DrayTek

Vigor130

VDSL2/ADSL2/2+ Modem

Your reliable networking solutions partner

User's Guide

V2.0

Vigor130 Series
VDSL2/ADSL2/2+ Modem
User's Guide

Version: 2.0

Firmware version: V3.8.5

(For future update, please visit DrayTek web site)

Date: June 1, 2022

Copyright Information

Copyright Declarations

Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows 7, 8 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 and Approval

Safety Instructions

- Read the installation guide thoroughly before you set up the modem.
- The modem is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the modem yourself.
- Do not place the modem in a damp or humid place, e.g. a bathroom.
- The modem should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.
- Do not expose the modem 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 modem, 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 tore-store 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.

Table of Contents

Introduction

Vigor130 Series is a VDSL2/ADSL2/2+ modem.

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

1.1 Web Configuration Buttons Explanation

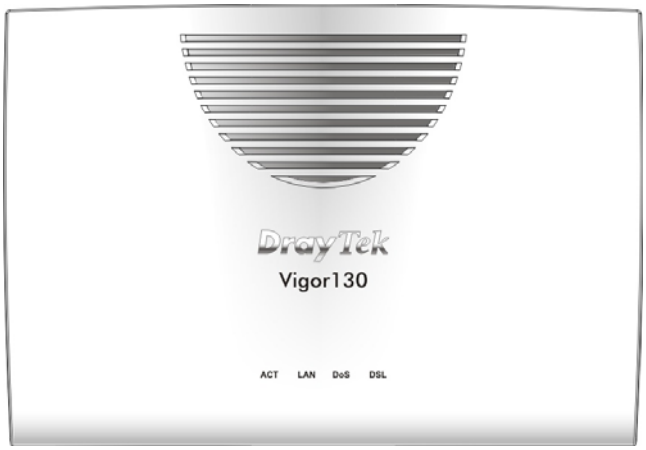
Several main buttons appeared on the web pages are defined as the following:

OK	Save and apply current settings.
Cancel	Cancel current settings and recover to the previous saved settings.
Clear	Clear all the selections and parameters settings, including selection from drop-down list. All the values must be reset with factory default settings.
Add	Add new settings for specified item.
Edit	Edit the settings for the selected item.
Delete	Delete the selected item with the corresponding settings.

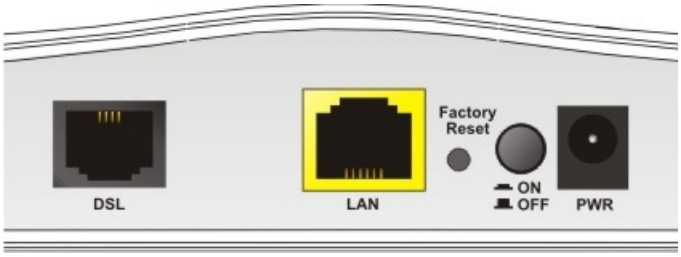
Note: For the other buttons shown on the web pages, please refer to Chapter 4 for detailed explanation.

1.2 LED Indicators and Connectors

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



LED	Status	Explanation
ACT	Off	The system is not ready or is failed.
	Blinking	The system is ready and can work normally.
LAN	On	A normal connection is through its corresponding port.
	Off	LAN is disconnected.
	Blinking	Data is transmitting (sending/receiving).
DoS	On	The DoS/DDoS function is active.
	Blinking	It will blink while detecting an attack.
DSL	On	DSL connection synchronized.
	Blinking	DSL connection is synchronizing.



