index : 1

Name:

Interface:

Available IP Objects

1-RD Department

2-Financial Dept

3-HR Department

>>

<<

Selected IP Objects

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Interface	Choose WAN, LAN or Any to display all the available IP objects with the specified interface.
Available IP Objects	All the available IP objects with the specified interface chosen above will be shown in this box.
Selected IP Objects	Click >> button to add the selected IP objects in this box.

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

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](#) >>

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 : 16

Name:	<input type="text"/>
Address Type:	Subnet Address <input type="button" value="v"/>
Mac Address:	00 : 00 : 00 : 00 : 00 : 00
Start IP Address:	<input type="text"/>
End IP Address:	<input type="text"/>
Prefix Length:	<input type="text"/>
Invert Selection:	<input type="checkbox"/>

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Address Type	<p>Determine the address type for the IPv6 address.</p> <p>Select Single Address if this object contains one IPv6 address only.</p> <p>Select Range Address if this object contains several IPv6s within a range.</p> <p>Select Subnet Address if this object contains one subnet for IPv6 address.</p> <p>Select Any Address if this object contains any IPv6 address.</p> <p>Select Mac Address if this object contains Mac address.</p> <div style="border: 1px solid black; padding: 2px; width: fit-content;"> <p>Range Address <input type="button" value="v"/></p> <p>Any Address</p> <p>Single Address</p> <p style="background-color: #e0e0e0;">Range Address</p> <p>Subnet Address</p> <p>Mac Address</p> </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.
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.	

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
<div style="border: 1px solid black; height: 100px;"></div>	<div style="border: 1px solid black; height: 100px;"></div>

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](#) >>

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.

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

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

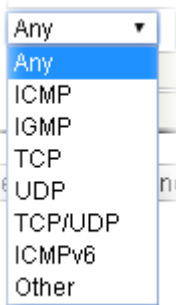
Objects Setting >> Service Type Object Setup

Profile Index : 1

Name	<input type="text" value="www"/>
Protocol	TCP <input type="text" value="6"/>
Source Port	= <input type="text" value="1"/> ~ <input type="text" value="65535"/>
Destination Port	= <input type="text" value="1"/> ~ <input type="text" value="65535"/>

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Protocol	Specify the protocol(s) which this profile will apply to. 
Source/Destination Port	Source Port and the Destination Port columns are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number. (=) - when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this profile. (!=) - when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type. (>) - the port number greater than this value is available. (<) - the port number less than this value is available for this profile.

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

Objects Setting >> Service Type Object

Service Type Object Profiles:

Index	Name	Index
<u>1.</u>	www	<u>17.</u>
<u>2.</u>	SIP	<u>18.</u>
<u>3.</u>		<u>19.</u>
<u>4.</u>		<u>20.</u>

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>	

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.

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

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

Objects Setting >> Service Type Group Setup

Profile Index : 1

Name:

Available Service Type Objects	Selected Service Type Objects
<div style="border: 1px solid black; padding: 2px;"> 1-www 2-SIP </div>	<div style="border: 1px solid black; height: 80px;"></div>
<input type="button" value=">>"/> <input type="button" value="<<"/>	

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Available Service Type Objects	All the available service objects that you have added on Objects Setting>>Service Type Object will be shown in this box.
Selected Service Type Objects	Click >> button to add the selected IP objects in this box.

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

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](#) >>

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.

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

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

Objects Setting >> Keyword Object Setup

Profile Index : 1

Name	<input type="text"/>
Contents	<input type="text"/>

Limit of Contents: Max 3 Words and 63 Characters.
Each word should be separated by a single space.

You can replace a character with %HEX.
Example:
Contents: backdoo%72 virus keep%20out

Result:
1. backdoor
2. virus
3. keep out

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile, e.g., game. Maximum 15 characters are allowed.
Contents	Type the content for such profile. For example, type <i>gambling</i> as Contents. When you browse the webpage, the page with gambling information will be watched out and be passed/blocked based on the configuration on Firewall settings.

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

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

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.

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

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

Objects Setting >> Keyword Group Setup

Profile Index : 1

Name:

Available Keyword Objects	Selected Keyword Objects(Max 16 Objects)
1-Key-1 2-Key-2	

Available settings are explained as follows:

Item	Description
Name	Type a name for this group. Maximum 15 characters are allowed.
Available Keyword Objects	You can gather keyword objects from Keyword Object page within one keyword group. All the available Keyword objects that you have created will be shown in this box.
Selected Keyword Objects	Click <input data-bbox="778 488 852 539" type="button" value=" >> "/> button to add the selected Keyword objects in this box.

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

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>	

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.

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

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

Objects Setting >> File Extension Object Setup

Profile Index: 1 Profile Name:

Categories	File Extensions
Image <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .bmp <input type="checkbox"/> .dib <input type="checkbox"/> .gif <input type="checkbox"/> .jpeg <input type="checkbox"/> .jpg <input type="checkbox"/> .jpg2 <input type="checkbox"/> .jp2 <input type="checkbox"/> .pct <input type="checkbox"/> .pcx <input type="checkbox"/> .pic <input type="checkbox"/> .pict <input type="checkbox"/> .png <input type="checkbox"/> .tif <input type="checkbox"/> .tiff
Video <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .asf <input type="checkbox"/> .avi <input type="checkbox"/> .mov <input type="checkbox"/> .mpe <input type="checkbox"/> .mpeg <input type="checkbox"/> .mpg <input type="checkbox"/> .mp4 <input type="checkbox"/> .qt <input type="checkbox"/> .rm <input type="checkbox"/> .wmv <input type="checkbox"/> .3gp <input type="checkbox"/> .3gpp <input type="checkbox"/> .3gpp2 <input type="checkbox"/> .3g2
Audio <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .aac <input type="checkbox"/> .aiff <input type="checkbox"/> .au <input type="checkbox"/> .mp3 <input type="checkbox"/> .m4a <input type="checkbox"/> .m4p <input type="checkbox"/> .ogg <input type="checkbox"/> .ra <input type="checkbox"/> .ram <input type="checkbox"/> .vox <input type="checkbox"/> .wav <input type="checkbox"/> .wma
Java <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .class <input type="checkbox"/> .jad <input type="checkbox"/> .jar <input type="checkbox"/> .jav <input type="checkbox"/> .java <input type="checkbox"/> .jcm <input type="checkbox"/> .js <input type="checkbox"/> .jse <input type="checkbox"/> .jsp <input type="checkbox"/> .jtk
ActiveX <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .alx <input type="checkbox"/> .apb <input type="checkbox"/> .axs <input type="checkbox"/> .ocx <input type="checkbox"/> .olb <input type="checkbox"/> .ole <input type="checkbox"/> .tlb <input type="checkbox"/> .viv <input type="checkbox"/> .vrm
Compression <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

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.

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-1Diagnostics

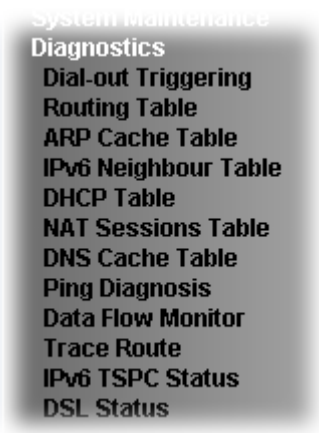
This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

If all above stages are done and the router still cannot run normally, it is the time for you to contact your dealer or DrayTek technical support for advanced help.

Web User Interface

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



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.

Diagnostics >> Dial-out Triggering

Dial-out Triggered Packet Header | [Refresh](#) |

HEX Format:

```
00 00 00 00 00 00 00-00 00 00 00 00 00-00 00
```



```
00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
```

Decoded Format:

```
0.0.0.0 -> 0.0.0.0
Pr 0 len 0 (0)
```

Available settings are explained as follows:

Item	Description
Decoded Format	It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.
Refresh	Click it to reload the page.

VI-1-2 Routing Table

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

Diagnostics >> View Routing Table

Current Running Routing Table	IPv6 Routing Table	Refresh
Key: C - connected, S - static, R - RIP, * - default, ~ - private		
C~ 192.168.1.0/ 255.255.255.0 directly connected LAN		

Note: WAN3, WAN4, WAN5 are router-borne WANs.

Diagnostics >> View Routing Table

Current Running Routing Table	IPv6 Routing Table	Refresh		
Destination	Interface	Flags	Metric	Next Hop
FE80::/64	LAN	U	256	
FF00::/8	LAN	U	256	

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

Ethernet ARP Cache Table			Clear	Refresh
IP Address	MAC Address	Netbios Name		
192.168.1.5	00-05-5D-E4-D8-EE	A1000351		

Show Comment

Available settings are explained as follows:

Item	Description
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 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		DHCPv6 IP Assignment Table			Refresh
DHCP server: Running					
Index	IP Address	MAC Address	Leased Time	HOST ID	
<input type="checkbox"/> Show Comment					

and

Diagnostics >> View DHCP Assigned IP Addresses

DHCP IP Assignment Table		DHCPv6 IP Assignment Table			Refresh
DHCPv6 server binding client:					
Index	IPv6 Address	MAC Address	Leased Time		
<input type="checkbox"/> Show Comment					

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 | [Refresh](#)

Private IP :Port	#Pseudo Port	Peer IP :Port	Interface
192.168.1.11 2491	52078	24.9.93.189 443	WAN1
192.168.1.11 2493	52080	207.46.25.2 80	WAN1
192.168.1.10 3079	52665	207.46.5.10 80	WAN1

Available settings are explained as follows:

Item	Description
Private IP:Port	It indicates the source IP address and port of local PC.
#Pseudo Port	It indicates the temporary port of the router used for NAT.
Peer IP:Port	It indicates the destination IP address and port of remote host.
Interface	It displays the representing number for different interface.
Refresh	Click it to reload the page.

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 device's Cache temporarily and displayed on **Diagnostics >> DNS Cache Table**.

Diagnostics >> DNS Cache Table

IPv4 DNS Cache Table	IPv6 DNS Cache Table	Clear	Refresh
Domain Name	IP Address	TTL (s)	

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

IPV4 IPV6
Note: If you want to ping a LAN PC or you don't want to specify which WAN to ping through, please select "Unspecified".
 Ping through:

Ping to: IP Address:

Result | [Clear](#) |

or

Diagnostics >> Ping Diagnosis

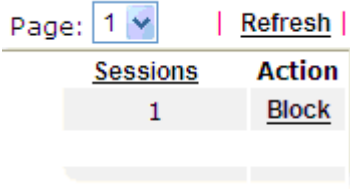

Ping Diagnosis

IPV4 IPV6
 Ping IPv6 Address:

Result | [Clear](#) |

Available settings are explained as follows:

Item	Description
IPV4 /IPV6	Choose the interface for such function.
Ping through	Use the drop down list to choose the WAN/LTE interface that you want to ping through or choose Unspecified to be determined by the router automatically.
Ping to	Use the drop down list to choose the destination that you want to ping.
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

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
 Trace through:
 Protocol:
 Host / IP Address:

Result | [Clear](#) |

or

Diagnostics >> Trace Route

Trace Route

IPV4 IPV6
 Trace Host / IP Address:

Result | [Clear](#) |

Available settings are explained as follows:

Item	Description
IPv4 / IPv6	Click one of them to display corresponding information for it.
Trace through	Use the drop down list to choose the interface that you want to ping through.

Protocol	Use the drop down list to choose the protocol that you want to ping through.
Host/IP Address	It indicates the IP address of the host.
Trace Host/IP Address	It indicates the IPv6 address of the host.
Run	Click this button to start route tracing work.
Clear	Click this link to remove the result on the window.

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	WAN2	Refresh
TSPC Enabled TSPC Connection Status Local Endpoint v4 Address : 114.44.54.220 Local Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b9 Router DNS name : 88886666.broker.freenet6.net Remote Endpoint v4 Address : 81.171.72.11 Remote Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b8 Tspc Prefix : 2001:05c0:1502:0d00:0000:0000:0000:0000 Tspc Prefixlen : 56 Tunnel Broker : amsterdam.freenet6.net Tunnel Status : Connected		

Available settings are explained as follows:

Item	Description
Refresh	Click this link to refresh this page manually.

VI-1-12 DSL Status

Such page is useful for RD debug or web technician.

Diagnostics >> DSL Status

General		Refresh		
ATU-R Information				
Type:	ADSL2/2+			
Hardware:				
Firmware:	05-04-08-00-00-06			
Power Mngt Mode:	DSL_G997_PMS_NA			
Line State:	TRAINING			
Running Mode:				
Vendor ID:	b5004946 544e0000			
ATU-C Information				
Vendor ID:	00000000 00000000 [unknown]			
Line Statistics				
	Downstream		Upstream	
Actual Rate	0	Kbps	0	Kbps
Attainable Rate	0	Kbps	0	Kbps
Path Mode	Fast		Fast	
Interleave Depth	0		0	
Actual PSD	0.0	dB	0.0	dB
	Near End		Far End	
Trellis	ON		ON	
Bitswap	OFF		OFF	
SNR Margin	0	dB	0	dB
Attenuation	0	dB	0	dB
CRC	0		0	
FECS	0	s	0	s
ES	0	s	0	s
SES	0	s	0	s
LOSS	0	s	0	s

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 LAN cable connections. Refer to “I-2 Hardware Installation” for details.
2. Make sure the ACT LED on the card blink once per second.
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



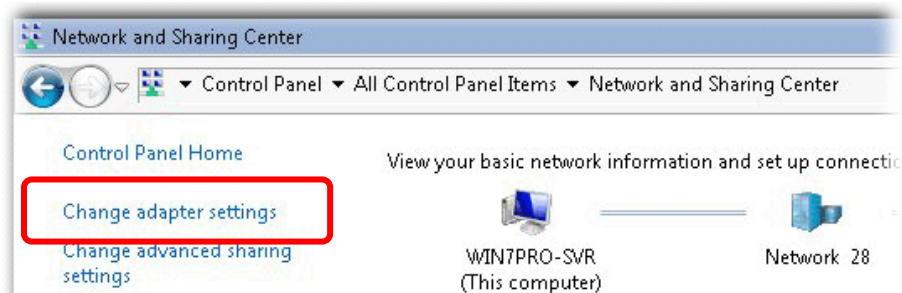
Info

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.

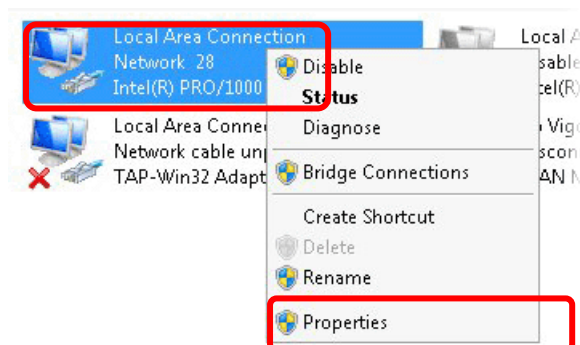
1. Open **All Programs>>Getting Started>>Control Panel**. Click **Network and Sharing Center**.



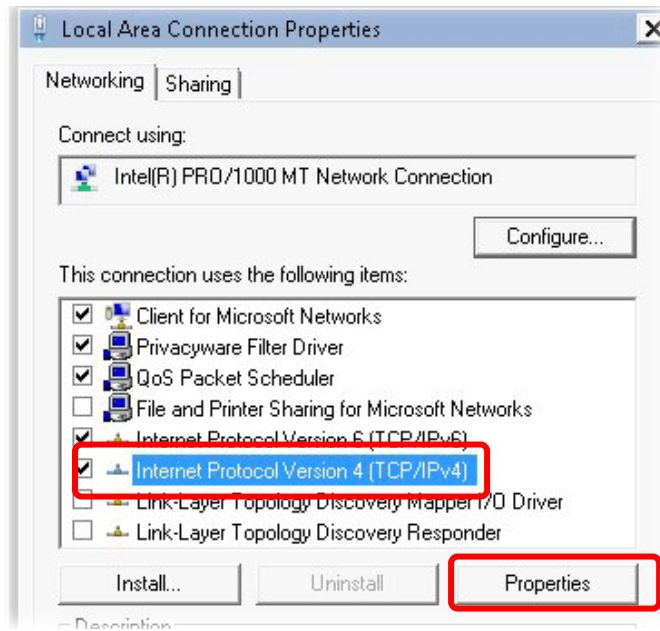
2. In the following window, click **Change adapter settings**.



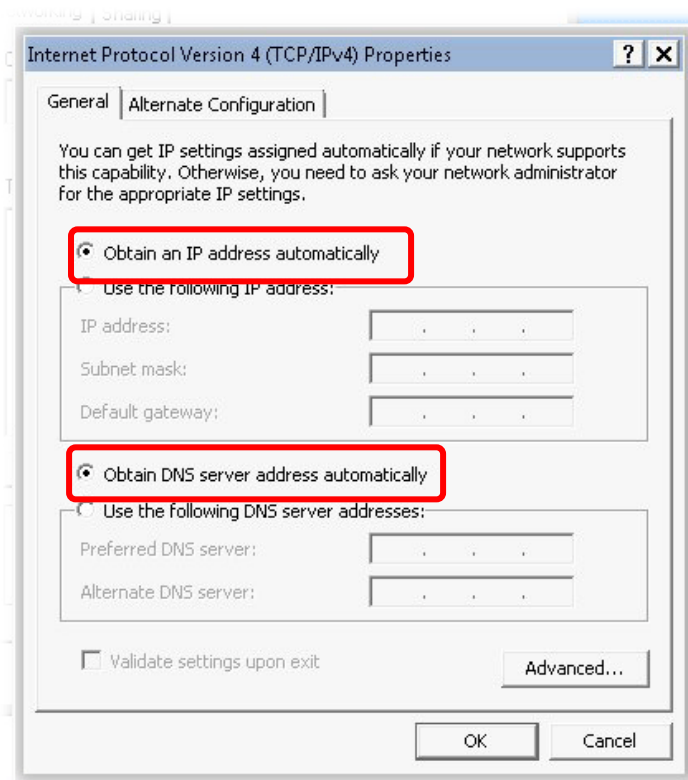
3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



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

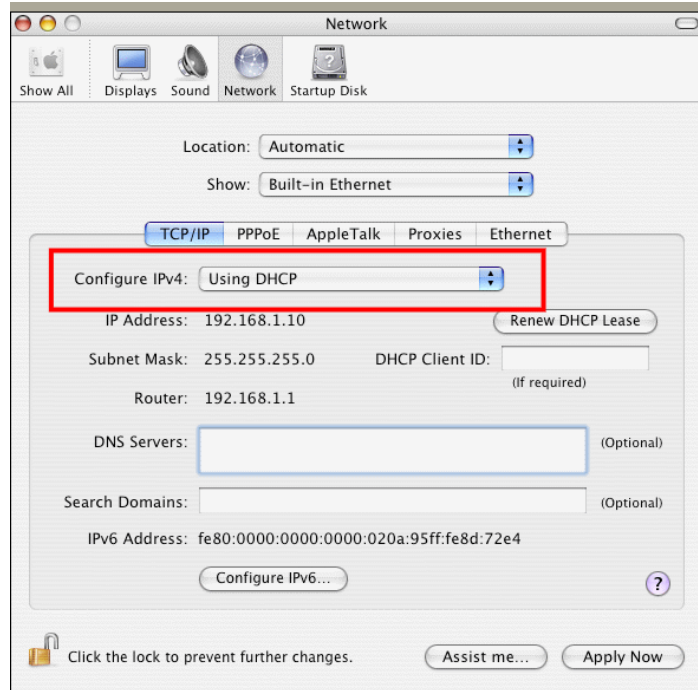


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



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.



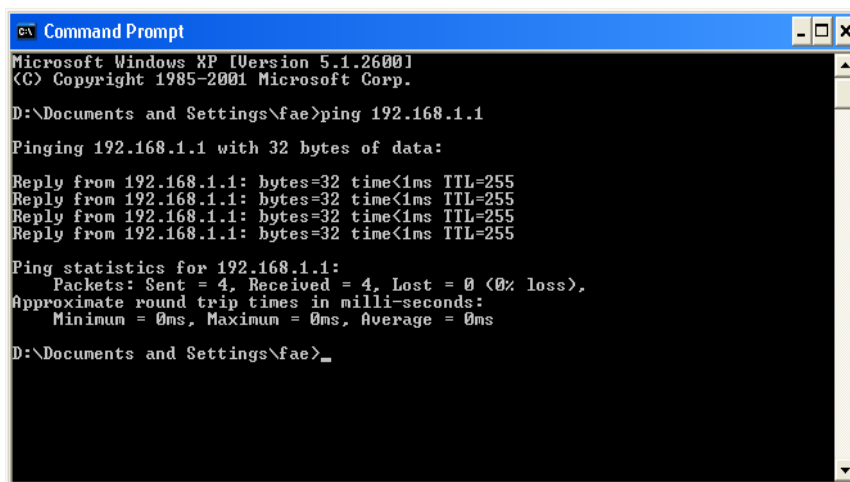
VI-4 Pinging the Device from Your Computer

The default gateway IP address of the device is 192.168.1.1. For some reason, you might need to use “ping” command to check the link status of the device. **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 VI-3)

Please follow the steps below to ping the router correctly.

For Windows

1. Open the Command Prompt window (from Start menu> Run).
2. Type command (for Windows 95/98/ME) or cmd (for Windows NT/ 2000/XP/Vista/7). The DOS command dialog will appear.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fae>_
```

3. Type ping 192.168.1.1 and press [Enter]. If the link is OK, the line of “Reply from 192.168.1.1:bytes=32 time<1ms TTL=255” will appear.
4. If the line does not appear, please check the IP address setting of your computer.

For Mac OS (Terminal)

1. Double click on the current used MacOs on the desktop.
2. Open the Application folder and get into Utilities.
3. Double click Terminal. The Terminal window will appear.
4. Type ping 192.168.1.1 and press [Enter]. If the link is OK, the line of “64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms” will appear.

```
Terminal - bash - 80x24
Last login: Sat Jan 3 02:24:18 on 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-2) are correct or not. If the LEDs are off, please:

- Change the **Physical Type** from **Auto negotiation** to other values (e.g., 100M full duplex).
- Next, change the physical type of modem (e.g., DSL/FTTX(GPON)/Cable modem) offered by ISP with the same value configured in Vigor device. Check if the LEDs on Vigor device are on or not.
- If not, please install an additional switch for connecting both Vigor device and the modem offered by ISP. Then, check if the LEDs on Vigor device are on or not.
- If the problem of LEDs cannot be solved by the above measures, please contact with the nearest reseller, or send an e-mail to DrayTek FAE for technical support.
- Check if the settings offered by ISP are configured well or not.

When the LEDs are on and correct, yet the WAN connection still cannot be up, please:

- Open **WAN >> Internet Access** page and then check whether the ISP settings are set correctly. Click **Details Page** of WAN1~WAN2 to review the settings that you configured previously.

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode	Details Page	IPv6
WAN1		ADSL	PPPoE / PPPoA	Details Page	IPv6
WAN2		Fiber	Static or Dynamic IP	Details Page	IPv6

Note: Only one WAN can support IPv6.

Advanced You can configure DHCP client options here.

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 device will return all the settings to the factory settings.

System Maintenance >> Reboot System

Reboot System

Do you want to reboot your router ?

- Using current configuration
 Using factory default configuration

Reboot Now

Auto Reboot Time Schedule

Index(1-15) in Schedule Setup: , , ,

Note: Action and Idle Timeout settings will be ignored.

OK

Cancel

Hardware Reset

While the device is running (ACT LED blinking), press the 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.

This page is left blank.

Part VII Telnet Commands

Accessing Telnet of VigorNIC 132

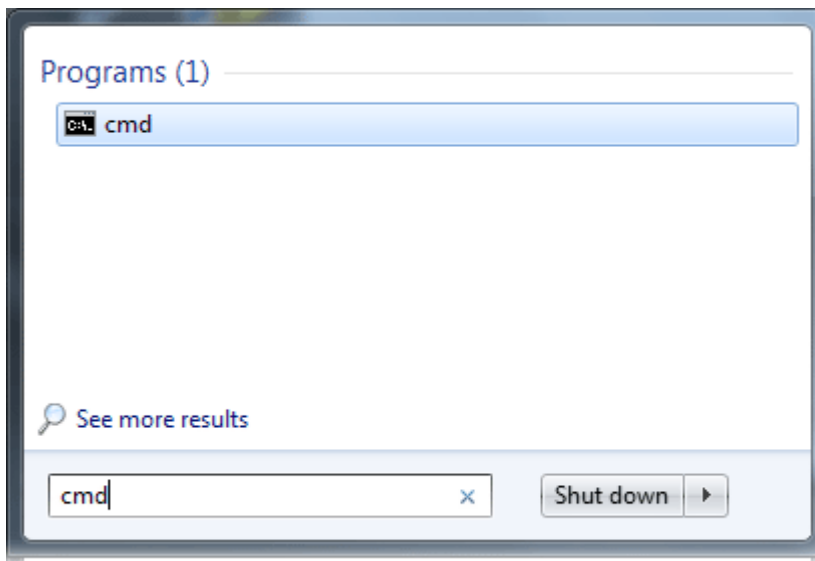
This chapter also gives you a general description for accessing telnet and describes the firmware versions for the routers explained in this manual.



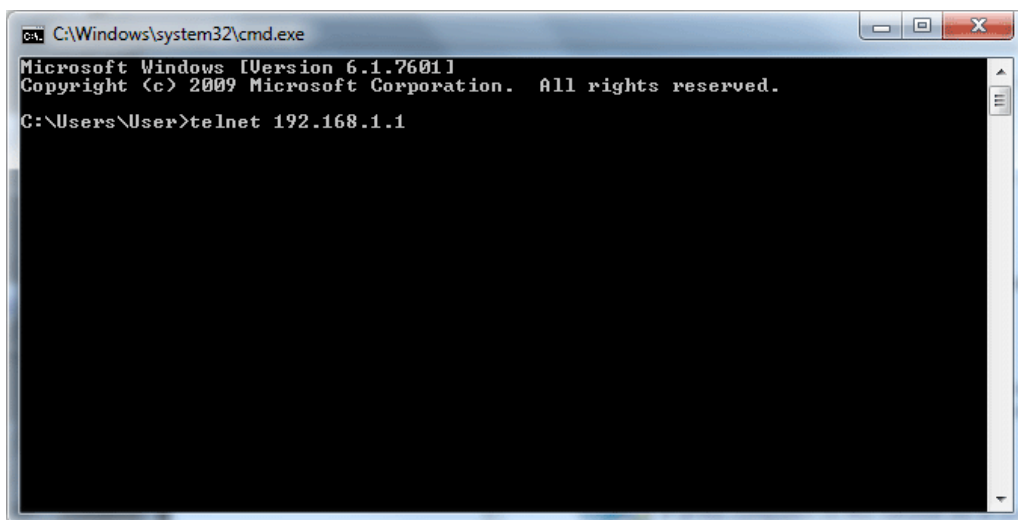
Info

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

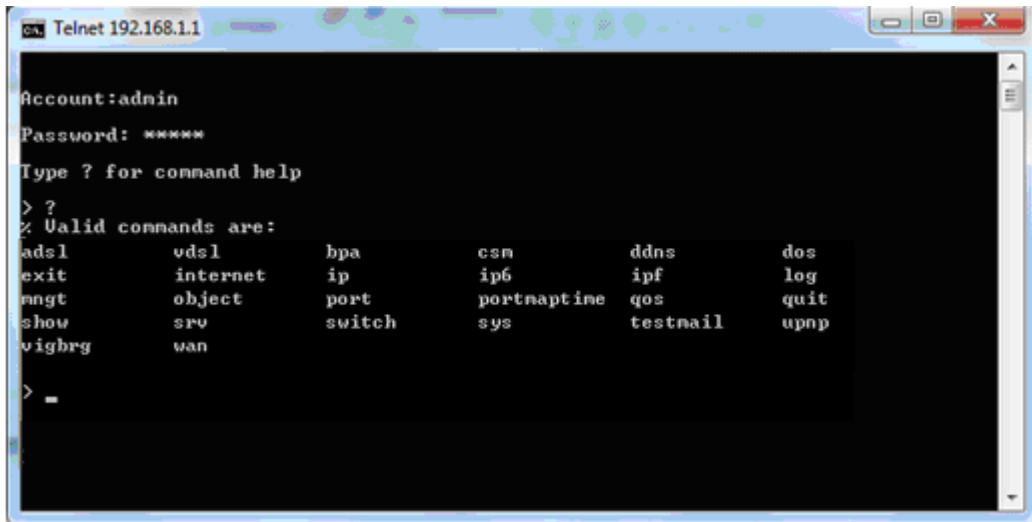
Type cmd and press Enter. The Telnet terminal will be open later.



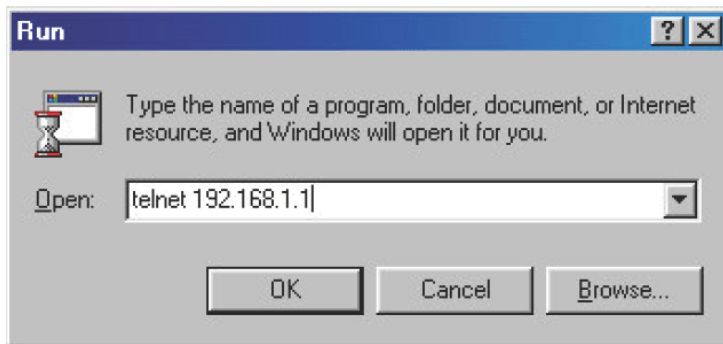
In the following window, type Telnet 192.168.1.1 as below and press Enter. Note that the IP address in the example is the default address of the router. If you have changed the default, enter the current IP address of the router.



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



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



Telnet Command: adsl txpct /adsl rxpct

This command allows the user to adjust the percentage of data transmission (receiving/transmitting) for QoS application.

Syntax

adsl txpct [auto:percent]

adsl rxpct [auto:percent]

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

Example

```
> adsl txpct auto
% tx percentage : 80
> adsl txpct 75
% tx percentage : 75
```

Telnet Command: adsl status

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

Syntax

adsl status [more | counts | hlog | qln | snr | bandinfo | olr]

Example

```
> > adsl status
----- ATU-R Info (hw: annex B, f/w: annex X) -----
Running Mode      :          State      : TRAINING
DS Actual Rate    :          0 bps      US Actual Rate    :          0 bps
DS Attainable Rate :          0 bps      US Attainable Rate :          0 bps
DS Path Mode      :          Fast       US Path Mode       :          Fast
DS Interleave Depth :          0        US Interleave Depth :          0
NE Current Attenuation :          0 dB    Cur SNR Margin     :          0 dB
DS actual PSD     :          0.0 dB      US actual PSD      :          0.0 dB
NE Rcvd Cells     :          0          NE Xmitted Cells   :          0
NE CRC Count      :          0          FE CRC Count       :          0
NE ES Count       :          0          FE ES Count        :          0
Xdsl Reset Times  :          0          Xdsl Link Times    :          0
ITU Version[0]    : b5004946          ITU Version[1]    : 544e0000
ADSL Firmware Version : 05-04-04-05-01-02
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: adsl ppp

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

Syntax

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

Syntax Description

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

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

Example

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

```
AcquireIP: Dhcp_client(1)
Idle timeout:-1
Username=draytek
Password=draytek
```

Telnet Command: adsl bridge

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

Syntax

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

Syntax Description

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

Example

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

Telnet Command: adsl idle

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

Syntax

`adsl idle [on | tcpmessage | tcpmessage_off]`

Syntax Description

Parameter	Description
<code>on</code>	DSL is under test mode. DSL debug tool mode is off.
<code>tcpmessage</code>	DSL debug tool mode is on.
<code>tcpmessage_off</code>	DSL debug tool mode is off.

Example

```
> adsl idle on
% DSL is under [IDLE/QUIET] test mode.
% DSL debug tool mode is off.
> adsl idle tcpmessage
% Set DSL debug tool mode on. Please reboot system to take effect.

> adsl idle tcpmessage_off
% Set DSL debug tool mode off. Please reboot system to take effect.
```

Telnet Command: adsl drivemode

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

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

Telnet Command: adsl reboot

This command can reboot the router.

Example

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


Telnet Command: adsl oamlb

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

Syntax

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

adsl oamlb chklink [*on/off*]

adsl oamlb [*log_on/log_off*]

Syntax Description

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

Example

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

Telnet Command: adsl vcilimit

This command can cancel the limit for vci value.

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

Syntax

adsl vcilimit [*n*]

Syntax Description

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

Example

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

Telnet Command: adsl annex

This command can display the annex interface of this router.

Example

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

Telnet Command: adsl automode

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

Syntax

`adsl automode [add|remove|set|default|show] [adsl_mode]`

Syntax Description

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

Example

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

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

Telnet Command: adsl showbins

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

Syntax

`adsl showbins [startbin endbin | up]`

Syntax Description

Parameter	Description
<i>startbin</i>	The number is between 0 ~ 4092.
<i>endbin</i>	The number is between 4 ~ 4095.
<i>up</i>	Show upstream information.

Example

```
> adsl showbins 2 30
DOWNSTREAM :
```

Bin	SNR	Gain	Bi	-	Bin	SNR	Gain	Bi	-	Bin	SNR	Gain	Bi	-	Bin	SNR	Gain	Bi
	dB	.1dB	ts			dB	.1dB	ts			dB	.1dB	ts			dB	.1dB	ts
Bin	SNR	Gain	Bi	-	Bin	SNR	Gain	Bi	-	Bin	SNR	Gain	Bi	-	Bin	SNR	Gain	Bi
	dB	.1dB	ts			dB	.1dB	ts			dB	.1dB	ts			dB	.1dB	ts

Telnet Command: adsl optn

This command allows you to configure DSL line feature.

Syntax

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

Syntax Description

Parameter	Description
<i>FUNC</i>	Available settings contain: 'bitswap', 'sra', 'aelem', 'g.vector', 'status', 'trellis', 'retx', 'default'.
<i>us/ds/bi</i>	us: upstream ds: downstream bi: bidirection. 'aelem' and 'g.vector' can be only on/off.
<i>value</i>	The value shall be hex digits. bitswap=0-2, sra=0,2,3,4.
<i>on/off</i>	Type "on" for enabling such function. Type "off" for disabling such function.

Example

```
> adsl optn default
trellis      [US] =      ON, [DS] =      ON.
bitswap     [US] =      0, [DS] =      0.
            [0: default(ON), 1: ON, 2: OFF]
sra         [US] =      0, [DS] =      0.
            [0: default(=3), 2: OFF, 3: ON , 4: DYNAMIC_SOS]
retx        [US] =      ON, [DS] =      ON.
aelem       ON
G.Vector    ON
```

Telnet Command: adsl savecfg

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

Example

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

Telnet Command: adsl vendorid

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

Syntax

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

Syntax Description

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

Example

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

Telnet Command: adsl atm

This command can set QoS parameter for ATM.

Syntax

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

`adsl atm scr [pvc_no][SCR]`

`adsl atm mbs [pvc_no][MBS]`

`adsl atm status`

Syntax Description

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

Example

```
> adsl atm pcr 1 200 max
% PCR is 200 for pvc 1.

> adsl atm pcr status
pvc  channel      PCR
-----
```

```

0      1      0
1      2      200
2      3      0
3      4      0
4      5      0
5      6      0
6      7      0
7      8      0
> adsl atm mbs 2 300 max
% MBS is 300 for pvc 2.

```

Telnet Command: adsl pvcbinding

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

Syntax

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

Syntax Description

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

Example

```

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

```

The above example means PVC3 has been bound to PVC5.

```

> adsl pvcbinding 3 -1
clear pvc-1 binding

```

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

Telnet Command: vdsl status

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

Syntax

vdsl status [*more* | *counts* | *hlog* | *qln* | *snr* | *bandinfo* | *olr*]

Example

```

> vdsl status
----- ATU-R Info (hw: annex A, f/w: annex A/B/C) -----
Running Mode      :          State      : TRAINING
DS Actual Rate    :          0 bps    US Actual Rate      :          0 bps
DS Attainable Rate :          0 bps    US Attainable Rate  :          0 bps
DS Path Mode      :          Fast     US Path Mode        :          Fast
DS Interleave Depth :          0      US Interleave Depth :          0
NE Current Attenuation :          0 dB    Cur SNR Margin      :          0 dB
DS actual PSD     :          0.0 dB    US actual PSD       :          0.0 dB
NE CRC Count      :          0        FE CRC Count        :          0
NE ES Count       :          0        FE ES Count         :          0
Xdsl Reset Times  :          0        Xdsl Link Times     :          0

```

```

ITU Version[0]      : b5004946      ITU Version[1]      : 544e0000
VDSL Firmware Version : 05-04-08-00-00-06
Power Management Mode : DSL_G997_PMS_NA
Test Mode          : DISABLE
----- ATU-C Info -----
Far Current Attenuation :      0 dB      Far SNR Margin      :      0 dB
CO ITU Version[0]      : 00000000      CO ITU Version[1]      : 00000000
DSLAM CHIPSET VENDOR   : < unknown >
>

```

Telnet Command: vdsl idle

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

Syntax

`vdsl idle [on | tcpmessage | tcpmessage_off]`

Syntax Description

Parameter	Description
<i>on</i>	DSL is under test mode. DSL debug tool mode is off.
<i>tcpmessage</i>	DSL debug tool mode is on.
<i>tcpmessage_off</i>	DSL debug tool mode is off.

Example

```

> vdsl idle on
% DSL is under [IDLE/QUIET] test mode.
% DSL debug tool mode is off.
> vdsl idle tcpmessage
% Set DSL debug tool mode on. Please reboot system to take effect.

> vdsl idle tcpmessage_off
% Set DSL debug tool mode off. Please reboot system to take effect.

```

Telnet Command: vdsl drivermode

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

1. Please connect dsl line to the DSLAM.
2. Waiting for dsl SHOWTIME.
3. Drop the dsl line.
4. Now, it is on continuous sending mode, and vdsl2/2+ led is always ON.
5. Use 'vdsl reboot' to restart dsl to normal mode.

Telnet Command: vdsl reboot

This command can reboot the DSL router.

Example

```

> vdsl reboot
% Adsl is Rebooting...

```

Telnet Command: vdsl annex

This command can display the annex interface of this router.

Example

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

Telnet Command: vdsl showbins

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

Syntax

`vdsl showbins [startbin endbin | up]`

Syntax Description

Parameter	Description
<i>startbin</i>	The number is between 0 ~ 4092.
<i>endbin</i>	The number is between 4 ~ 4095.
<i>up</i>	Show upstream information.

Example

```
> vdsl showbins 2 30
DOWNSTREAM :
-----
Bin  SNR  Gain Bi - Bin  SNR  Gain Bi - Bin  SNR  Gain Bi - Bin  SNR  Gain Bi
   dB  .1dB ts     dB  .1dB ts     dB  .1dB ts     dB  .1dB ts
-----
Bin  SNR  Gain Bi - Bin  SNR  Gain Bi - Bin  SNR  Gain Bi - Bin  SNR  Gain Bi
   dB  .1dB ts     dB  .1dB ts     dB  .1dB ts     dB  .1dB ts
```

Telnet Command: vdsl optn

This command allows you to configure DSL line feature.

Syntax

`vdsl optn FUNC [us/ds/bi [value/on/off]]`

Syntax Description

Parameter	Description
<i>FUNC</i>	Available settings contain: 'bitswap', 'sra', 'aelem', 'g.vector', 'status', 'trellis', 'retx', 'default'.
<i>us/ds/bi</i>	us: upstream ds: downstream bi: bidirection. 'aelem' and 'g.vector' can be only on/off.
<i>value</i>	The value shall be hex digits. bitswap=0-2, sra=0,2,3,4.
<i>on/off</i>	Type "on" for enabling such function.

Type "off" for disabling such function.

Example

```
> vdsl optn default
trellis      [US] =    ON, [DS] =    ON.
bitswap     [US] =    0, [DS] =    0.
             [0: default(ON), 1: ON, 2: OFF]
sra         [US] =    0, [DS] =    0.
             [0: default(=3), 2: OFF, 3: ON , 4: DYNAMIC_SOS]
retx        [US] =    ON, [DS] =    ON.
aelem       ON
G.Vector    ON
```

Telnet Command: vdsl savecfg

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

Example

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

Telnet Command: vdsl vendorid

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

Syntax

`vdsl vendorid [status/on/off/ set vid0 vid1]`

Syntax Description

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

Example

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

Telnet Command: vdsl inventory

This command is used to display information about CO or CPE.

Syntax

`vdsl inventory [co/cpe]`

Syntax Description

Parameter	Description
<i>co</i>	It means DSLAM (Digital Subscriber Line Access Multiplexer) or CO (Central Office).
<i>cpe</i>	It means CPE (Customer Premise Equipment).

Example

```

> vdsl inventory co
xDSL inventory info only available in showtime.
> vdsl inventory cpe
G.994 vendor ID           : 0XB5004946544E5444
  G.994.1 country code    : 0XB500
  G.994.1 provider code   : IFTN
  G.994.1 vendor info     : 0X5444
System vendor ID         : 0XB5004946544E0000
  System country code     : 0XB500
  System provider code    : IFTN
  System vendor info      : 0X000
Version number           : 3.8.2_RC4a_STD
Version number(16 octets) : 0X332E382E325F524334615F5354440000
Self-test result         : PASS
Transmission mode capability : 0X40004004C010400
>

```

Telnet Command: bpa

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

Syntax

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

Syntax Description

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

Example

```

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

```

```
ServerIP[1]:4  
  
-----index: 2 inactive-----  
UserName[2]:  
PassWord[2]:  
ServerIP[2]:0  
  
>
```

Telnet Command: csm 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 | -l [P/B/A/N] | uac | wf]`

`csm ucf obj INDEX -n PROFILE_NAME`

`csm ucf obj INDEX -p VALUE`

`csm ucf obj INDEX -l P/B/A/N`

`csm ucf obj INDEX uac`

`csm ucf obj INDEX wf`

Syntax Description

Parameter	Description
<i>show</i>	It means to display all of the profiles.
<i>setdefault</i>	It means to return to default settings for all of the profile.
<i>msg MSG</i>	It means de set the administration message. MSG means the content (less than 255 characters) of the message itself.
<i>obj</i>	It means to specify the object for the profile.
<i>INDEX</i>	It means to specify the index number of CSM profile, from 1 to 8.
<i>-n</i>	It means to set the profile name.
<i>PROFILE_NAME</i>	It means to specify the name of the profile (less than 16 characters)
<i>-p</i>	Set the priority (defined by the number specified in VALUE) for the profile.
<i>VALUE</i>	Number 0 to 3 represent different conditions. 0: It means Bundle: Pass. 1: It means Bundle: Block. 2: It means Either: URL Access Control First. 3: It means Either: Web Feature First.
<i>-l</i>	It means the log type of the profile. They are: P: Pass, B: Block, A: All, N: None
<i>MSG</i>	It means to specify the Administration Message, less then 255 characters
<i>uac</i>	It means to set URL Access Control part.
<i>wf</i>	It means to set Web Feature part.

Example

```
> csm ucf obj 1 -n game -l B
```

```

Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
Action:[pass]
[ ]Prevent web access from IP address.
No  Obj NO.   Object Name
-----
No  Grp NO.   Group Name
-----

```

Telnet Command: csm ucf obj INDEX uac

It means to configure the settings regarding to URL Access Control (uac).

Syntax

```

csm ucf obj INDEX uac -v
csm ucf obj INDEX uac -e
csm ucf obj INDEX uac -d
csm ucf obj INDEX uac -a P/B
csm ucf obj INDEX uac -i E/D
csm ucf obj INDEX uac -o KEY_WORD_Object_Index
csm ucf obj INDEX uac -g KEY_WORD_Group_Index

```

Syntax Description

Parameter	Description
<i>INDEX</i>	It means to specify the index number of CSM profile, from 1 to 8.
-v	It means to view the protocol configuration of the CSM profile.
-e	It means to enable the function of URL Access Control.
-d	It means to disable the function of URL Access Control.
-a	Set the action of specific application, P or B. B: Block. The web access meets the URL Access Control will be blocked. P: Pass. The web access meets the URL Access Control will be passed.
-i	Prevent the web access from any IP address. E: Enable the function. The Internet access from any IP address will be blocked. D: Disable the function.
-o	Set the keyword object.
<i>KEY_WORD_Object_Index</i>	Specify the index number of the object profile.
-g	Set the keyword group.
<i>KEY_WORD_Group_Index</i>	Specify the index number of the group profile.

Example

```
> csm ucf obj 1 uac -i E
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
Action:[pass]
[v]Prevent web access from IP address.
  No  Obj NO.   Object Name
  ---
  No  Grp NO.   Group Name
  ---

> csm ucf obj 1 uac -a B
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
Action:[block]
[v]Prevent web access from IP address.
  No  Obj NO.   Object Name
  ---
  No  Grp NO.   Group Name
  ---
```

Telnet Command: csm ucf obj INDEX wf

It means to configure the settings regarding to Web Feature (wf).

Syntax

csm ucf obj *INDEX wf -v*

csm ucf obj *INDEX wf -e*

csm ucf obj *INDEX wf -d*

csm ucf obj *INDEX wf -a P/B*

csm ucf obj *INDEX wf -s WEB_FEATURE*

csm ucf obj *INDEX wf -u WEB_FEATURE*

csm ucf obj *INDEX wf -f File_Extension_Object_index*

Syntax Description

Parameter	Description
<i>INDEX</i>	It means to specify the index number of CSM profile, from 1 to 8.
<i>-v</i>	It means to view the protocol configuration of the CSM profile.
<i>-e</i>	It means to enable the restriction of web feature.
<i>-d</i>	It means to disable the restriction of web feature.
<i>-a</i>	Set the action of web feature, P or B. B: Block. The web access meets the web feature will be blocked. P: Pass. The web access meets the web feature will be passed.
<i>-s</i>	It means to enable the the Web Feature configuration. Features available for configuration are: c: Cookie p: Proxy u: Upload
<i>-u</i>	It means to cancel the web feature configuration.
<i>-f</i>	It means to set the file extension object index number.
<i>File_Extension_Object_index</i>	Type the index number (1 to 8) for the file extension object.

Example

```
> csm ucf obj 1 wf -s c
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
Action:[block]
[v] Prevent web access from IP address.
No Obj NO.    Object Name
-----

No Grp NO.    Group Name
-----
```

```
[ ] Enable Restrict Web Feature
Action:[pass]
File Extension Object Index : [0]      Profile Name : []
[V] Cookie [ ] Proxy [ ] Upload
```

Telnet Command: ddns log

Displays the DDNS log.

Example

```
>ddns log
>
```

Telnet Command: ddns time

Sets and displays the DDNS time.

Syntax

ddns time <update in minutes>

Syntax Description

Parameter	Description
<i>Update in minutes</i>	Type the value as DDNS time. The range is from 1 to 14400.

Example

```
> ddns time
ddns time <update in minutes>
Valid: 1 ~ 1440
%Now: 1440
> ddns time 1000
ddns time <update in minutes>
Valid: 1 ~ 1440
%Now: 1000
```

Telnet Command: dos

This command allows users to configure the settings for DoS defense system.

Syntax

dos [-V | D | A]

dos [-s ATTACK_F [THRESHOLD][TIMEOUT]]

dos [-a | e [ATTACK_F][ATTACK_0] | d [ATTACK_F][ATTACK_0]]

Syntax Description

Parameter	Description
-V	It means to view the configuration of DoS defense system.
-D	It means to deactivate the DoS defense system.
-A	It means to activate the DoS defense system.
-s	It means to enable the defense function for a specific attack and set

	its parameter(s).
<i>ATTACK_F</i>	It means to specify the name of flooding attack(s) or portscan, e.g., synflood, udpflood, icmpflood, or postscan.
<i>THRESHOLD</i>	It means the packet rate (packet/second) that a flooding attack will be detected. Set a value larger than 20.
<i>TIMEOUT</i>	It means the time (seconds) that a flooding attack will be blocked. Set a value larger than 5.
<i>-a</i>	It means to enable the defense function for all attacks listed in <i>ATTACK_0</i> .
<i>-e</i>	It means to enable defense function for a specific attack(s).
<i>ATTACK_0</i>	It means to specify a name of the following attacks: ip_option, tcp_flag, land, teardrop, smurf, pingofdeath, traceroute, icmp_frag, syn_frag, unknow_proto, fraggle.
<i>-d</i>	It means to disable the defense function for a specific attack(s).

Example

```
>dos -A
The Dos Defense system is Activated
>dos -s synflood 50 10
Synflood is enabled! Threshold=50 <pke/sec> timeout=10 <pke/sec>
```

Telnet Command: exit

Type this command will leave telnet window.

Telnet Command: Internet

This command allows you to configure detailed settings for WAN connection.

Syntax

internet *-W n -M n [-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
<i>-M n</i>	M means to set Internet Access Mode (Mandatory) and n means different modes (represented by 0 - 3) n=0: Offline n=1: PPPoE n=2: Dynamic IP n=3: Static IP
<i><command><parameter>[...]</i>	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
<i>-S <isp name></i>	It means to set ISP Name (max. 23 characters).
<i>-P <on/off></i>	It means to enable PPPoE Service.
<i>-u <username></i>	It means to set username (max. 49 characters) for Internet accessing.
<i>-p <password></i>	It means to set password (max. 49 characters) for Internet accessing.

-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.
-V	It means to view Internet Access profile.

Example

```
>internet -M 1 -S tcom -u username -p password -a 0 -t -1 -i 0.0.0.0
WAN1 Internet Mode set to PPPoE/PPPoA
WAN1 ISP Name set to tcom
WAN1 Username set to username
WAN1 Password set successful
WAN1 PPP Authentication Type set to PAP/CHAP
WAN1 Idle timeout set to always-on
WAN1 Gateway IP set to 0.0.0.0
> internet -V
WAN1 Internet Mode:PPPoE
ISP Name: tcom
Username: username
Authentication: PAP/CHAP
Idle Timeout: -1
WAN IP: Dynamic IP
```

Telnet Command: ip 2ndsubnet

This command allows users to enable or disable the IP routing subnet for your router.

Syntax

ip 2ndsubnet <Enable/Disable>

Syntax Description

Parameter	Description
<i>Enable</i>	Enable the function.
<i>Disable</i>	Disable the function.

Example

```
> ip 2ndsubnet enable
2nd subnet enabled!
```

Telnet Command: ip 2ndaddr

This command allows to set the IP routed subnet for the router.

Syntax

ip pubaddr ?

ip pubaddr <2nd subnet IP address>

Syntax Description

Parameter	Description
?	Display an IP address which allows users set as the second subnet IP address.
2nd subnet IP address	Specify an IP address. The system will set the one that you specified as the second subnet IP address.

Example

```
> > ip 2ndaddr ?
% ip addr <2nd subnet IP address>
% Now: 192.168.2.1

> ip 2ndaddr 192.168.2.5
% Set 2nd subnet IP address done !!!
```

Telnet Command: ip 2ndmask

This command allows users to set the mask for IP routed subnet of your router.

Syntax

ip 2ndmask ?

ip 2ndmask <2nd subnet mask>

Syntax Description

Parameter	Description
?	Display an IP address which allows users set as the second subnet mask.
public subnet IP address	Specify a subnet mask. The system will set the one that you specified as the second subnet mask.

Example

```
> ip pubmask ?
% ip pubmask <public subnet mask>
% Now: 255.255.255.0

> ip pubmask 255.255.0.0
% Set public subnet mask done !!!
```

Telnet Command: ip aux

This command is used for configuring WAN IP Alias.

Syntax

```
ip aux add [IP] [Join to NAT Pool][wanX]
```

```
ip aux remove [index][wanX]
```

Syntax Description

Parameter	Description
<i>add</i>	It means to create a new WAN IP address.
<i>remove</i>	It means to delete an existed WAN IP address.
<i>IP</i>	It means the auxiliary WAN IP address.
<i>Join to NAT Pool</i>	0 (disable) or 1 (enable).
<i>wanX</i>	Add or remove an address for WAN interface.
<i>index</i>	Type the index number of the table displayed on your screen.

Example

```
> > ip aux add 192.168.1.65 1
% 192.168.1.65 has added in index 2.

> ip aux ?% ip aux add [IP] [Join to NAT Pool]
> ip aux ?% ip aux add [IP] [Join to NAT Pool] [wanX]
%% ip aux remove [Index] [wanX]

%%      Where IP = Auxiliary WAN IP Address.
%%      Join to NAT Pool = 0 or 1.
%%      Index = The Index number of table.
%%      wanX = add/remove an address for WANX.
```

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

Now auxiliary WAN2 IP Address table:

Index no.	Status	IP address	NAT IP pool
1	Disable	0.0.0.0	Yes

When you type *ip aux?*, the current auxiliary WAN IP Address table will be shown as the following:

Index no.	Status	IP address	IP pool
1	Enable	172.16.3.229	Yes

2	Enable	172.16.3.56	No
3	Enable	172.16.3.113	No

Telnet Command: ip addr

This command allows users to set/add a specified LAN IP your router.

Syntax

ip addr [*IP address*]

Syntax Description

Parameter	Description
<i>IP address</i>	It means the LAN IP address.

Example

```
>ip addr 192.168.50.1
% Set IP address OK !!!
```



Info

When the LAN IP address is changed, the start IP address of DHCP server are still the same. To make the IP assignment of the DHCP server being consistent with this new IP address (they should be in the same network segment), the IP address of the PC must be fixed with the same LAN IP address (network segment) set by this command for accessing into the web user interface of the router. Later, modify the start addresses for the DHCP server.

Telnet Command: ip nmask

This command allows users to set/add a specified netmask for your router.

Syntax

`ip nmask [IP netmask]`

Syntax Description

Parameter	Description
<i>IP netmask</i>	It means the netmask of LAN IP.

Example

```
> ip nmask 255.255.0.0
% Set IP netmask OK !!!
```

Telnet Command: ip arp

ARP displays the matching condition for IP and MAC address.

Syntax

`ip arp add [IP address] [MAC address] [LAN or WAN]`

`ip arp del [IP address] [LAN or WAN]`

`ip arp flush`

`ip arp status`

`ip arp accept [0/1/2/3/4/5status]`

`ip arp setCacheLife [time]`

In which, **arp add** allows users to add a new IP address into the ARP table; **arp del** allows users to remove an IP address; **arp flush** allows users to clear arp cache; **arp status** allows users to review current status for the arp table; **arp accept** allows to accept or reject the source /destination MAC address; **arp setCacheLife** allows users to configure the duration in which ARP caches can be stored on the system. If **ip arp setCacheLife** is set with "60", it means you have an ARP cache at 0 second. Sixty seconds later without any ARP messages received, the system will think such ARP cache is expired. The system will issue a few ARP request to see if this cache is still valid.

Syntax Description

Parameter	Description
<i>IP address</i>	It means the LAN IP address.
<i>MAC address</i>	It means the MAC address of your router.
<i>LAN or WAN</i>	It indicates the direction for the arp function.
<i>0/1/2/3/4/5</i>	0: disable to accept illegal source mac address 1: enable to accept illegal source mac address 2: disable to accept illegal dest mac address 3: enable to accept illegal dest mac address 4: Decline VRRP mac into arp table 5: Accept VRRP mac into arp table status: display the setting status.
<i>Time</i>	Available settings will be 10, 20, 30, ... 2550 seconds.

Example

```
> ip arp accept status
Accept illegal source mac arp: disable

Accept illegal dest mac arp: disable

Accept VRRP mac into arp table: disable
> ip arp status
[ARP Table]
  Index IP Address      MAC Address      Netbios Name
  1    192.168.1.113    00-05-5D-E4-D8-EE  A1000351
```

Telnet Command: ip dhcpc

This command is available for WAN DHCP.

Syntax

`ip dhcpc option`

`ip dhcpc option -h/l`

`ip dhcpc option -d [idx]`

`ip dhcpc option -e [1 or 0] -w [wan unumber] -c [option number] -v [option value]`

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

`ip dhcpc option -u [idx unumber]`

`ip dhcpc release [wan number]`

`ip dhcpc renew [wan number]`

`ip dhcpc status`

Syntax Description

Parameter	Description
<i>option</i>	It is an optional setting for DHCP server. -h: display usage -l: list all custom set DHCP options -d: delete custom dhcp client option by index number -e: enable/disable option feature, 1:enable, 0:disable -w: set WAN number (e.g., 1=WAN1) -c: set option number: 0-255 -v: set option value by string -x: set option value by raw byte (hex) -u: update by index number
<i>release</i>	It means to release current WAN IP address.
<i>renew</i>	It means to renew the WAN IP address and obtain another new one.
<i>status</i>	It displays current status of DHCP client.

Example

```
>ip dhcpc status
I/F#3 DHCP Client Status:
```

```

DHCP Server IP      : 172.16.3.7
WAN Ipm             : 172.16.3.40
WAN Netmask         : 255.255.255.0
WAN Gateway         : 172.16.3.1
Primary DNS         : 168.95.192.1
Secondary DNS       : 0.0.0.0
Leased Time         : 259200
Leased Time T1     : 129600
Leased Time T2     : 226800
Leased Elapsed     : 259194
Leased Elapsed T1  : 129594
Leased Elapsed T2  : 226794

```

Telnet Command: ip ping

This command allows users to ping IP address of WAN1/WAN2/PVC3/PVC4/PVC5 for verifying if the WAN connection is OK or not.

Syntax

`ip ping [IP address] [WAN1/WAN2/PVC3/PVC4/PVC5]`

Syntax Description

Parameter	Description
<i>IP address</i>	It means the WAN IP address.
<i>WAN1/WAN2/PVC3/PVC4/PVC5</i>	It means the WAN port /PVC that the above IP address passes through.

Example

```

>ip ping 172.16.3.229 WAN1
Pinging 172.16.3.229 with 64 bytes of Data:
Receive reply from 172.16.3.229, time=0ms
Receive reply from 172.16.3.229, time=0ms
Receive reply from 172.16.3.229, time=0ms
Packets: Sent = 5, Received = 5, Lost = 0 <0% loss>

```

Telnet Command: ip tracert

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

Syntax

`ip tracert [Host/IP address] [WAN1/WAN2] [Udp/Icmp]`

Syntax Description

Parameter	Description
<i>IP address</i>	It means the target IP address.
<i>WAN1/WAN2</i>	It means the WAN port that the above IP address passes through.
<i>Udp/Icmp</i>	It means the UDP or ICMP.

Example

```
>ip tracert 22.128.2.62 WAN1
Traceroute to 22.128.2.62, 30 hops max
 1  172.16.3.7  10ms
 2  172.16.1.2  10ms
 3  Request Time out.
 4  168.95.90.66  50ms
 5  211.22.38.134  50ms
 6  220.128.2.62  50ms
Trace complete
```

Telnet Command: ip telnet

This command allows users to access specified device by telnet.

Syntax

`ip telnet [IP address][Port]`

Syntax Description

Parameter	Description
<i>IP address</i>	Type the WAN or LAN IP address of the remote device.
<i>Port</i>	Type a port number (e.g., 23). Available settings: 0 ~65535.

Example

```
> ip telnet 172.17.3.252 23
>
```

Telnet Command: ip rip

This command allows users to set the RIP (routing information protocol) of IP.

Syntax

`ip rip [0/1/2]`

Syntax Description

Parameter	Description
<i>0/1/2</i>	0 means disable; 1 means first subnet and 2 means second subnet.

Example

```
> ip rip 1
%% Set RIP 1st subnet.
```


Telnet Command: ip wanrip

This command allows users to set the RIP (routing information protocol) of WAN IP.

Syntax

```
ip wanrip [ifno] -e [0/1]
```

Syntax Description

Parameter	Description
<i>ifno</i>	It means the connection interface. 1: WAN1,2: WAN2, 3: PVC3,4: PVC4,5: PVC5 Note: PVC3 -PVC5 are virtual WANs.
-e	It means to disable or enable RIP setting for specified WAN interface. 1: Enable the function of setting RIP of WAN IP. 0: Disable the function.

Example

```
> ip wanrip ?
Valid ex:ip wanrip <ifno> -e <0/1>
<ifno> 1: WAN1,2: WAN2
       3: PVC3,4: PVC4,5: PVC5
-e <0/1> 0: disable, 1: enable
Now status:
WAN[1] Rip Protocol disable
WAN[2] Rip Protocol disable
WAN[3] Rip Protocol disable
WAN[4] Rip Protocol disable
WAN[5] Rip Protocol disable
> ip wanrip 5 -e 1
> ip wanrip ?
Valid ex:ip wanrip <ifno> -e <0/1>
<ifno> 1: WAN1,2: WAN2
       3: PVC3,4: PVC4,5: PVC5
-e <0/1> 0: disable, 1: enable
Now status:
WAN[1] Rip Protocol disable
WAN[2] Rip Protocol disable
WAN[3] Rip Protocol disable
WAN[4] Rip Protocol disable
WAN[5] Rip Protocol enable
```

Telnet Command: ip route

This command allows users to set static route.

Syntax

```
ip route add [dst] [netmask][gateway][ifno][rtype]
```

```
ip route del [dst] [netmask][rtype]
```

```
ip route status
```

```
ip route cnc
```

```
ip route default [wan1/wan2/off/?]
```

```
ip route clean [1/0]
```

Syntax Description

Parameter	Description
<i>add</i>	It means to add an IP address as static route.
<i>del</i>	It means to delete specified IP address.
<i>status</i>	It means current status of static route.
<i>dst</i>	It means the IP address of the destination.
<i>netmask</i>	It means the netmask of the specified IP address.
<i>gateway</i>	It means the gateway of the connected router.
<i>ifno</i>	It means the connection interface. 3=WAN1 5=WAN3,6=WAN4,7=WAN5 However, WAN3, WAN4, WAN5 are router-borne WANs
<i>rtype</i>	It means the type of the route. default : default route; static: static route.
<i>cnc</i>	It means current IP range for CNC Network.
<i>default</i>	Set WAN1/WAN2/off as current default route.
<i>clean</i>	Clean all of the route settings. 1: Enable the function. 0: Disable the function.

Example

```
> ip route add 172.16.2.0 255.255.255.0 172.16.2.4 3 static
> ip route status

Codes: C - connected, S - static, R - RIP, * - default, ~ - private
C~      192.168.1.0/ 255.255.255.0 is directly connected, LAN1
S       172.16.2.0/ 255.255.255.0 via 172.16.2.4, WAN1
```

Telnet Command: ip igmp_proxy

This command allows users to enable/disable igmp proxy server.

Syntax

`ip igmp_proxy set`

`ip igmp_proxy reset`

`ip igmp_proxy wan`

`ip igmp_proxy t_home[on/off/show/help]`

`ip igmp_proxy query`

`ip igmp_proxy ppp [0/1]`

`ip igmp_proxy status`

Syntax Description

Parameter	Description
<code>set</code>	It means to enable proxy server.
<code>reset</code>	It means to disable proxy server.
<code>wan</code>	It means to specify WAN interface for IGMP service.
<code>t_home</code>	It means to specify t_home proxy server for using.
<code>On/off/show/help</code>	It means to turn on/off/display or get more information of the T_home service.
<code>query</code>	It means to set IGMP general query interval. The default value is 125000 ms.
<code>ppp</code>	0 - No need to set IGMP with PPP header. 1 - Set IGMP with PPP header.
<code>status</code>	It means to display current status for proxy server.

Example

```
> ip igmp t_home on
%T-Home Setting:
%T-Home Service is turned on.
%WAN1 : Enabled, connection type: PPPoE, without tag for ADSL
%WAN5 : Enabled, connection type: DHCP, tag: 8
%: PVC4(WAN5) is bound to PVC0(WAN1), protocol=MPoA 1483 Bridge
%IGMP Proxy Interface: WAN5(PVC)
%WAN5 for Router-borne Application/ IPTV on/off: ON
> ip igmp_proxy query 130000
This command is for setting IGMP General Query Interval
The default value is 125000 ms
Current Setting is:130000 ms
>
```

Telnet Command: ip dmz

Specify MAC address of certain device as the DMZ host.

Syntax

`ip dmz [mac]`

Syntax Description

Parameter	Description
<i>mac</i>	It means the MAC address of the device that you want to specify

Example

```
>ip dmz ?
% ip dmz <mac>, now : 00-00-00-00-00-00
> ip dmz 11-22-33-44-55-66
> ip dmz ?
% ip dmz <mac>, now : 11-22-33-44-55-66
>
```

Telnet Command: ip session

This command allows users to set maximum session limit number for the specified IP; set message for exceeding session limit and set how many seconds the IP session block works.

Syntax

`ip session on`

`ip session off`

`ip session default [num]`

`ip session defaultp2p [num]`

`ip session status`

`ip session show`

`ip session timer [num]`

`ip session [block/unblock][IP]`

`ip session [add/del][IP1-IP2][num][p2pnum]`

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on session limit for each IP.
<i>off</i>	It means to turn off session limit for each IP.
<i>default [num]</i>	It means to set the default number of session num limit.
<i>Defaultp2p [num]</i>	It means to set the default number of session num limit for p2p.
<i>status</i>	It means to display the current settings.
<i>show</i>	It means to display all session limit settings in the IP range.
<i>timer [num]</i>	It means to set when the IP session block works. The unit is second.

<i>[block/unblock][IP]</i>	It means to block/unblock the specified IP address. Block: The IP cannot access Internet through the router. Unblock: The specified IP can access Internet through the router.
<i>add</i>	It means to add the session limits in an IP range.
<i>del</i>	It means to delete the session limits in an IP range.
<i>IP1-IP2</i>	It means the range of IP address specified for this command.
<i>num</i>	It means the number of the session limits, e.g., 100.
<i>p2pnum</i>	It means the number of the session limits, e.g., 50 for P2P.

Example

```
>ip session default 100
> ip session add 192.168.1.5-192.168.1.100 100 50
> ip session on
> ip session status

IP range:
  192.168.1.5 - 192.168.1.100 : 100

Current ip session limit is turn on

Current default session number is 100
```

Telnet Command: ip bandwidth

This command allows users to set maximum bandwidth limit number for the specified IP.

Syntax

ip bandwidth on

ip bandwidth off

ip bandwidth default [tx_rate][rx_rate]

ip bandwidth status

ip bandwidth show

ip bandwidth [add/del] [IP1-IP2][tx][rx][shared]

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on the IP bandwidth limit.
<i>off</i>	It means to turn off the IP bandwidth limit.
<i>default [tx_rate][rx_rate]</i>	It means to set default tx and rx rate of bandwidth limit. The range is from 0 - 65535 Kpbs.
<i>status</i>	It means to display the current settings.
<i>show</i>	It means to display all the bandwidth limits settings within the IP range.
<i>add</i>	It means to add the bandwidth within the IP range.
<i>del</i>	It means to delete the bandwidth within the IP range.
<i>IP1-IP2</i>	It means the range of IP address specified for this command.

<i>tx</i>	It means to set transmission rate for bandwidth limit.
<i>rx</i>	It means to set receiving rate for bandwidth limit.
<i>shared</i>	It means that the bandwidth will be shared for the IP range.

Example

```

> ip bandwidth default 200 800
> ip bandwidth add 192.168.1.50-192.168.1.100 10 60
> ip bandwidth status

IP range:
  192.168.1.50 - 192.168.1.100 : Tx:10K Rx:60K

Current ip Bandwidth limit is turn off

Auto adjustment is off

```

Telnet Command: ip bindmac

This command allows users to set IP-MAC binding for LAN host.

Syntax

`ip bindmac on`

`ip bindmac off`

`ip bindmac strict_on`

`ip bindmac show`

`ip bindmac add [IP][MAC][Comment]`

`ip bindmac del [IP]/all`

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on IP bindmac policy. Even the IP is not in the policy table, it can still access into network.
<i>off</i>	It means to turn off all the bindmac policy.
<i>strict_on</i>	It means that only those IP address in IP bindmac policy table can access into network.
<i>show</i>	It means to display the IP address and MAC address of the pair of binded one.
<i>add</i>	It means to add one ip bindmac.
<i>del</i>	It means to delete one ip bindmac.
<i>IP</i>	It means to type the IP address for binding with specified MAC address.
<i>MAC</i>	It means to type the MAC address for binding with the IP address specified.
<i>Comment</i>	It means to type words as a brief description.
<i>All</i>	It means to delete all the IP bindmac settings.

Example

```
> ip bindmac add 192.168.1.46 00:50:7f:22:33:55 just for test
> ip bindmac show
ip bind mac function is turned ON
IP : 192.168.1.46 bind MAC : 00-50-7f-22-33-55 Comment : just
```

Telnet Command: ip maxnatuser

This command is used to set the maximum number of NAT users.

Syntax

`ip maxnatuser user no`

Syntax Description

Parameter	Description
<i>User no</i>	A number specified here means the total NAT users that Vigor device supports. 0 - It means no limitation.

Example

```
> ip maxnatuser 100
% Max NAT user = 100
```

Telnet Command: ip6 addr

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

Syntax

`ip6 addr -s [prefix] [prefix-length] [LAN|WAN1|WAN2|iface#]`

`ip6 addr -d [prefix] [prefix-length] [LAN|WAN1|WAN2|iface#]`

`ip6 addr -a [LAN|WAN1|WAN2|iface#]`

Syntax Description

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

Example

```
> ip6 addr -a
LAN
Unicast Address:
FE80::250:7FFF:FE00:0/64 (Link)
Multicast Address:
FF02::2
FF02::1:FF00:0
FF02::1
```


Telnet Command: ip6 dhcp req_opt

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

Syntax

`ip6 dhcp req_opt [LAN/WAN1/WAN2/iface#] [-<command> <parameter>| ...]`

Syntax Description

Parameter	Description
<i>req_opt</i>	It means option-request.
<i>LAN/WAN1/WAN2/iface#</i>	It means to specify LAN or WAN interface for such address.
<i>[<command> <parameter> ...]</i>	The available commands with parameters are listed below. <i>[...]</i> means that you can type in several commands in one line.
<i>-a</i>	It means to show current DHCPv6 status.
<i>-s</i>	It means to ask the SIP.
<i>-S</i>	It means to ask the SIP name.
<i>-d</i>	It means to ask the DNS setting.
<i>-D</i>	It means to ask the DNS name.
<i>-n</i>	It means to ask NTP.
<i>-i</i>	It means to ask NIS.
<i>-I</i>	It means to ask NIS name.
<i>-p</i>	It means to ask NISP.
<i>-P</i>	It means to ask NISP name.
<i>-b</i>	It means to ask BCMCS.
<i>-B</i>	It means to ask BCMCS name.
<i>-r</i>	It means to ask refresh time.
<i>Parameter</i>	1: the parameter related to the request will be displayed. 0: the parameter related to the request will not be displayed.

Example

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

Telnet Command: ip6 dhcp client

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

Syntax

`ip6 dhcp client [WAN1/WAN2/iface#] [-<command> <parameter>| ...]`

Syntax Description

Parameter	Description
<i>client</i>	It means the dhcp client settings.

<i>[<command> <parameter> ...]</i>	The available commands with parameters are listed below. <i>[...]</i> means that you can type in several commands in one line.
<i>-a</i>	It means to show current DHCPv6 status.
<i>-p [IAID]</i>	It means to request identity association ID for Prefix Delegation.
<i>-n [IAID]</i>	It means to request identity association ID for Non-temporary Address.
<i>-c [parameter]</i>	It means to send rapid commit to server.
<i>-i [parameter]</i>	It means to send information request to server.
<i>-e[parameter]</i>	It means to enable or disable the DHCPv6 client. 1: Enable 0: Disable

Example

```

> ip6 dhcp client WAN2 -p 2008::1
> ip6 dhcp client WAN2 -a
  Interface WAN2 has following DHCPv6 client settings:
    DHCPv6 client enabled
    request IA_PD whose IAID equals to 2008
> ip6 dhcp client WAN2 -n 1023456
> ip6 dhcp client WAN2 -a
  Interface WAN2 has following DHCPv6 client settings:
    DHCPv6 client enabled
    request IA_NA whose IAID equals to 2008
> system reboot

```

Telnet Command: ip6 dhcp server

This command allows you to configure DHCPv6 server.

Syntax

`ip6 dhcp server [-<command> <parameter>| ...]`

Syntax Description

Parameter	Description
<i>server</i>	It means the dhcp server settings.
<i>[<command> <parameter> ...]</i>	The available commands with parameters are listed below. <i>[...]</i> means that you can type in several commands in one line.
<i>-a</i>	It means to show current DHCPv6 status.
<i>-i<pool_min_addr></i>	It means to set the start IPv6 address of the address pool.
<i>-x<pool_max_addr></i>	It means to set the end IPv6 address of the address pool.
<i>-d<addr></i>	It means to set the first DNS IPv6 address.
<i>-D<addr></i>	It means to set the second DNS IPv6 address.
<i>-c<parameter></i>	It means to send rapid commit to server. 1: Enable 0: Disable
<i>-e<parameter></i>	It means to enable or disable the DHCPv6 server. 1: Enable 0: Disable

Example

```
> ip6 dhcp server -d FF02::1
> ip6 dhcp server -i ff02::1
> ip6 dhcp server -x ff02::3
> ip6 dhcp server -a
% Interface LAN has following DHCPv6 server settings:
%   DHCPv6 server disabled
%   maximum address of the pool: FF02::3
%   minimum address of the pool: FF02::1
%   1st DNS IPv6 Addr: FF02::1
```

Telnet Command: ip6 internet

This command allows you to configure settings for accessing Internet.

Syntax

```
ip6 internet -W n -M n [-<command> <parameter> | ... ]
```

Syntax Description

Parameter	Description
-W n	W means to set WAN interface and n means different selections. Default is WAN1. n=1: WAN1 n=2: WAN2 n=3: WAN3 . . n=X: WANx
-M n	M means to set Internet Access Mode (Mandatory) and n means different modes (represented by 0 - 5) n= 0: Offline, n=1: PPP, n=2: TSPC, n=3: AICCU, n=4: DHCPv6, n=5: Static n=6:6in4-Static n=7:6rd
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-m n	It means to set IPv6 MTU. N = any value (0 means "unspecified").
-u <username>	It means to set Username. <username>= type a name as the username (maximum 63 characters).
-p <password>	It means to set Password. <password> = type a password (maximum 63 characters).
-s <server>	It means to set Tunnel Server IP.

	<server>= IPv4 address or URL (maximum 63 characters).
-d <server>	It means to set the primary DNS Server IP. <server>= type an IPv6 address for first DNS server.
-D <server>	It means to set the secondary DNS Server IP. <server>= type an IPv6 address for second DNS server.
-t <dhcp/ra/none>	It means to set IPv6 PPP WAN test mode for DHCP or RADVD. <dhcp/ra/none>= type IPv6 address.
-V	It means to view IPv6 Internet Access Profile.
-o	It means to set AICCU always on. 1=On, 0=Off

Example

```
> ip6 internet -W 2 -M 2 -u 88886666 -p draytek123456 -s
amsterdam.freenet6.net
  This setting will take effect after rebooting.
  Please use "sys reboot" command to reboot the router.
> system reboot
```

Telnet Command: ip6 neigh

This command allows you to display IPv6 neighbour table.

Syntax

```
ip6 neigh -s[ inet6_addr] [eth_addr] [LAN/WAN1/WAN2]
```

```
ip6 neigh -d [inet6_addr] [LAN/WAN1/WAN2]
```

```
ip6 neigh -a [inet6_addr] [-N LAN/WAN1/WAN2]
```

Syntax Description

Parameter	Description
-s	It means to add a neighbour.
-d	It means to delete a neighbour.
-a	It means to show neighbour status.
inet6_addr	Type an IPv6 address
eth_addr	Type submask address.
LAN/WAN1/WAN2	Specify an interface for the neighbor.

Example

```
> ip6 neigh -s 2001:2222:3333::1111 00:50:7F:11:ac:22:WAN2
  Neighbour 2001:2222:3333::1111 successfully added!
> ip6 neigh -a
```

I/F	ADDR	MAC	STATE
LAN	FF02::1	33-33-00-00-00-01	CONNECTED
WAN2	2001:5C0:1400:B::10B8	00-00-00-00-00-00	CONNECTED
WAN2	2001:2222:3333::1111	00-00-00-00-00-00	CONNECTED
WAN2	2001:2222:6666::1111	00-00-00-00-00-00	CONNECTED

WAN2 ::	00-00-00-00-00-00	CONNECTED
LAN ::		NONE
>		

Telnet Command: ip6 neigh

This command allows you to add a proxy neighbour.

Syntax

```
ip6 neigh -s inet6_addr [LAN/WAN1/WAN2]
```

```
ip6 neigh -d inet6_addr [LAN/WAN1/WAN2]
```

```
ip6 neigh -a [inet6_addr] [-N LAN/WAN1/WAN2]
```

Syntax Description

Parameter	Description
-s	It means to add a proxy neighbour.
-d	It means to delete a proxy neighbour.
-a	It means to show proxy neighbour status.
inet6_addr	Type an IPv6 address
LAN/WAN1/WAN2	Specify an interface for the proxy neighbor.

Example

```
> ip6 neigh -s FE80::250:7FFF:FE12:300 LAN
%      Neighbour FE80::250:7FFF:FE12:300 successfully added!
```

Telnet Command: ip6 route

This command allows you to

Syntax

```
ip6 route -s [prefix] [prefix-length] [gateway] [LAN/WAN1/WAN2/iface#] [-D]
```

```
ip6 route -d [prefix] [prefix-length]
```

```
ip6 route -a [LAN/WAN1/WAN2/iface#]
```

Syntax Description

Parameter	Description
-s	It means to add a route.
-d	It means to delete a route.
-a	It means to show the route status.
-D	It means that such route will be treated as the default route.
prefix	It means to type the prefix number of IPv6 address.
prefix-length	It means to type a fixed value as the length of the prefix.
gateway	It means the gateway of the router.
LAN/WAN1/WAN2/iface#	It means to specify LAN or WAN interface for such address.

Example

```
> ip6 route -s FE80::250:7FFF:FE12:500 16 FE80::250:7FFF:FE12:100 LAN
%      Route FE80::250:7FFF:FE12:500/16 successfully added!
> ip6 route -a LAN
```

PREFIX/PREFIX-LEN	_EXPIRES_	_NEXT-HOP_	I/F	METRIC	STATE	FLAGS
FE80::/128	0	::	LAN	0	UNICAST	U
FE80::250:7FFF:FE00:0/128	0	::	LAN	0	UNICAST	U
FE80::/64	0		LAN	256	UNICAST	U
FE80::/16	0	FE80::250:7FFF:FE12:100	LAN	1024	UNICAST	UGA
FF02::1/128	0	FF02::1	LAN	0	UNICAST	UC
FF00::/8	0		LAN	256	UNICAST	U
::/0	0		LAN	-1	UNREACHABLE	!

Telnet Command: ip6 ping

This command allows you to ping an IPv6 address or a host.

Syntax

`ip6 ping [IPv6 address/Host] [LAN/WAN1/WAN2]`

Syntax Description

Parameter	Description
<i>IPv6 address/Host</i>	It means to specify the IPv6 address or host for ping.
<i>LAN/WAN1/WAN2</i>	It means to specify LAN or WAN interface for such address.

Example

```
> ip6 ping 2001:4860:4860::8888 WAN2

Pinging 2001:4860:4860::8888 with 64 bytes of Data:

Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms

Packets: Sent = 5, Received = 5, Lost = 0 <% loss>
>
```

Telnet Command: ip6 tracert

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

Syntax

`ip6 tracert [IPv6 address/Host][LAN//WAN1/WAN2]`

Syntax Description

Parameter	Description
<i>IPv6 address/Host</i>	It means to specify the IPv6 address or host for ping.

Example

```
> ip6 tracert 2001:4860:4860::8888
traceroute to 2001:4860:4860::8888, 30 hops max through protocol ICMP
 1 2001:5C0:1400:B::10B8      340 ms
 2 2001:4DE0:1000:A22::1     330 ms
 3 2001:4DE0:A::1           330 ms
 4 2001:4DE0:1000:34::1     340 ms
 5 2001:7F8:1: :A501:5169:1 330 ms
 6 2001:4860::1:0:4B3       350 ms
 7 2001:4860::8:0:2DAF     330 ms
 8 2001:4860::2:0:66E     340 ms
 9 Request timed out.      *
10 2001:4860:4860::8888   350 ms
Trace complete.
>
```

Telnet Command: ip6 tspan

This command allows you to display TSPC status.

Syntax

`ip6 tspan [ifno]`

Syntax Description

Parameter	Description
<i>ifno</i>	It means the connection interface. Ifno=1 (means WAN1) Info=2 (means WAN2)

Example

```
> ip6 tspan 2
Local Endpoint v4 Address : 111.243.177.223
Local Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b9
Router DNS name : 88866666.broker.freenet6.net
Remote Endpoint v4 Address :81.171.72.11
Remote Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b8
Tspan Prefixlen : 56
Tunnel Broker: Amsterdam.freenet.net
```



```
Status: Connected
>
```

Telnet Command: ip6 radvd

This command allows you to enable or disable RADVD server.

Syntax

`ip6 radvd -s [1|0] [lifetime]`

`ip6 radvd -V`

Syntax Description

Parameter	Description
<code>-s</code>	It means to enable or disable the default lifetime of the RADVD server. 1: Enable the RADVD server. 0: Disable the RADVD server.
<code>Lifetime</code>	It means to set the lifetime. The lifetime associated with the default router in units of seconds. It's used to control the lifetime of the prefix. The maximum value corresponds to 18.2 hours. A lifetime of 0 indicates that the router is not a default router and should not appear on the default router list. Type the number (unit: second) you want.
<code>-V</code>	It means to show the RADVD configuration.
<code>-r</code>	It means RA default test.
<code>-r [num]</code>	It means RA test for item [num].

Example

```
> ip6 radvd -s 1 1800
> ip6 radvd -V
% IPv6 Radvd Config:
Radvd : Enable, Default Lifetime : 1800 seconds
```

Telnet Command: ip6 mngt

This command allows you to manage the settings for access list.

Syntax

`ip6 mngt list`

`ip6 mngt list [add<index> <prefix> <prefix-length>|remove <index>|flush]`

`ip6 mngt status`

`ip6 mngt [http|telnet|ping|https|ssh] [on|off]`

Syntax Description

Parameter	Description
<code>list</code>	It means to show the setting information of the access list.
<code>status</code>	It means to show the status of IPv6 management.
<code>add</code>	It means to add an IPv6 address which can be used to execute

	management through Internet.
<i>index</i>	It means the number (1, 2 and 3) allowed to be configured for IPv6 management.
<i>prefix</i>	It means to type the IPv6 address which will be used for accessing Internet.
<i>prefix-length</i>	It means to type a fixed value as the length of the prefix.
<i>remove</i>	It means to remove (delete) the specified index number with IPv6 settings.
<i>flush</i>	It means to clear the IPv6 access table.
<i>http/telnet/ping/https/ssh</i>	These protocols are used for accessing Internet.
<i>on/off</i>	It means to enable (on) or disable (off) the Internet accessing through http/telnet/ping.

Example

```

> ip6 mngt list add 1 FE80::250:7FFF:FE12:1010 128
> ip6 mngt list add 2 FE80::250:7FFF:FE12:1020 128
> ip6 mngt list add 3 FE80::250:7FFF:FE12:2080 128
> ip6 mngt list
% IPv6 Access List :
Index  IPv6 Prefix      Prefix Length
=====
1      FE80::250:7FFF:FE12:1010      128
2      FE80::250:7FFF:FE12:1020      128
3      FE80::250:7FFF:FE12:2080      128

> ip6 mngt status
% IPv6 Remote Management :
telnet : off,  http : off,    ping : off

```

Telnet Command: ip6 online

This command allows you to check the online status of IPv6 LAN /WAN.

Syntax

ip6 online [ifno]

Syntax Description

Parameter	Description
<i>ifno</i>	It means the connection interface. 0=LAN1 1=WAN1 2=WAN2

Example

```

> ip6 online 0
% LAN 1 online status :
% Interface : UP
% IPv6 DNS Server: :: Static
% IPv6 DNS Server: :: Static
% IPv6 DNS Server: :: Static

```

```

% Tx packets = 408, Tx bytes = 32160, Rx packets = 428, Rx bytes = 33636

> ip6 online 1
% WAN 1 online status :
% IPv6 WAN1 Disabled
% Default Gateway : ::
% UpTime : 0:00:00
% Interface : DOWN
% IPv6 DNS Server: :: Static
% IPv6 DNS Server: :: Static
% IPv6 DNS Server: :: Static
% Tx packets = 0, Tx bytes = 0, Rx packets = 0, Rx bytes = 0

```

Telnet Command: ip6 aiccu

This command allows you to set IPv6 settings for WAN interface with connection type of AICCU.

Syntax

`ip6 aiccu [ifno]`

`ip6 aiccu subnet [add <ifno> <prefix> <prefix-length>|remove <ifno>|show <info>]`

Syntax Description

Parameter	Description
<i>ifno</i>	It means the connection interface. 1=WAN1 2=WAN2
<i>add</i>	It means to add an IPv6 address which can be used to execute management through Internet.
<i>prefix</i>	It means to type the IPv6 address which will be used for accessing Internet.
<i>prefix-length</i>	It means to type a fixed value as the length of the prefix.
<i>remove</i>	It means to remove (delete) the specified index number with IPv6 settings.
<i>show</i>	It means to display the AICCU status.

Example

```

> ip6 aiccu subnet add 2 2001:1111:0000::1111 64
> ip6 aiccu 2
Status: Connecting

>ip6 aiccu subnet show 2
IPv6 WAN2 AICCU Subnet Prefix Config:
2001:1111::1111/64
>

```

Telnet Command: ip6 ntp

This command allows you to set IPv6 settings for NTP (Network Time Protocols) server.

Syntax

```
ip6 ntp -h
ip6 ntp -v
ip6 ntp -p [0/1]
```

Syntax Description

Parameter	Description
-h	It is used to display the usage of such command.
-v	It is used to show the NTP state.
-p <0/1>	It is used to specify NTP server for IPv6. 0 - Auto 1 - First Query IPv6 NTP Server.

Example

```
> ip6 ntp -p 1
% Set NTP Priority: IPv6 First
```

Telnet Command: ipf view

IPF users to view the version of the IP filter, to view/set the log flag, to view the running IP filter rules.

Syntax

```
ipf view [-VcdhrtzZ]
```

Syntax Description

Parameter	Description
-V	It means to show the version of this IP filter.
-c	It means to show the running call filter rules.
-d	It means to show the running data filter rules.
-h	It means to show the hit-number of the filter rules.
-r	It means to show the running call and data filter rules.
-t	It means to display all the information at one time.
-z	It means to clear a filter rule's statistics.
-Z	It means to clear IP filter's gross statistics.

Example

```
> ipf view -V -c -d
ipf: IP Filter: v3.3.1 (1824)
Kernel: IP Filter: v3.3.1
Running: yes
Log Flags: 0x80947278 = nonip
Default: pass all, Logging: available
```

Telnet Command: ipf set

This command is used to set general rule for firewall.

Syntax

`ipf set [Options]`

`ipf set [SET_NO] rule [RULE_NO] [Options]`

Syntax Description

Parameter	Description
<i>Options</i>	There are several options provided here, such as <code>-v</code> , <code>-c [SET_NO]</code> , <code>-d [SET_NO]</code> ,... and etc.
<i>SET_NO</i>	It means to specify the index number (from 1 to 12) of filter set.
<i>RULE_NO</i>	It means to specify the index number (from 1 to 7) of filter rule set.
<code>-v</code>	Type <code>"-v"</code> to view the configuration of general set.
<code>-c [SET_NO]</code>	It means to setup Call Filter, e.g., <code>-c 2</code> . The range for the index number you can type is <code>"0"</code> to <code>"12"</code> (0 means "disable").
<code>-d [SET_NO]</code>	It means to setup Data Filter, e.g., <code>-d 3</code> . The range for the index number you can type is <code>"0"</code> to <code>"12"</code> (0 means "disable").
<code>-l [VALUE]</code>	It means to setup Log Flag, e.g., <code>-l 2</code> Type <code>"0"</code> to disable the log flag. Type <code>"1"</code> to display the log of passed packet. Type <code>"2"</code> to display the log of blocked packet. Type <code>"3"</code> to display the log of non-matching packet.
<code>-p [VALUE]</code>	It means to setup actions for packet not matching any rule, e.g., <code>-p 1</code> Type <code>"0"</code> to let all the packets pass; Type <code>"1"</code> to block all the packets.
<code>-R <v4/v6> <Enable/Disable></code>	Accept routing packet from WAN. i.e: <code>-R "v4 0"</code> : Set Accept routing packet from WAN by IPv4 is enable i.e: <code>-R "v4 1"</code> : Set Accept routing packet from WAN by IPv6 is disable i.e: <code>-R "v6 0"</code> : Set Accept routing packet from WAN by IPv4 is enable i.e: <code>-R "v6 1"</code> : Set Accept routing packet from WAN by IPv6 is disable
<code>-L [VALUE]</code>	Enable/Disable Strict Security Firewall. VALUE : 0:Disable, 1:Enable.
<code>-C [VALUE]</code>	Setup code page. VALUE : code page number ("?" for more information).
<code>-U [URL_NO]</code>	It means to configure URL content filter for the packets not matching with any rule, e.g., <code>-U 1</code> Type <code>"0"</code> to let all the packets pass; Type <code>"1"</code> to block all the packets.
<code>-a [AD_SET]</code>	It means to configure the advanced settings.
<code>-f [VALUE]</code>	It means to accept large incoming fragmented UDP or ICMP packets. VALUE : 0:Disable, 1:Enable
<code>-E [VALUE]</code>	It means to set the maximum count (0-10000) for session limitation.
<code>-Q [VALUE]</code>	It means to set the QoS class. VALUE: 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    : None

Actions for packet not matching any rule:
  Pass or Block      : Pass
  CodePage           : ANSI(1252)-Latin I
  Max Sessions Limit: 60000
  Current Sessions  : 0
  Mac Bind IP        : Non-Strict
  QOS Class          : None
  APP Enforcement    : None
  URL Content Filter: None
  Load-Balance policy : Auto-select
-----
CodePage              : ANSI(1252)-Latin I
Window size           : 65535
Session timeout       : 1440
DrayTek Banner        : Enable
-----
Apply IP filter to VPN incoming packets      : Enable
Accept large incoming fragmented UDP or ICMP packets: Enable
-----
Strict Security Checking
  [ ]APP Enforcement
>

```

Telnet Command: ipf rule

This command is used to set filter rule for firewall.

Syntax

`ipf rule s r [-<command> <parameter> | ...`

`ipf rule s r -v`

Syntax Description

Parameter	Description
<i>s</i>	Such word means Filter Set, range form 1-12.
<i>r</i>	Such word means Filter Rule, range from 1-7.
<Command><parameter>	The following lists all of the available commands with parameters.
-e	It means to enable or disable the rule setting. 0- disable 1- enable
-s o:g <obj>	It means to specify source IP object and IP group.

	<p>o - indicates "object".</p> <p>g - indicates "group".</p> <p>obj - indicates index number of object or index number of group. Available settings range from 1-192. For example, "-s g 3" means the third source IP group profile.</p>
<p><i>-s u <Address Type> <Start IP Address> <End IP Address> / <Address Mask></i></p>	<p>It means to configure source IP address including address type, start IP address, end IP address and address mask.</p> <p>u - It means "user defined".</p> <p><i>Address Type</i> - Type the number (representing different address type).</p> <p>0 - Subnet Address</p> <p>1 - Single Address</p> <p>2 - Any Address</p> <p>3 - Range Address</p> <p>Example:</p> <p>Set Subnet Address => -s u 0 192.168.1.10 255.255.255.0</p> <p>Set Single Address => -s u 1 192.168.1.10</p> <p>Set Any Address => -s u 2</p> <p>Set Range Address => -s u 3 192.168.1.10 192.168.1.15</p>
<p><i>-d u <Address Type> <Start IP Address> <End IP Address> / <Address Mask></i></p>	<p>It means to configure destination IP address including address type, start IP address, end IP address and address mask.</p> <p>u - It means "user defined".</p> <p><i>Address Type</i> - Type the number (representing different address type).</p> <p>0 - Subnet Address</p> <p>1 - Single Address</p> <p>2 - Any Address</p> <p>3 - Range Address</p> <p>Example:</p> <p>Set Subnet Address => -d u 0 192.168.1.10 255.255.255.0</p> <p>Set Single Address => -d u 1 192.168.1.10</p> <p>Set Any Address => -d u 2</p> <p>Set Range Address => -d u 3 192.168.1.10 192.168.1.15</p>
<p><i>-d o:g <obj></i></p>	<p>It means to specify destination IP object and IP group.</p> <p>o - indicates "object".</p> <p>g - indicates "group"</p> <p><obj>- indicates index number of object or index number of group. Available settings range from 1-192. For example, "-d g 1" means the first destination IP group profile.</p>
<p><i>-S o:g <obj></i></p>	<p>It means to specify Service Type object and IP group.</p> <p>o - indicates "object".</p> <p>g - indicates "group"</p> <p><obj> - indicates index number of object or index number of group. Available settings range from 1-96. For example, "-S 0 1" means the first service type object profile.</p>
<p><i>-S u <protocol> <source_port_value> <destination_port_vale></i></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	<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>
-q	<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	<p>It means load balance policy.</p> <p>Such function is used for "debug" only.</p>
-E	<p>It means to enable APP Enforcement.</p>
-a<index>	<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>
-u<index>	<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>
-c	<p>It means to set code page. Different number represents different code page.</p> <p>0. None</p> <ol style="list-style-type: none"> 1. ANSI(1250)-Central Europe 2. ANSI(1251)-Cyrillic 3. ANSI(1252)-Latin I 4. ANSI(1253)-Greek 5. ANSI(1254)-Turkish 6. ANSI(1255)-Hebrew 7. ANSI(1256)-Arabic 8. ANSI(1257)-Baltic 9. ANSI(1258)-Viet Nam 10. OEM(437)-United States 11. OEM(850)-Multilingual Latin I 12. OEM(860)-Portuguese 13. OEM(861)-Icelandic 14. OEM(863)-Canadian French 15. OEM(865)-Nordic 16. ANSI/OEM(874)-Thai 17. ANSI/OEM(932)-Japanese Shift-JIS 18. ANSI/OEM(936)-Simplified Chinese GBK 19. ANSI/OEM(949)-Korean 20. ANSI/OEM(950)-Traditional Chinese Big5
-C <Windows Size> <Session_Timeout>	<p>It means to set Window size and Session timeout (Minute).</p> <p><Windows Size> - Available settings range from 1 ~ 65535.</p> <p><Session_Timeout> - Make the best utilization of network resources.</p>
-v	<p>It is used to show current filter/rule settings.</p>

Example

```
> ipf rule 2 1 -e 1 -s "o 1" -d "o 2" -S "o 1" -F 2
> ipf rule 2 1 -v

Filter Set 2 Rule 1:

Status      : Enable
Comments: xNetBios -> DNS
Index(1-15) in Schedule Setup: <null>, <null>, <null>, <null>

Direction   : LAN -> WAN
Source IP    : Group1,
Destination IP: Group2,
Service Type : TCP/UDPGroup1,
Fragments    : Don't Care

Pass or Block      : Block Immediately
Branch to Other Filter Set: None
Max Sessions Limit : 32000
Current Sessions   : 0
Mac Bind IP        : Non-Strict
Qos Class          : None
APP Enforcement    : None
URL Content Filter : None
Load-Balance policy : Auto-select
Log                : Disable
-----
----
CodePage           : ANSI(1252)-Latin I
Window size        : 65535
Session timeout    : 1440
DrayTek Banner     : Enable
-----
---
Strict Security Checking
  [ ]APP Enforcement
```

Telnet Command: ipf flowtrack

This command is used to set and view flowtrack sessions.

Syntax

```
ipf flowtrack set [-re]
```

```
ipf flowtrack view [-f]
```

```
ipf flowtrack [-i][/-p][/-t]
```

Syntax Description

Parameter	Description
<i>-r</i>	It means to refresh the flowtrack.
<i>-e</i>	It means to enable or disable the flowtrack. 0: Disable 1: Enable
<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
```

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 [-cfhptwx?] [-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
-h	It means to show this usage help.
-p	It means to show PPP/MP log.
-t	It means to show all logs saved in the log buffer.
-w	It means to show WAN log.
-x	It means to show packet body hex dump.

Example

```

> log -w
25:36:25.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
  Client IP      = 0.0.0.0
  Your IP       = 0.0.0.0
  Next server IP = 0.0.0.0
  Relay agent IP = 0.0.0.0
25:36:33.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
  Client IP      = 0.0.0.0
  Your IP       = 0.0.0.0
  Next server IP = 0.0.0.0
  Relay agent IP = 0.0.0.0
25:36:41.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
  Client IP      = 0.0.0.0
  Your IP       = 0.0.0.0
  Next server IP = 0.0.0.0
  Relay agent IP = 0.0.0.0
25:36:49.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
  Client IP      = 0.0.0.0
  Your IP       = 0.0.0.0
  Next server IP = 0.0.0.0
  Relay agent IP = 0.0.0.0
25:36:57.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
  Client IP      = 0.0.0.0
  Your IP       = 0.0.0.0
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
```

Telnet Command: mngt ftpport

This command allows users to set FTP port for management.

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/t r069</i>	It means to specify one of the servers/protocols for enabling or disabling.
<i>on/off</i>	on - enable the function. off - disable the function.

Example

```
> mngt rmtcfg ftp on
Enable server fail
Remote configure function has been disabled
please enable by enter mngt rmtcfg enable

> mngt rmtcfg enable
%% Remote configure function has been enabled.
> mngt rmtcfg ftp on
%% FTP server has been enabled.
```

Telnet Command: mngt echoicmp

This command allows users to reject or accept PING packets from the Internet.

Syntax

mngt echoicmp *[enable]*

mngt echoicmp *[disable]*

Syntax Description

Parameter	Description
<i>enable</i>	It means to accept the echo ICMP packet.
<i>disable</i>	It means to drop the echo ICMP packet.

Example

```
> mngt echoicmp enable
%% Echo ICMP packet enabled.
```

Telnet Command: mngt accesslist

This command allows you to specify that the system administrator can login from a specific host or network. A maximum of three IPs/subnet masks is allowed.

Syntax

mngt accesslist *list*

mngt accesslist *add [index][ip addr][mask]*

mngt accesslist *remove [index]*

mngt accesslist *flush*

Syntax Description

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

<i>list</i>	It can display current setting for your reference.
<i>add</i>	It means adding a new entry.
<i>index</i>	It means to specify the number of the entry.
<i>ip addr</i>	It means to specify an IP address.
<i>mask</i>	It means to specify the subnet mask for the IP address.
<i>remove</i>	It means to delete the selected item.
<i>flush</i>	It means to remove all the settings in the access list.

Example

```
> mngt accesslist add 1 192.168.1.89 255.255.255.0
%% Set OK.
> mngt accesslist list
%% Access list :
  Index IP address      Subnet mask
=====
  1      192.168.1.89    255.255.255.0
```

Telnet Command: mngt snmp

This command allows you to configure SNMP for management.

Syntax

mngt snmp [-<command> <parameter> | ...]

Syntax Description

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

Example

```
> mngt snmp -e 1 -g draytek -s DK -m 192.168.1.1 -t trapcom -n 10.20.3.40
-T 88
SNMP Agent Turn on!!!
Get Community set to draytek
```



```

Set Community set to DK
Manager Host IP set to 192.168.1.1
Trap Community set to trapcom
Notification Host IP set to 10.20.3.40
Trap Timeout set to 88 seconds

```

Telnet Command: 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: <code>object ip obj 1 -v</code>
<i>-n NAME</i>	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: <code>object ip obj 9 -n bruce</code>
<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: <code>object ip obj 8 -i 0</code>
<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: <code>object ip obj 3 -s 1</code>
<i>-a TYPE</i>	It means to set the address type and IP for the IP object profile. TYPE=0, means Mask TYPE=1, means Single TYPE=2, means Any TYPE=3, means Rang Example: <code>object ip obj 3 -a 2</code>
<i>[START_IP]</i>	When the TYPE is set with 2, you have to type an IP address as a starting point and another IP address as end point. Type an IP address.
<i>[END/MASK_IP]</i>	Type an IP address (different with START_IP) as the end IP address.

Example

```

> object ip obj 1 -n marketing
> object ip obj 1 -a 1 192.168.1.45
> object ip obj 1 -v
IP Object Profile 1
Name      :[marketing]
Interface:[Any]
Address type:[single]
Start ip address:[192.168.1.45]
End/Mask ip address:[0.0.0.0]
Invert Selection:[0]

```

Telnet Command: object ip grp

This command is used to integrate several IP objects under an IP group profile.

Syntax

`object ip grp setdefault`

`object ip grp INDEX -v`

`object ip grp INDEX -n NAME`

`object ip grp INDEX -i INTERFACE`

`object ip grp INDEX -a IP_OBJ_INDEX`

Syntax Description

Parameter	Description
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number of the specified group profile.
<i>-v</i>	It means to view the information of the specified group profile. Example: <i>object ip grp 1 -v</i>
<i>-n NAME</i>	It means to define a name for the IP group. NAME: Type a name with less than 15 characters. Example: <i>object ip grp 8 -n bruce</i>
<i>-i INTERFACE</i>	It means to define an interface for the IP group. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=2, means WAN Example: <i>object ip grp 3 -i 0</i>
<i>-a IP_OBJ_INDEX</i>	It means to specify IP object profiles for the group profile. Example: <i>:object ip grp 3 -a 1 2 3 4 5</i> The IP object profiles with index number 1,2,3,4 and 5 will be group under such profile.

Example

```

> object ip grp 2 -n First
IP Group Profile 2
Name      :[First]
Interface:[Any]
Included ip object index:
[0:][0]

```

```
[1:][0]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]

> object ip grp 2 -i 1
> object ip grp 2 -a 1 2
IP Group Profile 2
Name      :[First]
Interface:[Lan]
Included ip object index:
[0:][1]
[1:][2]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]
```

Telnet Command: object ipv6 obj

This command is used to create an IP object profile.

Syntax

object ip obj setdefault

object ip obj *INDEX* -v

object ip obj *INDEX* -n *NAME*

object ip obj *INDEX* -i *INTERFACE*

object ip obj *INDEX* -s *INVERT*

object ip obj *INDEX* -a *TYPE* [*START_IP*] [*END/MASK_IP*]

Syntax Description

Parameter	Description
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number of the specified object profile.
-v	It means to view the information of the specified object profile. Example: <i>object ip obj 1 -v</i>
-n <i>NAME</i>	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: <i>object ip obj 9 -n bruce</i>
-i <i>INTERFACE</i>	It means to define an interface for the IP object. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=3, means WAN Example: <i>object ip obj 8 -i 0</i>
-s <i>INVERT</i>	It means to set invert selection for the object profile. INVERT=0, means disabling the function. INVERT=1, means enabling the function. Example: <i>object ip obj 3 -s 1</i>
-a <i>TYPE</i>	It means to set the address type and IP for the IP object profile. TYPE=0, means Mask TYPE=1, means Single TYPE=2, means Any TYPE=3, means Rang Example: <i>object ip obj 3 -a 2</i>
[<i>START_IP</i>]	When the TYPE is set with 2, you have to type an IP address as a starting point and another IP address as end point. Type an IP address.
[<i>END/MASK_IP</i>]	Type an IP address (different with <i>START_IP</i>) as the end IP address.

Example

```
> object ip obj 1 -n marketing
> object ip obj 1 -a 1 192.168.1.45
> object ip obj 1 -v
IP Object Profile 1
Name      :[marketing]
```

```

Interface:[Any]
Address type:[single]
Start ip address:[192.168.1.45]
End/Mask ip address:[0.0.0.0]
Invert Selection:[0]

```

Telnet Command: object ipv6 grp

This command is used to integrate several IP objects under an IP group profile.

Syntax

`object ip grp setdefault`

`object ip grp INDEX -v`

`object ip grp INDEX -n NAME`

`object ip grp INDEX -i INTERFACE`

`object ip grp INDEX -a IP_OBJ_INDEX`

Syntax Description

Parameter	Description
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number of the specified group profile.
<i>-v</i>	It means to view the information of the specified group profile. Example: <i>object ip grp 1 -v</i>
<i>-n NAME</i>	It means to define a name for the IP group. NAME: Type a name with less than 15 characters. Example: <i>object ip grp 8 -n bruce</i>
<i>-i INTERFACE</i>	It means to define an interface for the IP group. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=2, means WAN Example: <i>object ip grp 3 -i 0</i>
<i>-a IP_OBJ_INDEX</i>	It means to specify IP object profiles for the group profile. Example: <i>:object ip grp 3 -a 1 2 3 4 5</i> The IP object profiles with index number 1,2,3,4 and 5 will be group under such profile.

Example

```

> object ip grp 2 -n First
IP Group Profile 2
Name   :[First]
Interface:[Any]
Included ip object index:
[0:][0]
[1:][0]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]

```

```

[7:][0]

> object ip grp 2 -i 1
> object ip grp 2 -a 1 2
IP Group Profile 2
Name      :[First]
Interface:[Lan]
Included ip object index:
[0:][1]
[1:][2]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]

```

Telnet Command: object service obj

This command is used to create service object profile.

Syntax

object service obj setdefault

object service obj INDEX -v

object service obj INDEX -n NAME

object service obj INDEX -p PROTOCOL

object service obj INDEX -s CHK [START_P] [END_P]

object service obj INDEX -d CHK [START_P] [END_P]

Syntax Description

Parameter	Description
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number of the specified service object profile.
<i>-v</i>	It means to view the information of the specified service object profile. Example: <i>object service obj 1 -v</i>
<i>-n NAME</i>	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: <i>object service obj 9 -n bruce</i>
<i>-i PROTOCOL</i>	It means to define a PROTOCOL for the service object profile. PROTOCOL =0, means any PROTOCOL =1, means ICMP PROTOCOL =2, means IGMP PROTOCOL =6, means TCP PROTOCOL =17, means UDP PROTOCOL =255, means TCP/UDP Other values mean other protocols. Example: <i>object service obj 8 -i 0</i>
<i>CHK</i>	It means the check action for the port setting. 0=equal(=), when the starting port and ending port values are the

	<p>same, it indicates one port; when the starting port and ending port values are different, it indicates a range for the port and available for this service type.</p> <p>1=not equal(!=), when the starting port and ending port values are the same, it indicates all the ports except the port defined here; when the starting port and ending port values are different, it indicates that all the ports except the range defined here are available for this service type.</p> <p>2=larger(>), the port number greater than this value is available..</p> <p>3=less(<), the port number less than this value is available for this profile.</p>
<code>-s CHK [START_P] [END_P]</code>	<p>It means to set source port check and configure port range (1-65565) for TCP/UDP.</p> <p>END_P, type a port number to indicate source port.</p> <p>Example: <code>object service obj 3 -s 0 100 200</code></p>
<code>-d CHK [START_P] [END_P]</code>	<p>It means to set destination port check and configure port range (1-65565) for TCP/UDP.</p> <p>END_P, type a port number to indicate destination port.</p> <p>Example: <code>object service obj 3 -d 1 100 200</code></p>

Example

```

> object service obj 1 -n limit
> object service obj 1 -p 255
> object service obj 1 -s 1 120 240
> object service obj 1 -d 1 200 220
> object service obj 1 -v
Service Object Profile 1
Name      :[limit]
Protocol  :[255]
Source port check action:[!=]
Source port range:[120~240]
Destination port check action:[!=]
Destination port range:[200~220]

```

Telnet Command: object service grp

This command is used to integrate several service objects under a service group profile.

Syntax

```

object service grp setdefault
object service grp INDEX -v
object service grp INDEX -n NAME
object service grp INDEX -a SER_OBJ_INDEX

```

Syntax Description

Parameter	Description
<code>setdefault</code>	It means to return to default settings for all profiles.
<code>INDEX</code>	It means the index number of the specified group profile.
<code>-v</code>	It means to view the information of the specified group profile. Example: <code>object service grp 1 -v</code>
<code>-n NAME</code>	It means to define a name for the service group.

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

Example

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

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

Telnet Command: object kw

This command is used to create keyword profile.

Syntax

```
object kw obj setdefault
object kw obj show PAGE
object kw obj INDEX -v
object kw obj INDEX -n NAME
object kw obj INDEX -a CONTENTS
```

Syntax Description

Parameter	Description
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>show PAGE</i>	It means to show the contents of the specified profile.

	PAGE: type the page number.
<i>show</i>	It means to show the contents for all of the profiles.
<i>INDEX</i>	It means the index number of the specified keyword profile.
<i>-v</i>	It means to view the information of the specified keyword profile.
<i>-n NAME</i>	It means to define a name for the keyword profile. NAME: Type a name with less than 15 characters.
<i>-a CONTENTS</i>	It means to set the contents for the keyword profile. Example: <i>object kw obj 40 -a test</i>

Example

```

> object kw obj 1 -n children
Profile 1
Name   :[children]
Content:[]
> object kw obj 1 -a gambling
Profile 1
Name   :[children]
Content:[gambling]

> object kw obj 1 -v
Profile 1
Name   :[children]
Content:[gambling]

```

Telnet Command: object fe

This command is used to create File Extension Object profile.

Syntax

`object fe show`

`object fe setdefault`

`object fe obj INDEX -v`

`object fe obj INDEX -n NAME`

`object fe obj INDEX -e CATEGORY/FILE_EXTENSION`

`object fe obj INDEX -d CATEGORY/FILE_EXTENSION`

Syntax Description

Parameter	Description
<i>show</i>	It means to show the contents for all of the profiles.
<i>setdefault</i>	It means to return to default settings for all profiles.
<i>INDEX</i>	It means the index number (from 1 to 8) of the specified file extension object profile.
<i>-v</i>	It means to view the information of the specified file extension object profile.
<i>-n NAME</i>	It means to define a name for the file extension object profile. NAME: Type a name with less than 15 characters.
<i>-e</i>	It means to enable the specific CATEGORY or FILE_EXTENSION.

<code>-d</code>	It means to disable the specific CATEGORY or FILE_EXTENSION
<code>CATEGORY/FILE_EXTENSION</code>	<p>CATEGORY: Image, Video, Audio, Java, ActiveX, Compression, Execution Example: <code>object fe obj 1 -e Image</code></p> <p>FILE_EXTENSION: ".bmp", ".dib", ".gif", ".jpeg", ".jpg", ".jpg2", ".jp2", ".pct", ".pcx", ".pic", ".pict", ".png", ".tif", ".tiff", ".asf", ".avi", ".mov", ".mpe", ".mpeg", ".mpg", ".mp4", ".qt", ".rm", ".wmv", ".3gp", ".3gpp", ".3gpp2", ".3g2", ".aac", ".aiff", ".au", ".mp3", ".m4a", ".m4p", ".ogg", ".ra", ".ram", ".vox", ".wav", ".wma", ".class", ".jad", ".jar", ".jav", ".java", ".jcm", ".js", ".jse", ".jsp", ".jtk", ".alx", ".apb", ".axs", ".ocx", ".olb", ".ole", ".tlb", ".viv", ".vrm", ".ace", ".arj", ".bzip2", ".bz2", ".cab", ".gz", ".gzip", ".rar", ".sit", ".zip", ".bas", ".bat", ".com", ".exe", ".inf", ".pif", ".reg", ".scr" Example: <code>object fe obj 1 -e .bmp</code></p>

Example

```

> object fe obj 1 -n music
> object fe obj 1 -e Audio
> object fe obj 1 -v
Profile Index: 1
Profile Name:[music]

-----
Image category:
[ ].bmp [ ].dib [ ].gif [ ].jpeg [ ].jpg [ ].jpg2 [ ].jp2 [ ].pct
[ ].pcx [ ].pic [ ].pict [ ].png [ ].tif [ ].tiff
-----
Video category:
[ ].asf [ ].avi [ ].mov [ ].mpe [ ].mpeg [ ].mpg [v].mp4 [ ].qt
[ ].rm [v].wmv [ ].3gp [ ].3gpp [ ].3gpp2 [ ].3g2
-----
Audio category:
[v].aac [v].aiff [v].au [v].mp3 [v].m4a [v].m4p [v].ogg [v].ra
[v].ram [v].vox [v].wav [v].wma
-----
Java category:
[ ].class [ ].jad [ ].jar [ ].jav [ ].java [ ].jcm [ ].js [ ].jse
[ ].jsp [ ].jtk
-----
ActiveX category:
[ ].alx [ ].apb [ ].axs [ ].ocx [ ].olb [ ].ole [ ].tlb [ ].viv
[ ].vrm
-----
Compression category:
[ ].ace [ ].arj [ ].bzip2 [ ].bz2 [ ].cab [ ].gz [ ].gzip [ ].rar
[ ].sit [ ].zip

```

```
-----  
-----  
Execution category:  
[ ].bas [ ].bat [ ].com [ ].exe [ ].inf [ ].pif [ ].reg [ ].scr
```

Telnet Command: port

This command allows users to set the speed for specific port of the router.

Syntax

port [*1, wan2, all*] [*AN, 100F, 100H, 10F, 10H, status*]

port status

port wanfc

Syntax Description

Parameter	Description
<i>1, 2, 3, 4, 5, 6, wan2, all</i>	It means the number of LAN port and WAN port.
<i>AN... 10H</i>	It means the physical type for the specific port. AN: auto-negotiate. 100F: 100M Full Duplex. 100H: 100M Half Duplex. 10F: 10M Full Duplex. 10H: 10M Half Duplex.
<i>status</i>	It means to view the Ethernet port status.
<i>wanfc</i>	It means to set WAN flow control.

Example

```
> port 1 100F
%Set Port 1 Force speed 100 Full duplex OK !!!
```

Telnet Command: portmuptime

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

Syntax

portmuptime [*-<command> <parameter> | ...*]

Syntax Description

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

<code>-f</code>	It means to flush all portmaps (useful for diagnostics).
<code>-l <List></code>	List all settings.

Example

```
> portmuptime -t 86400 -u 300 -i 10
> portmuptime -l
----- Current setting -----
TCP Timeout   : 86400 sec.
UDP Timeout   : 300 sec.
IGMP Timeout  : 10 sec.
TCP WWW Timeout: 60 sec.
TCP SYN Timeout: 60 sec.
```

Telnet Command: qos setup

This command allows user to set general settings for QoS.

Syntax

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

Syntax Description

Parameter	Description
<code>[<command> <parameter> ...]</code>	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
<code>-h</code>	Type it to display the usage of this command.
<code>-m <mode></code>	It means to define which traffic the QoS control settings will apply to and enable QoS control. 0: disable. 1: in, apply to incoming traffic only. 2: out, apply to outgoing traffic only. 3: both, apply to both incoming and outgoing traffic. Default is enable (for outgoing traffic).
<code>-i <bandwidth></code>	It means to set inbound bandwidth in kbps (Ethernet WAN only). The available setting is from 1 to 100000.
<code>-o <bandwidth></code>	It means to set outbound bandwidth in kbps (Ethernet WAN only). The available setting is from 1 to 100000.
<code>-r <index:ratio></code>	It means to set ratio for class index, in %.
<code>-u <mode></code>	It means to enable bandwidth control for UDP. 0: disable 1: enable Default is disable.
<code>-p <ratio></code>	It means to enable bandwidth limit ratio for UDP.
<code>-t <mode></code>	It means to enable/disable Outbound TCP ACK Prioritize. 0: disable 1: enable
<code>-V</code>	Show all the settings.
<code>-D</code>	Set all to factory default (for all WANs).
<code>[...]</code>	It means that you can type in several commands in one line.

Example

```
> qos setup -m 3 -i 9500 -o 8500 -r 3:20 -u 1 -p 50 -t 1

WAN1 QoS mode is both
Wan 1 is XDSL model ,don,t need to set up
Wan 1 is XDSL model ,don,t need to set up
WAN1 class 3 ratio set to 20
WAN1 udp bandwidth control set to enable
WAN1 udp bandwidth limit ratio set to 50
WAN1 Outbound TCP ACK Prioritizel set to enable
QoS WAN1 set complete; restart QoS
>
```

Telnet Command: qos class

This command allows user to set QoS class.

Syntax

qos class -c [*no*] -[*a|e|d*] [*no*][-<command> <parameter> | ...]

Syntax Description

Parameter	Description
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-h	Type it to display the usage of this command.
-c <no>	Specify the inde number for the class. Available value for <no> contains 1, 2 and 3. The default setting is class 1.
-n <name>	It means to type a name for the class.
-a	It means to add rule for specified class.
-e <no>	It means to edit specified rule. <no>: type the index number for the rule.
-d <no>	It means to delete specified rule. <no>: type the index number for the rule.
-m <mode>	It means to enable or disable the specified rule. 0: disable, 1: enable
-l <addr>	Set the local address. <i>Addr1</i> - It means Single address. Please specify the IP address directly, for example, "-l 172.16.3.9". <i>addr1:addr2</i> - It means Range address. Please specify the IP addresses, for example, "-l 172.16.3.9: 172.16.3.50." <i>addr1:subnet</i> - It means the subnet address with start IP address. Please type the subnet and the IP address, for example, "-l 172.16.3.9:255.255.0.0". <i>any</i> - It means Any address. Simple type "-l" to specify any address for this command.
-r <addr>	Set the remote address. <i>addr1</i> - It means Single address. Please specify the IP address directly, for example, "-r 172.16.3.9". <i>addr1:addr2</i> - It means Range address. Please specify the IP addresses, for example, "-r 172.16.3.9: 172.16.3.50." <i>addr1:subnet</i> - It means the subnet address with start IP address. Please type the subnet and the IP address, for example, "-r 172.16.3.9:255.255.0.0". <i>any</i> - It means Any address. Simple type "-r" to specify any address for this command.
-p <DSCP id>	Specify the ID.
-s <Service type>	Specify the predefined service type by typing the number. The available types are listed as below: 1:ANY 2:DNS 3:FTP 4:GRE 5:H.323 6:HTTP 7:HTTPS 8:IKE 9:IPSEC-AH 10:IPSEC-ESP 11:IRC 12:L2TP 13:NEWS 14:NFS 15:NNTP 16:PING 17:POP3 18:PPTP 19:REAL-AUDIO 20:RTSP 21:SFTP 22:SIP 23:SMTP 24:SNMP 25:SNMP-TRAPS 26:SQL-NET 27:SSH 28:SYSLOG 29:TELNET 30:TFTP

<code>-u<Service type></code>	Define service type. Available value: 1-40.
<code>-S <d/s></code>	Show the content for specified DSCP ID/Service type.
<code>-V <1/2/3></code>	Show the rule in the specified class.
<code>[...]</code>	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
<code>-a <name></code>	It means to add rule.
<code>-e <no></code>	It means to edit user defined service type. "no" means the index number. Available numbers are 1-40.
<code>-d <no></code>	It means to delete user defined service type. "no" means the index number. Available numbers are 1-40.
<code>-n <name></code>	It means the name of the service.
<code>-t <type></code>	It means protocol type. 6: tcp(default) 17: udp 0: tcp/udp <1-254>: other
<code>-p <port></code>	It means service port. The typing format must be [start:end] (ex., 510:330).
<code>-l</code>	List user defined types. "no" means the index number. Available numbers are 1-40.

Example

```
> qos type -a draytek -t 6 -p 510:1330

service name set to draytek
service type set to 6:TCP
Port type set to Range
Service Port set to 510 ~ 1330
>
```

Telnet Command: quit

This command can exit the telnet command screen.

Telnet Command: show lan1/lan2/dhcp

This command displays current status of LAN IP address settings.

Example

```
> > show lan1
%% 1st subnet settings:
%%   IP address: 192.168.1.1
%%   Subnet mask: 255.255.255.0
%%   RIP : [Disable]

> show lan2
%% 2nd subnet settings:
%%   Status: [Inactive]
%%   IP address: 192.168.2.5
%%   Subnet mask: 255.255.255.0
%%   RIP : [Disable]

> show dhcp
%% DHCP settings:
%%   Status: [Active]
%%   Start IP address for offering: 192.168.1.10
%%   Maximus offer IP address count: 200
%%   Default gateway: 192.168.1.1

%%   DHCP Relay: [Inactive]
```

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 192.168.1.65

%      WAN2 DMZ mapping status:
Index  Status  WAN2 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]
```

Telnet Command: show openport

This command displays current status of open port setting.

Example

```
> show openport
%%     Openport settings:
Index  Status  Comment          Local IP Address
*****
                        No data entry.
```

Telnet Command: show nat

This command displays current status of NAT.

Example

```
> show nat
Port Redirection Running Table:

Index  Protocol  Public Port  Private IP    Private Port
-----
  1          0          0  0.0.0.0        0
  2          0          0  0.0.0.0        0
  3          0          0  0.0.0.0        0
  4          0          0  0.0.0.0        0
  5          0          0  0.0.0.0        0
```

6	0	0	0.0.0.0	0
7	0	0	0.0.0.0	0
8	0	0	0.0.0.0	0
9	0	0	0.0.0.0	0
10	0	0	0.0.0.0	0
11	0	0	0.0.0.0	0
12	0	0	0.0.0.0	0
13	0	0	0.0.0.0	0
14	0	0	0.0.0.0	0
15	0	0	0.0.0.0	0
16	0	0	0.0.0.0	0
17	0	0	0.0.0.0	0
18	0	0	0.0.0.0	0
19	0	0	0.0.0.0	0
20	0	0	0.0.0.0	0
--- MORE --- ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]				

Telnet Command: show portmap

This command displays the table of NAT Active Sessions.

Example

```
> show portmap
-----
-
Private_IP:Port Pseudo_IP:Port Peer_IP:Port [Timeout/Protocol/Flag]
-----
-
```

Telnet Command: show pmtime

This command displays the reuse time of NAT session.

Level0: It is the default setting.

Level1: It will be applied when the NAT sessions are smaller than 25% of the default setting.

Level2: It will be applied when the NAT sessions are smaller than the eighth of the default setting.

Example

```
> show pmtime
Level0 TCP=86400001 UDP=300001 ICMP=10001
Level1 TCP=600000 UDP=90000 ICMP=7000
Level2 TCP=60000 UDP=30000 ICMP=5000
```

Telnet Command: show session

This command displays current status of current session.

Example

```
> show session
% Maximum Session Number: 10000
% Maximum Session Usage: 0
% Current Session Usage: 0
```

```

% Current Session Used(include waiting for free): 0
% WAN1 Current Session Usage: 0
% WAN2 Current Session Usage: 0

```

Telnet Command: show status

This command displays current status of LAN and WAN connections.

Example

```

> show status
System Uptime:70:12:46
LAN Status
Primary DNS:8.8.8.8          Secondary DNS:8.8.4.4
IP Address:192.168.1.1      Tx Rate:41354    Rx Rate:10951

WAN 1 Status: Disconnected
Enable:Yes      Line:xDSL      Name:tcom
Mode:PPPoE      Up Time:0:00:00    IP:---          GW IP:---
TX Packets:0    TX Rate:0          RX Packets:0    RX Rate:0

WAN 2 Status: Disconnected
Enable:Yes      Line:Ethernet     Name:
Mode:Static IP  Up Time:0:00:00    IP:0.0.0.0      GW IP:0.0.0.0
TX Packets:0    TX Rate:0          RX Packets:0    RX Rate:0

ADSL Information:      ADSL Firmware Version:05-04-04-05-01-02
Mode:                  State:TRAINING    TX Block:0      RX Block:0
Corrected Blocks:0    Uncorrected Blocks:0
UP Speed:0            Down Speed:0      SNR Margin:0    Loop Att.:0

```

Telnet Command: show adsl

This command displays current status of ADSL.

Example

```

> show adsl
----- ATU-R Info (hw: annex B, f/w: annex X) -----
Running Mode      :          State      : TRAINING
DS Actual Rate   :          0 bps    US Actual Rate   :          0 bps
DS Attainable Rate :          0 bps    US Attainable Rate :          0 bps
DS Path Mode     :          Fast     US Path Mode     :          Fast
DS Interleave Depth :          0      US Interleave Depth :          0
NE Current Attenuation :          0 dB    Cur SNR Margin   :          0 dB
DS actual PSD    :          0.0 dB    US actual PSD    :          0.0 dB
NE Rcvd Cells    :          0        NE Xmitted Cells  :          0
NE CRC Count     :          0        FE CRC Count     :          0
NE ES Count      :          0        FE ES Count      :          0
Xdsl Reset Times :          0        Xdsl Link Times  :          0
ITU Version[0]   : b5004946        ITU Version[1]   : 544e0000
ADSL Firmware Version : 05-04-04-05-01-02
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: show statistic

This command displays statistics for WAN interface.

Syntax

show statistic

show statistic reset *[interface]*

Syntax Description

Parameter	Description
<i>reset</i>	It means to reset the transmitted/received bytes to Zero.
<i>interface</i>	It means to specify WAN1 ~WAN5 (including multi-PVC) interface for displaying related statistics.

Example

```
> show statistic
WAN1 total TX: 0 Bytes ,RX: 0 Bytes
WAN2 total TX: 0 Bytes ,RX: 0 Bytes
WAN3 total TX: 0 Bytes ,RX: 0 Bytes
WAN4 total TX: 0 Bytes ,RX: 0 Bytes
WAN5 total TX: 0 Bytes ,RX: 0 Bytes
>
```

Telnet Command: `srv dhcp public`

This command allows users to configure DHCP server for second subnet.

Syntax

```
srv dhcp public start [IP address]
```

```
srv dhcp public cnt [IP counts]
```

```
srv dhcp public status
```

```
srv dhcp public add [MAC Addr XX-XX-XX-XX-XX-XX]
```

```
srv dhcp public del [MAC Addr XX-XX-XX-XX-XX-XX/all/ALL]
```

Syntax Description

Parameter	Description
<i>start</i>	It means the starting point of the IP address pool for the DHCP server.
<i>IP address</i>	It means to specify an IP address as the starting point in the IP address pool.
<i>cnt</i>	It means the IP count number.
<i>IP counts</i>	It means to specify the number of IP addresses in the pool. The maximum is 10.
<i>status</i>	It means the execution result of this command.
<i>add</i>	It means creating a list of hosts to be assigned.
<i>del</i>	It means removing the selected MAC address.
<i>MAC Addr</i>	It means to specify MAC Address of the host.
<i>all/ALL</i>	It means all of the MAC addresses.

Example

```
Vigor> ip route add 192.168.1.56 255.255.255.0 192.168.1.12 3 default
Vigor> srv dhcp public status
Index  MAC Address
```

Telnet Command: `srv dhcp dns1`

This command allows users to set Primary IP Address for DNS Server in LAN.

Syntax

```
srv dhcp dns1 [?]
```

```
srv dhcp dns1 [DNS IP address]
```

Syntax Description

Parameter	Description
<i>?</i>	It means to display current IP address of DNS 1 for the DHCP server.
<i>DNS IP address</i>	It means the IP address that you want to use as DNS1. Note: The IP Routed Subnet DNS must be the same as NAT Subnet DNS).

Example

```
> srv dhcp dns1 168.95.1.1
% srv dhcp dns1 <DNS IP address>
% Now: 168.95.1.1
(IP Routed Subnet dns same as NAT Subnet dns)
```

Telnet Command: srv dhcp dns2

This command allows users to set Secondary IP Address for DNS Server in LAN.

Syntax

```
srv dhcp dns2 [?]
```

```
srv dhcp dns2 [DNS IP address]
```

Syntax Description

Parameter	Description
<i>?</i>	It means to display current IP address of DNS 2 for the DHCP server.
<i>DNS IP address</i>	It means the IP address that you want to use as DNS2. Note: The IP Routed Subnet DNS must be the same as NAT Subnet DNS).

Example

```
> srv dhcp dns2 10.1.1.1
% srv dhcp dns2 <DNS IP address>
% Now: 10.1.1.1
(IP Routed Subnet dns same as NAT Subnet dns)
```

Telnet Command: `srv dhcp frcdnsmanl`

This command can force the router to invoke DNS Server IP address.

Syntax

`srv dhcp frcdnsmanl [on]`

`srv dhcp frcdnsmanl [off]`

Syntax Description

Parameter	Description
<code>?</code>	It means to display the current status.
<code>on</code>	It means to use manual setting for DNS setting.
<code>Off</code>	It means to use auto settings acquired from ISP.

Example

```
> srv dhcp frcdnsmanl on
% Domain name server now is using manual settings!
> srv dhcp frcdnsmanl off
% Domain name server now is using auto settings!
```

Telnet Command: `srv dhcp gateway`

This command allows users to specify gateway address for DHCP server.

Syntax

`srv dhcp gateway [?]`

`srv dhcp gateway [Gateway IP]`

Syntax Description

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

Example

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


Telnet Command: `srv dhcp ipcnt`

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

Syntax

```
srv dhcp ipcnt [?]
```

```
srv dhcp ipcnt [IP counts]
```

Syntax Description

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

Example

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

Telnet Command: `srv dhcp off`

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

Telnet Command: `srv dhcp on`

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

Telnet Command: `srv dhcp relay`

This command allows users to set DHCP relay setting.

Syntax

```
srv dhcp relay servip [server ip]
```

```
srv dhcp relay subnet [index]
```

Syntax Description

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

Example

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

Telnet Command: `srv dhcp startip`

Syntax

srv dhcp startip [?]

srv dhcp startip [IP address]

Syntax Description

Parameter	Description
?	It means to display current used start IP address.
IP address	It means the IP address that you can specify for the DHCP server as the starting point.

Example

```
> srv dhcp startip 192.168.1.53
This setting will take effect after rebooting.
Please use "sys reboot" command to reboot the router.
```

Telnet Command: srv dhcp status

This command can display general information for the DHCP server, such as IP address, MAC address, leased time, host ID and so on.

Example

```
> srv dhcp status
DHCP server: Relay Agent
Default gateway: 192.168.1.1
Index   IP Address      MAC Address      Leased Time      HOST ID
1       192.168.1.113  00-05-5D-E4-D8-EE  17:20:08        A1000351
```

Telnet Command: `srv dhcp leasetime`

This command can set the lease time for the DHCP server.

Syntax

`srv dhcp leasetime [?]`

`srv dhcp leasetime [Lease Time (sec)]`

Syntax Description

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

Example

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

Telnet Command: `srv dhcp nodetype`

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

Syntax

`srv dhcp nodetype <count>`

Syntax Description

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

Example

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

Telnet Command: `srv dhcp primWINS`

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

Syntax

```
srv dhcp primWINS [WINS IP address]
```

```
srv dhcp primWINS clear
```

Syntax Description

Parameter	Description
<i>WINS IP address</i>	It means the IP address of primary WINS server.
<i>clear</i>	It means to remove the IP address settings of primary WINS server.

Example

```
> srv dhcp primWINS 192.168.1.88
> srv dhcp primWINS ?
%% srv dhcp primWINS <WINS IP address>
%% srv dhcp primWINS clear
% Now: 192.168.1.88
```

Telnet Command: `srv dhcp secWINS`

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

Syntax

```
srv dhcp secWINS [WINS IP address]
```

```
srv dhcp secWINS clear
```

Syntax Description

Parameter	Description
<i>WINS IP address</i>	It means the IP address of secondary WINS server.
<i>clear</i>	It means to remove the IP address settings of second WINS server.

Example

```
> srv dhcp secWINS 192.168.1.180
> srv dhcp secWINS ?
%% srv dhcp secWINS <WINS IP address>
%% srv dhcp secWINS clear
% Now: 192.168.1.180
```

Telnet Command: `srv dhcp expired_RecycleIP`

This command can set the time to check if the IP address can be assigned again by DHCP server or not.

Syntax

`srv dhcp expRecycleIP <sec time>`

Syntax Description

Parameter	Description
<i>sec time</i>	It means to set the time (5-300 seconds) for checking if the IP can be assigned again or not.

Example

```
Vigor> srv dhcp expRecycleIP 250
% DHCP expired_RecycleIP = 250
```

Telnet Command: `srv dhcp tftp`

This command can set the TFTP server as the DHCP server.

Syntax

`srv dhcp tftp <TFTP server name>`

Syntax Description

Parameter	Description
<i>TFTP server name</i>	It means to type the name of TFTP server.

Example

```
> srv dhcp tftp TF123
> srv dhcp tftp ?
%% srv dhcp tftp <TFTP server name>
% Now: TF123
```

Telnet Command: `srv dhcp option`

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

Syntax

`srv dhcp option -h`

`srv dhcp option -l`

`srv dhcp option -d [idx]`

`srv dhcp option -e [1 or 0] -c [option number] -v [option value]`

`srv dhcp option -e [1 or 0] -c [option number] -a [option value]`

`srv dhcp option -e [1 or 0] -c [option number] -x [option value]`

`srv dhcp option -u [idx unumber]`

Syntax Description

Parameter	Description
<i>-h</i>	It means to display usage of this command.
<i>-l</i>	It means to display all the user defined DHCP options.
<i>-d[idx]</i>	It means to delete the option number by specifying its index number.
<i>-e [1 or 0]</i>	It means to enable/disable custom option feature. 1:enable 0:disable
<i>-c</i>	It means to set option number. Available number ranges from 0 to 255.
<i>-v</i>	It means to set option number by typing string.
<i>-a</i>	It means to set the option value by specifying the IP address.
<i>-x</i>	It means to set option number with the format of Hexadecimal characters.
<i>-u</i>	It means to update the option value of the sepecified index.
<i>idx number</i>	It means the index number of the option value.

Example

```

> srv dhcp option -e 1 -c 18 -v /path
> srv dhcp option -l
% state  idx interface          opt type  data

% enable 1  ALL LAN                18 ASCII  /path

```

Telnet Command: `srv nat dmz`

This command allows users to set DMZ host. Before using this command, please set WAN IP Alias first.

Syntax

`srv nat dmz n m [-<command> <parameter> | ...]`

Syntax Description

Parameter	Description
<i>n</i>	It means to map selected WAN IP to certain host. 1: wan1 2: wan2
<i>m</i>	It means the index number of the DMZ host. Default setting is "1" (WAN 1). It is only available for Static IP mode. If you use other mode, you can set 1 ~ 8 in this field. If WAN IP alias has been configured, then the number of DMZ host can be added more.
<i>[<command> <parameter> ...]</i>	The available commands with parameters are listed below. <i>[...]</i> means that you can type in several commands in one line.
<i>-e</i>	It means to enable/disable such feature. 1:enable 0:disable
<i>-i</i>	It means to specify the private IP address of the DMZ host.
<i>-r</i>	It means to remove DMZ host setting.
<i>-v</i>	It means to display current status.

Example

```
> srv nat dmz 1 1 -i 192.168.1.96
> srv nat dmz -v
%      WAN1 DMZ mapping status:
Index  Status  WAN1 aux IP    Private IP
-----
1      Disable  0.0.0.0 192.168.1.96
```

Telnet Command: `srv nat ipsecpass`

This command allows users to enable or disable IPSec ESP tunnel passthrough and IKE source port (500) preservation.

Syntax

`srv nat ipsecpass [options]`

Syntax Description

Parameter	Description
<i>[options]</i>	The available commands with parameters are listed below.
<i>on</i>	It means to enable IPSec ESP tunnel passthrough and IKE source port (500) preservation.
<i>off</i>	It means to disable IPSec ESP tunnel passthrough and IKE source port (500) preservation.

<i>status</i>	It means to display current status for checking.
---------------	--------------------------------------------------

Example

```
> srv nat ipsecpass status
%% Status: IPsec ESP pass-thru and IKE src_port:500 preservation is OFF.
```

Telnet Command: `srv nat openport`

This command allows users to set open port settings for NAT server.

Syntax

```
srv nat openport n m [-<command> <parameter> | ... ]
```

Syntax Description

Parameter	Description
<i>n</i>	It means the index number for the profiles. The range is from 1 to 20.
<i>m</i>	It means to specify the sub-item number for this profile. The range is from 1 to 10.
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-a <enable>	It means to enable or disable the open port rule profile. 0: disable 1:enable
-c <comment>	It means to type the description (less than 23 characters) for the defined network service.
-i <local ip>	It means to set the IP address for local computer. Local ip: Type an IP address in this field.
-w <idx>	It means to specify the public IP. 1: WAN1 Default, 2: WAN1 Alias 1, ...and so on.
-p <protocol>	Specify the transport layer protocol. Available values are TCP, UDP and ALL.
-s<start port>	It means to specify the starting port number of the service offered by the local host. The range is from 0 to 65535.
-e<end port>	It means to specify the ending port number of the service offered by the local host. The range is from 0 to 65535.
-v	It means to display current settings.
-r <remove>	It means to delete the specified open port setting. remove: Type the index number of the profile.
-f <flush>	It means to return to factory settings for all the open ports profiles.

Example

```
> srv nat openport 1 1 -a 1 -c games -i 192.168.1.100 -w 1 -p TCP -s 23 -e 83
> srv nat openport -v
```



```

%% Status: Enable
%% Comment: games
%% Private IP address: 192.168.1.100
Index  Protocal      Start Port    End Port
*****
  1.    TCP          23           83

%% Status: Disable
%% Comment:
%% Private IP address: 0.0.0.0
Index  Protocal      Start Port    End Port
*****

%% Status: Disable
%% Comment:
%% Private IP address: 0.0.0.0
Index  Protocal      Start Port    End Port
*****
>

```

Telnet Command: `srv nat portmap`

This command allows users to set port redirection table for NAT server.

Syntax

`srv nat portmap add [idx][serv name][proto][pub port][pri ip][pri port][wan1/wan2]`

`srv nat portmap del [idx]`

`srv nat portmap disable [idx]`

`srv nat portmap enable [idx] [proto]`

`srv nat portmap flush`

`srv nat portmap table`

Syntax Description

Parameter	Description
<i>Add[idx]</i>	It means to add a new port redirection table with an index number. Available index number is from 1 to 10.
<i>serv name</i>	It means to type one name as service name.
<i>proto</i>	It means to specify TCP or UDP as the protocol.
<i>pub port</i>	It means to specify which port can be redirected to the specified Private IP and Port of the internal host.
<i>pri ip</i>	It means to specify the private IP address of the internal host providing the service.
<i>pri port</i>	It means to specify the private port number of the service offered by the internal host.
<i>wan1/wan2</i>	It means to specify WAN interface for the port redirection.
<i>del [idx]</i>	It means to remove the selected port redirection setting.
<i>disable [idx]</i>	It means to inactivate the selected port redirection setting.
<i>enable [idx]</i>	It means to activate the selected port redirection setting.
<i>flush</i>	It means to clear all the port mapping settings.

table

It means to display Port Redirection Configuration Table.

Example

```
> srv nat portmap add 1 game tcp 80 192.168.1.11 100 wan1
> srv nat portmap table
```

NAT Port Redirection Configuration Table:

Index	Service Name	Protocol	Public Port	Private IP	Private Port
1	game	6	80	192.168.1.11	100
-1					
2		0	0		-2
3		0	0		-2
4		0	0		-2
5		0	0		-2
6		0	0		-2
7		0	0		-2
8		0	0		-2
9		0	0		-2
10		0	0		-2
11		0	0		-2
12		0	0		-2
13		0	0		-2
14		0	0		-2
15		0	0		-2
16		0	0		-2
17		0	0		-2
18		0	0		-2
19		0	0		-2
20		0	0		-2

Protocol: 0 = Disable, 6 = TCP, 17 = UDP

Telnet Command: `srv nat status`

This command allows users to view NAT Port Redirection Running Table.

Example

```
> srv nat status
```

NAT Port Redirection Running Table:

Index	Protocol	Public Port	Private IP	Private Port
1	6	80	192.168.1.11	100
2	0	0	0.0.0.0	0
3	0	0	0.0.0.0	0
4	0	0	0.0.0.0	0
5	0	0	0.0.0.0	0

6	0	0	0.0.0.0	0
7	0	0	0.0.0.0	0
8	0	0	0.0.0.0	0
9	0	0	0.0.0.0	0
10	0	0	0.0.0.0	0
11	0	0	0.0.0.0	0
12	0	0	0.0.0.0	0
13	0	0	0.0.0.0	0
14	0	0	0.0.0.0	0
15	0	0	0.0.0.0	0
16	0	0	0.0.0.0	0
17	0	0	0.0.0.0	0
18	0	0	0.0.0.0	0
19	0	0	0.0.0.0	0
20	0	0	0.0.0.0	0

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

Telnet Command: `srv nat showall`

This command allows users to view a summary of NAT port redirection setting, open port and DMZ settings.

Example

```
> srv nat showall ?
```

Index	Proto	WAN IP:Port	Private IP:Port	Act

R01	TCP	0.0.0.0:80	192.168.1.11:100	Y
O01	TCP	0.0.0.0:23~83	192.168.1.100:23~83	Y
D01	All	0.0.0.0	192.168.1.96	Y

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

Telnet Command: `switch -i`

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

Syntax

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

Syntax Description

Parameter	Description
<i>switch idx_no</i>	It means the index number of the switch profile.
<i>option</i>	The available commands with parameters are listed below. <i>cmd</i> <i>acc</i> <i>traffic [on/off/status/tx/rx]</i>

<i>cmd</i>	It means to send command to the client.
<i>acc</i>	It means to set the client authentication account and password.
<i>traffic</i> <i>[on/off/status/tx/rx]</i>	It means to turn on/off or display the data transmission from the client.

Example

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

Telnet Command: switch status

This command is used to check if auto discovery for external devices is enabled or disabled.

Example

```
> switch status
External Device auto discovery status : Disable

No Respond to External Device : Enable

>
```

Telnet Command: sys admin

This command is used for RD engineer to access into test mode of Vigor device.

Telnet Command: sys cfg

This command reset the router with factory default settings. When a user types this command, all the configuration will be reset to default setting.

Syntax

sys cfg default

sys cfg status

Syntax Description

Parameter	Description
<i>default</i>	It means to reset current settings with default values.
<i>status</i>	It means to display current profile version and status.

Example

```
> sys cfg status
Profile version: 3.0.0   Status: 1 (0x491e5e6c)
> sys cfg default
>
```

Telnet Command: sys cmdlog

This command displays the history of the commands that you have typed.

Example

```
> sys cmdlog
% Commands Log: (The lowest index is the newest !!!)
 [1] sys cmdlog
 [2] sys cmdlog ?
 [3] sys ?
 [4] sys cfg status
 [5] sys cfg ?
```

Telnet Command: sys ftpd

This command displays current status of FTP server.

Syntax

sys ftpd *on*

sys ftpd *off*

Syntax Description

Parameter	Description
<i>on</i>	It means to turn on the FTP server of the system.
<i>off</i>	It means to turn off the FTP server of the system.

Example

```
> sys ftpd on
% sys ftpd turn on !!!
```

Telnet Command: sys domainname

This command can set and remove the domain name of the system when DHCP mode is selected for WAN.

Syntax

sys domainname [*wan1/wan2*] [*Domain Name Suffix*]

sys domainname [*wan1/wan2*] clear

Syntax Description

Parameter	Description
<i>wan1/wan2</i>	It means to specify WAN interface for assigning a name for it.
<i>Domain Name Suffix</i>	It means the name for the domain of the system. The maximum number of characters that you can set is 40.
<i>clear</i>	It means to remove the domain name of the system.

Example

```
> sys domainname wan1 clever
> sys domainname wan2 intellegent
> sys domainname ?
% sys domainname <wan1/wan2> <Domain Name Suffix (max. 40 characters)>
% sys domainname <wan1/wan2> clear
% Now: wan1 == clever, wan2 ==intelligent
>
```

Telnet Command: sys iface

This command displays the current interface connection status (UP or Down) with IP address, MAC address and Netmask for the router.

Example

```
> sys iface
Interface 0 Ethernet:
Status: UP
IP Address: 192.168.1.1      Netmask: 0xFFFFFFFF00 (Private)
IP Address: 0.0.0.0        Netmask: 0xFFFFFFFF
MAC: 00-50-7F-00-00-00
Interface 4 Ethernet:
Status: DOWN
IP Address: 0.0.0.0        Netmask: 0x00000000
MAC: 00-50-7F-00-00-02
Interface 5 Ethernet:
Status: DOWN
IP Address: 0.0.0.0        Netmask: 0x00000000
MAC: 00-50-7F-00-00-03
Interface 6 Ethernet:
Status: DOWN
IP Address: 0.0.0.0        Netmask: 0x00000000
MAC: 00-50-7F-00-00-04
```

```
Interface 7 Ethernet:
Status: DOWN
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-05
Interface 8 Ethernet:
Status: DOWN
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-06

Interface 9 Ethernet:
Status: DOWN
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-07
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
>
```

Telnet Command: sys name

This command can set and remove the name for the router when DHCP mode is selected for WAN.

Syntax

```
sys name [wan1] [ASCII string]
```

```
sys name [wan1] clear
```

Syntax Description

Parameter	Description
<i>wan1</i>	It means to specify WAN interface for assigning a name for it.
<i>ASCII string</i>	It means the name for router. The maximum character that you can set is 20.

Example

```
> sys name wan1 drayrouter
> sys name ?
% sys name <wan1/wan2> <ASCII string (max. 20 characters)>
% sys name <wan1/wan2> clear
% Now: wan1 == drayrouter, wan2 ==
```

Note: Such name can be used to recognize router's identification in SysLog dialog.

Telnet Command: sys passwd

This command allows users to set password for the administrator.

```
sys passwd [ASCII string]
```

Syntax Description

Parameter	Description
<i>ASCII string</i>	It means the password for administrator. The maximum character that you can set is 23.

Example

```
> sys passwd admin123
>
```

Telnet Command: sys reboot

This command allows users to restart the router immediately.

Example

```
> sys reboot
>
```


Telnet Command: sys autoreboot

This command allows users to restart the router automatically within a certain time.

Syntax

`sys autoreboot [on/off/hour(s)]`

Syntax Description

Parameter	Description
<i>on/off</i>	On - It means to enable the function of auto-reboot. Off - It means to disable the function of auto-reboot.
<i>hours</i>	It means to set the time schedule for router reboot. For example, if you type "2" in this field, the router will reboot with an interval of two hours.

Example

```
> sys autoreboot on
autoreboot is ON
> sys autoreboot 2
autoreboot is ON
autoreboot time is 2 hour(s)
```

Telnet Command: sys commit

This command allows users to save current settings to FLASH. Usually, current settings will be saved in SRAM. Yet, this command will save the file to FLASH.

Example

```
> sys commit
>
```

Telnet Command: sys tftpd

This command can turn on TFTP server for upgrading the firmware.

Example

```
> sys tftpd
% TFTP server enabled !!!
```

Telnet Command: sys cc

This command can display current country code and wireless region of this device.

Example

```
> sys cc
Country Code      : 0x 0 [International]
Wireless Region Code: 0x30
>
```

Telnet Command: sys version

This command can display current version for the system.

Example

```
> sys version
Router Model: VigorNIC 132Vn+   Version: 3.7.4.1 English
Profile version: 3.0.0   Status: 1 (0x49165e6c)
Router IP: 192.168.1.1   Netmask: 255.255.255.0
Firmware Build Date/Time: Mar 20 2014 14:09:50
Router Name: drayrouter
Revision: 40055 2860_374
VDSL2 Firmware Version: 05-04-08-00-00-06
```

Telnet Command: sys qrybuf

This command can display the system memory status and leakage list.

Example

```
> sys qrybuf
System Memory Status and Leakage List

Buf sk_buff ( 200B), used#: 1647, cached#: 30
Buf KMC4088 (4088B), used#: 0, cached#: 8
Buf KMC2552 (2552B), used#: 1641, cached#: 42
Buf KMC1016 (1016B), used#: 7, cached#: 1
Buf KMC504 ( 504B), used#: 8, cached#: 8
Buf KMC248 ( 248B), used#: 26, cached#: 22
Buf KMC120 ( 120B), used#: 67, cached#: 61
Buf KMC56 ( 56B), used#: 20, cached#: 44
Buf KMC24 ( 24B), used#: 58, cached#: 70
Dynamic memory: 13107200B; 4573168B used; 190480B/0B in level 1/2
cache.

FLOWTRACK Memory Status
# of free = 12000
# of maximum = 0
# of flowstate = 12000
# of lost by siganture = 0
# of lost by list = 0
```

Telnet Command: sys pollbuf

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

Syntax

sys pollbuf *[on]*

sys pollbuf *[off]*

Syntax Description

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

<i>off</i>	It means to turn off pulling buffer.
------------	--------------------------------------

Example

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

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

Telnet Command: sys britask

This command can improve triple play quality.

Syntax

`sys britask [on]`

`sys britask [off]`

Syntax Description

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

Example

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

Telnet Command: sys tr069

This command can set CPE settings for applying in VigorACS.

Syntax

`sys tr069 get [parm] [option]`

`sys tr069 set [parm] [value]`

`sys tr069 getnoti [parm]`

`sys tr069 setnoti [parm] [value]`

`sys tr069 log`

`sys tr069 debug [on/off]`

`sys tr069 save`

`sys tr069 inform [event code]`

`sys tr069 port [port num]`

`sys tr069 cert_auth [on/off]`

Syntax Description

Parameter	Description
<i>get [parm] [option]</i>	It means to get parameters for tr-069. option=<nextlevel>: only gets nextlevel for GetParameterNames.

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

Example

```

> sys tr069 get Int. nextlevel
Total number of parameter is 24
Total content length of parameter is 915
InternetGatewayDevice.LANDeviceNumberOfEntries
InternetGatewayDevice.WANDeviceNumberOfEntries
InternetGatewayDevice.DeviceInfo.
InternetGatewayDevice.ManagementServer.
InternetGatewayDevice.Time.
InternetGatewayDevice.Layer3Forwarding.
InternetGatewayDevice.LANDevice.
InternetGatewayDevice.WANDevice.
InternetGatewayDevice.Services.
InternetGatewayDevice.X_00507F_InternetAcc.
InternetGatewayDevice.X_00507F_LAN.
InternetGatewayDevice.X_00507F_NAT.
InternetGatewayDevice.X_00507F_Firewall.
InternetGatewayDevice.X_00507F_Bandwidth.
InternetGatewayDevice.X_00507F_Applications.
InternetGatewayDevice.X_00507F_VPN.
InternetGatewayDevice.X_00507F_VoIP.
InternetGatewayDevice.X_00507F_WirelessLAN.
InternetGatewayDevice.X_00507F_System.
InternetGatewayDevice.X_00507F_Status.

InternetGatewayDevice.X_00507F_Diagnostics.

```

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

Telnet Command: sys sip_alg

This command can turn on/off SIP ALG (Application Layer Gateway) for traversal.

Syntax

```
sys sip_alg [1]
```

```
sys sip_alg [0]
```

Syntax Description

Parameter	Description
1	It means to turn on SIP ALG.
0	It means to turn off SIP ALG.

Example

```
> sys sip_alg ?
usage: sys sip_alg [value]
 0 - disable SIP ALG
 1 - enable SIP ALG
current SIP ALG is disabled
```

Telnet Command: sys diag_log

This command is used for RD debug.

Syntax

```
sys diag_log [status| enable| disable| flush| lineno [w] | level [x] | feature [on/off] [y]/
log]
```

Syntax Description

Parameter	Description
<i>status</i>	It means to show the status of diagnostic log.
<i>enable</i>	It means to enable the function of diag_log.
<i>disable</i>	It means to disenable the function of diag_log.
<i>flush</i>	It means the flush log buffer.
<i>lineno [w]</i>	It means the total lines for displaying message. w - Available value ranges from 100 to 50000.
<i>level[x]</i>	It determines the level of data displayed. x - Available value ranges from 0 to 12. The larger the number is, the detailed the data is displayed.
<i>feature [on/off][y]</i>	It is used to specify the function of the log. Supported features include SYS and DSL (Case-Insensitive). Default setting is "on" for "DSL".
<i>voip_feature [on/off][vf_name]</i>	It means VoIP feature. Type on to enable the feature or type off to disable the feature. vf_name: available settings include DRVTAPI, DRVMMC, DRVMP, DRVFXO, DRVHAL, PSMPHONE, PSMSUPP, PSM, FXO, PSMISDN,

	DTMFPSER, CALLERID (Case-Insensitive).
<i>log</i>	It means the dump log buffer.

Example

```

> sys diag_log status
Status:
diag_log is Enabled.
lineno : 10000.
level : 3.
Enabled feature: SYS DSL
> sys diag_log log
0:00:02 [DSL] Current modem firmware: AnnexA_548006_544401
0:00:02 [DSL] Modem firmware feature: 5, ADSL_A, VDSL2
0:00:02 [DSL] xtseCfg=04 00 04 00 0c 01 00 07
0:00:02 [DSL] don't have last showtime mode!! set next mode to VDSL!!
0:00:02 [DSL] Status has changed: Stopped(0) -> FwWait(3)
0:00:02 [DSL] Status has changed: FwWait(3) -> Starting(1)
0:00:02 [DSL] Status has changed: Starting(1) -> Running(2)
0:00:02 [DSL] Status was switched: firmwareReady(3) to Init(5)
0:00:02 [DSL] Status was switched: Init(5) to Restart(10)
0:00:02 [DSL] Status was switched: Restart(10) to
FirmwareRequest(1)
0:00:02 [DSL] Line state has changed: 00000000 -> 000000FF
0:00:02 [DSL] Entering VDSL2 mode
0:00:03 [DSL] modem code: [05-04-08-00-00-06]
0:00:05 [DSL] Status was switched: FirmwareRequest(1) to
firmwareReady(3)
0:00:05 [DSL] Status was switched: firmwareReady(3) to Init(5)
0:00:05 [DSL] >> nXtseA=0d, nXtseB=00, nXtseV=07, nFwFeatures=5
0:00:05 [DSL] >> nHsToneGroupMode=0, nHsToneGroup=106,
nToneSet=43, nCamState
=2
0:00:05 [DSL] Line state has changed: 000000FF -> 00000100
0:00:05 [DSL] Line state has changed: 00000100 -> 00000200
0:00:05 [DSL] Status was switched: Init(5) to Train(6)

```

Telnet Command: sys daylightsave

This command is used to configure daylight saving setting.

Syntax

sys daylightsave [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
<i>[<command> <parameter> ...]</i>	The available commands with parameters are listed below. <i>[...]</i> means that you can type in several commands in one line.
<i>-v</i>	Show daylight saving setting.
<i>-r</i>	Set to factory default settings.
<i>-e <0/1></i>	Disable/enable daylight saving setting.

	(0: disable, 1:enable)
<code>-t <0/1/2></code>	Set daylight saving type. (0:default, 1:time range, 2:yearly) If "0" is used, Vigor system will use the default settings as daylight saving configuration.
<code>-s <year> <month> <day> <hour></code>	Set the starting point for date range type. <year> : after 2013 <month>: 1 ~ 12 <day>: 1 ~ 31 <hour>: 0 ~ 23 For example, <i>sys daylightsave -s 2014 3 10 12</i>
<code>-d <year> <month> <day> <hour></code>	Set the ending point for date range type. <year> : after 2013 <month>: 1 ~ 12 <day>: 1 ~ 31 <hour>: 0 ~ 23
<code>-y <month> <th weekday> <day in week> <hour></code>	Set the starting point 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 For example, <i>sys daylightsave -y 9 1 0 14</i>
<code>-z <month> <th weekday> <day in week> <hour></code>	Set the ending poring 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 For example, <i>sys daylightsave -z 3 1 6 14</i>

Example

```
> sys daylightsave -y 9 1 0 14
% Start: Yearly on Sep 1th Sun 14:00
> sys daylightsave -z 3 1 6 14
% End: Yearly on Mar 1th Sat 14:00
```

Telnet Command: sys dnsCacheTbl

This command is used to display the content of DNS IPv4 or IPv6 entry and TTL limit value.

Syntax

`sys dnsCacheTbl [-<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.

-l	Show DNS IPv4 entry in the DNS cache table.
-s	Show DNS IPv6 entry in the DNS cache table.
-v	Show TTL limit value in the DNS cache.
-t <tll>	Set TTL limit value in the DNS cache. 0:no limit or "n" seconds (n >= 5)
-c	Clear DNS cache table.

Example

```
> sys dnsCacheTbl -t 20
% Set TTL limit: 20 seconds.
% When TTL larger than 20s , delete the DNS entry in the router's DNS
cache tabl
e.
> sys dnsCacheTbl -v
% TTL limit: 20 seconds
% When TTL larger than 20s , delete the DNS entry in the router's DNS
cache tabl
e.
```

Telnet Command: sys syslog

This command is used to enable /disable saving records on syslog for functions /features (e.g., Firewall, Mail, Save to Syslog Server, and so on).

Syntax

sys syslog -a <enable> [-<command> <parameter> | ...]

Syntax Description

Parameter	Description
[<command> <parameter> ...]	The available commands with parameters are listed below. [...] means that you can type in several commands in one line.
-a <enable>	Enable / disable the SysLog Access Setup. (0: disable, 1:enable)
-s <enable>	Enable / disable Syslog Save to Syslog Server. (0: disable, 1:enable)
-i <ip>	Type the server IP address.
-d <port>	Type the destination port (ranges form 1-65535).
-u <enable>	Enable / disable Syslog Save to USB Disk. (0: disable, 1:enable)
-m <enable>	Enable / disable Mail Syslog. (0: disable, 1:enable)
-f <enable>	Enable / disable Firewall Log. (0: disable, 1:enable)
-v <enable>	Enable / disable VPN Log (0: disable, 1:enable)
-e <enable>	Enable / disable User Access Log. (0: disable, 1:enable)

-c <enable>	Enable / disable Call Log. (0: disable, 1:enable)
-w <enable>	Enable / disable WAN Log. (0: disable, 1:enable)
-r <enable>	Enable / disable Router/DSL Information. (0: disable, 1:enable)
-t <enable>	Enable / disable AlertLog Setup. (0: disable, 1:enable)
-o <port>	Type the AlertLog Port (ranges from 1-65535).

Example

```
> sys syslog -a 1 -s 1 -i 192.168.1.25 -d 514
> sys syslog show
SysLog / Mail Alert Setup : 1
Syslog Save to Syslog Server : 1
Syslog Save to USB Disk : 0
Server IP Address : 192.168.1.25
Destination Port : 514
Mail Syslog : 0
Firewall Log : 1
VPN Log : 1
User Access Log : 1
Call Log : 1
WAN Log : 1
Router/DSL information : 1
AlertLog Setup : 0
AlertLog Port : 514
>
```

Telnet Command: sys time

This command is used to specify time zone for Vigor device system.

Syntax

sys time server <domain>

sys time inquire

sys time show

sys time zone <index>

Syntax Description

Parameter	Description
server <domain>	The max length: 39 bytes.
zone <index>	Definition for "index". 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 73
Set Time Zone OK

> sys time show
***** System Time *****
Current System Time: [2000 Jan 04 Tue 00:16:24]
Time Server: [pool.ntp.org]
Time Zone Index: [73]. GMT+12:00
*****
```

Telnet Command: testmail

This command is used to display current settings for sending test mail.

Example

```
> testmail
Send out test mail
Mail Alert:[Disable]
SMTP_Server:[0.0.0.0]
Mail to:[]
Return-Path:[]
```

Telnet Command: upnp off

This command can close UPnP function.

Example

```
>upnp off
UPNP say bye-bye
```

Telnet Command: upnp on

This command can enable UPnP function.

Example

```
>upnp on
UPNP start.
```

Telnet Command: upnp nat

This command can display IGD NAT status.

Example

```
> upnp nat ?
***** IGD NAT Status *****

((0))
InternalClient >>192.168.1.10<<, RemoteHost >>0.0.0.0<<
InternalPort >>21<<, ExternalPort >>21<<
PortMapProtocol >>TCP<<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
Ftp Example [MICROSOFT]
((1))
InternalClient >>0.0.0.0<<, RemoteHost >>0.0.0.0<<
InternalPort >>0<<, ExternalPort >>0<<
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
0<<

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

Telnet Command: upnp service

This command can display the information of the UPnP service. UPnP service must be enabled first.

Example

```
> upnp on
UPNP start.

> upnp service
>>>> SERVICE TABLE1 <<<<<
  serviceType urn:schemas-microsoft-com:service:OSInfo:1
  serviceId   urn:microsoft-com:serviceId:OSInfo1
  SCPDURL     /upnp/OSInfo.xml
  controlURL  /OSInfo1
  eventURL    /OSInfoEvent1
  UDN         uuid:774e9bbe-7386-4128-b627-001daa843464

>>>> SERVICE TABLE2 <<<<<
```

```

serviceType
urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1
  serviceId urn:upnp-org:serviceId:WANCommonIFC1
  SCPDURL /upnp/WComIFCX.xml
  controlURL /upnp?control=WANCommonIFC1
  eventURL /upnp?event=WANCommonIFC1
  UDN uuid:2608d902-03e2-46a5-9968-4a54ca499148
.
.
.

```

Telnet Command: upnp subscribe

This command can show all UPnP services subscribed.

Example

```

> upnp on
UPNP start.
> upnp subscribe
Vigor> upnp subscribe
>>>> (1) serviceType urn:schemas-microsoft-com:service:OSInfo:1

----- Subscribtion1 -----

sid = 7a2bbdd0-0047-4fc8-b870-4597b34da7fb

eventKey =1, ToSendEventKey = 1

expireTime =6926

active =1

DeliveryURLs
=<http://192.168.1.113:2869/upnp/eventing/twtnpnsiun>

>>>> (2) serviceType
urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1

----- Subscribtion1 -----

sid = d9cd47a5-d9c9-4d3d-8043-d03a82f27983

eventKey =1, ToSendEventKey = 1
.
.
.

```

Telnet Command: upnp tmpvs

This command can display current status of temp Virtual Server of your router.

Example

```
Vigor> upnp tmpvs
```

```

***** Temp virtual server status *****

((0))
real_addr >>192.168.1.10<<, pseudo_addr >>172.16.3.229<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>TCP<<
time >>0<<

((1))
real_addr >>0.0.0.0<<, pseudo_addr >>0.0.0.0<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>0<<
time >>0<<
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
```

Telnet Command: upnp wan

This command is used to specify WAN interface to apply UPnP.

Syntax

upnp wan [*n*]

Syntax Description

Parameter	Description
<i>n</i>	It means to specify WAN interface to apply UPnP. n=0, it means to auto-select WAN interface. n=1, WAN1 n=2, WAN2

Example

```

> upnp wan 1
use wan1 now.
```

Telnet Command: vigbrg on

This command can make the router to be regarded as a modem but not a router.

Example

```

> vigbrg on
%Enable Vigor Bridge Function!
```

Telnet Command: vigbrg off

This command can disable vigor bridge function.

Example

```

> vigbrg off
```

```
%Disable Vigor Bridge Function!
```

Telnet Command: **vigbrg status**

This command can show whether the Vigor Bridge Function is enabled or disabled.

Example

```
> vigbrg status  
%Vigor Bridge Function is enable!  
  
%Wan1 management is disable!
```

Telnet Command: vigbrg cfigip

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 cfigip [*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 cfigip 192.168.1.15
> vigbrg cfigip ?
% Vigor Bridge Config IP,
% Now: 192.168.1.15
```

Telnet Command: vigbrg wan1on

This command is used to enable the bridge WAN1 management.

Example

```
> vigbrg wan1on
%Enable Vigor Bridge Wan1 management!
```

Telnet Command: vigbrg wan1off

This command is used to disable the bridge WAN1 management.

Example

```
> vigbrg wan1off
%Disable Vigor Bridge Wan1 management!
```

Telnet Command: wan ppp_mru

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

Syntax

wan ppp_mru <*WAN interface number*> <*MRU size*>

Syntax Description

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

Example


```

>wan ppp_mru 1 ?
% Now: 1492

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

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

```

Telnet Command: wan mtu / wan mtu2

This command allows users to adjust the size of MTU for WAN1/WAN2.

Syntax

wan mtu *[value]*

wan mtu2 *[value]*

Syntax Description

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

Example

```

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

```

Telnet Command: wan DF_check

This command allows you to enable or disable the function of DF (Don't fragment)

Syntax

wan DF_check *[on]*

wan DF_check *[off]*

Syntax Description

Parameter	Description
<i>on/off</i>	It means to enable or disable DF.

Example

```
> wan DF_check on
%DF bit check enable!
> wan DF_check off
%DF bit check disable (reset DF bit)!
```

Telnet Command: wan disable

This command allows you to disable WAN connection.

Example

```
> wan disable WAN
%WAN disabled.
```

Telnet Command: wan enable

This command allows you to enable WAN connection.

Example

```
> wan enable WAN
%WAN1 enabled.
```

Telnet Command: wan forward

This command allows you to enable or disable the function of WAN forwarding. The packets are allowed to be transmitted between different WANs.

Syntax

`wan forward [on]`

`wan forward [off]`

Syntax Description

Parameter	Description
<i>on/off</i>	It means to enable or disable WAN forward.

Example

```
> wan forward ?
%WAN forwarding is Disable!

> wan forward on
%WAN forwarding is enable!
```

Telnet Command: wan status

This command allows you to display the status of WAN connection, including connection mode, TX/RX packets, DNS settings and IP address.

Example

```
> wan status
WAN1: Offline, stall=N
Mode: ---, Up Time=00:00:00
IP=---, GW IP=---
```

```
TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0
Primary DNS=0.0.0.0, Secondary DNS=0.0.0.0
```

```
PVC_WAN3: Offline, stall=N
Mode: ---, Up Time=00:00:00
IP=---, GW IP=---
TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0
```

```
PVC_WAN4: Offline, stall=N
Mode: ---, Up Time=00:00:00
IP=---, GW IP=---
TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0
```

```
PVC_WAN5: Offline, stall=N
Mode: ---, Up Time=00:00:00
IP=---, GW IP=---
TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0
```

Telnet Command: wan vdsl

This command allows you to configure display current VDSL status and configure the fallback mode for WAN connection.

Syntax

`wan vdsl [show basic]`

`wan vdsl [fbk_mode]`

Syntax Description

Parameter	Description
<code>show basic</code>	It means to display current VDSL status.
<code>fbk_mode</code>	It means to display current status of Fallback Mode used. Available modes to be set as fallback mode include, Auto Vdsl_only Adsl_only

Example

```
> wan vdsl show basic
ADSL
Link Status:    TRAINING
Firmware Version:    05-04-04-04-00-01
ADSL Profile:
Basic  Status  Upstream      Downstream      Unit
Actual Data Rate:    0      0      Kb/s
SNR:    0      0      0.1dB
> wan vdsl fbk_mode vdsl_only
Set VDSL fallback mode to VDSL ONLY
Reboot system to take effect
>
```

Telnet Command: wan detect

This command allows you to configure WAN connection detection. When Ping Detection is enabled (for Static IP or DHCP or PPPoE mode), Router pings specified IP addresses to detect the WAN connection.

Syntax

```
wan detect [wan1/wan2][on/off/always_on]
```

```
wan detect [wan1/wan2] target [ip addr]
```

```
wan detect [wan1/wan2] ttl [value]
```

```
wan detect status
```

Syntax Description

Parameter	Description
<i>on</i>	Enable ping detection. The IP address of the target shall be set.
<i>off</i>	Enable ARP detection (default).
<i>always_on</i>	Disable link detect, always connected(only support static IP)
<i>target</i>	Set the ping target.
<i>ip addr</i>	It means the IP address used for detection. Type an IP address in this field.
<i>ttl</i>	It means to set the ping TTL value (work as trace route) If you do not set any value for ttl here or just type 0 here, the system will use default setting (255) as the ttl value.
<i>status</i>	It means to show the current status.

Example

```
> wan detect status
WAN1: always on
WAN2: off
WAN3: off
WAN4: off
WAN5: off
> wan detect wan1 target 192.168.1.78
Set OK

> wan detect wan1 on
Set OK

> wan detect status
WAN1: on, Target=192.168.1.78, TTL=255
WAN2: off
WAN3: off
WAN4: off
WAN5: off
>
```

Telnet Command: wan lb

This command allows you to Enable/Disable for each WAN to join auto load balance member.

Syntax

wan lb [wan1/wan2/...] on

wan lb [wan1/wan2/...] off

wan lb status

Syntax Description

Parameter	Description
wan1/wan2	Specify which WAN will be applied with load balance.
on	Make WAN interface as the member of load balance.
off	Cancel WAN interface as the member of load balance.
status	Show the current status.

Example

```
> wan lb status
WAN1: on
WAN2: on
WAN3: on
WAN4: on
WAN5: on
```

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.

Syntax

wan mvlan [pvc_no/status/save/enable/disable] [on/off/clear/tag tag_no] [service type/vlan priority] [px ...]

wan mvlan keptag[pvc_no][on/off]

Syntax Description

Parameter	Description
pvc_no	It means index number of PVC. There are 10 PVC, 0(Channel-1) to 9(Channel-9) allowed to be configured. However, bridge mode can be set on PVC number 2 to 9.
status	It means to display the whole Bridge status.
save	It means to save the configuration into flash of Vigor device.
enable/disable	It means to enable/disable the Multi-VLAN function.
on/off	It means to turn on/off bridge mode for the specific channel.
clear	It means to turn off/clear the port.
tag tag_no	It means to tag a number for the VLAN. -1: No need to add tag number. 1-4095: Available setting numbers used as tagged number.
service type	It means to specify the service type for VLAN. 0: Normal. 1: IGMP.
vlan priority	It means to specify the priority for the VALN setting.

	Range is from 0 to 7.
<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 Service Type Tag Priority
-----
7 ON 0 Normal 0(OFF) 0
>
```

Telnet Command: wan multifno

This command allows you to specify a channel (in Multi-PVC/VLAN) to make bridge connection to a specified WAN interface.

Syntax

`wan multifno [channel #] [WAN interface #]`

`wan multifno status`

Syntax Description

Parameter	Description
<i>channel #</i>	There are 4 (?) channels including VLAN and PVC. Available settings are: 1=Channel 1 3=Channel 3 4=Channel 4 5=Channel 5
<i>WAN interface #</i>	Type a number to indicate the WAN interface. 1=WAN1 2=WAN2
<i>status</i>	It means to display current bridge status.

Example

```
> wan multifno 5 1
% Configured channel 5 uplink to WAN1
> wan multifno status
% Channel 3 uplink ifno: 3
% Channel 4 uplink ifno: 3
% Channel 5 uplink ifno: 3
>
```

Telnet Command: wan vlan

This command allows you to configure the VLAN tag of WAN1 or WAN2.

Syntax

`wan vlan wan [#] [adsl/vdsl] tag [value]`

wan vlan wan [#] [adsl/vdsl] [enable/disable]

wan vlan wan [#] [adsl/vdsl] 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>stat</i>	Display current VLAN status.

Example

```
> wan vlan stat

% Interface      Pri      Tag      Enabled
% =====
% WAN1 (ADSL)   0        0
% WAN1 (VDSL)   0        0
>
```