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

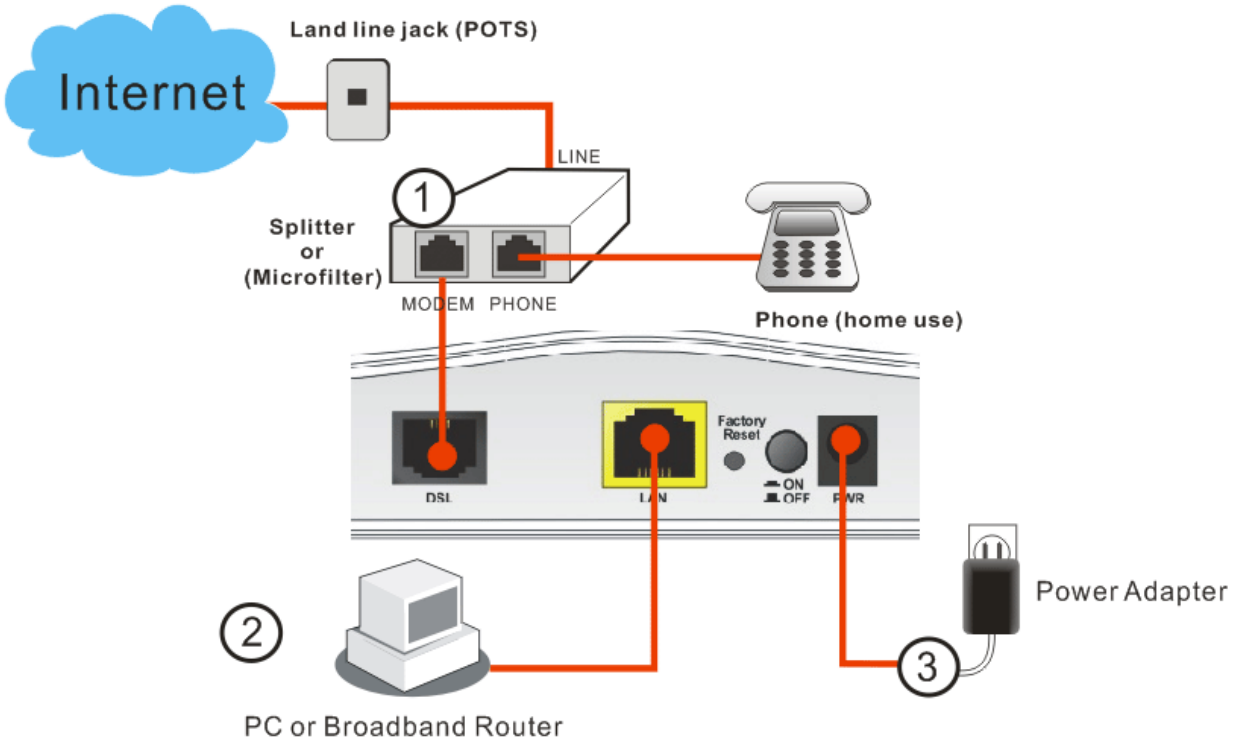
1.3 Hardware Installation

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

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

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

(For the detailed information of LED status, please refer to section 1.2.)



2 Basic Setup

For using the modem properly, it is necessary for you to change the password of web configuration for security and adjust primary basic settings.

2.1 Accessing Web Page

1. Make sure your PC connects to the modem correctly.

> **Notice:** You may either simply set up your computer to get IP dynamically from the modem or set up the IP address of the computer to be the same subnet as **the default IP address of Vigor modem 192.168.1.1**. For the detailed information, please refer to the later section - Trouble Shooting of the guide.

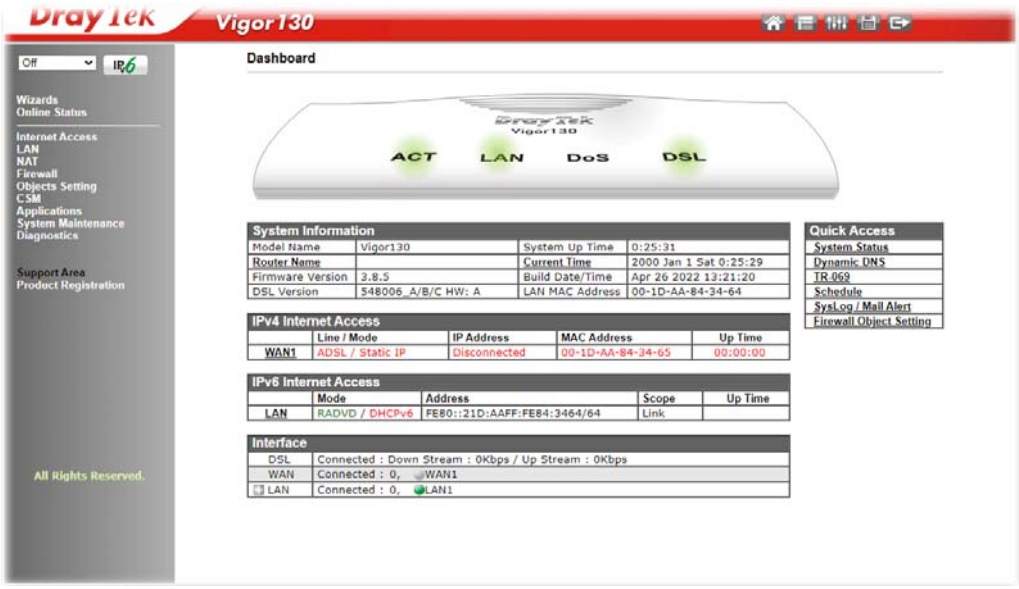
2. Open a web browser on your PC and type **http://192.168.1.1.** A pop-up window will open to ask for username and password. Please type “admin/admin” as the username and password. Then click **Login**.

> **Notice:** If you fail to access to the web configuration, please go to “Trouble Shooting” for detecting and solving your problem.

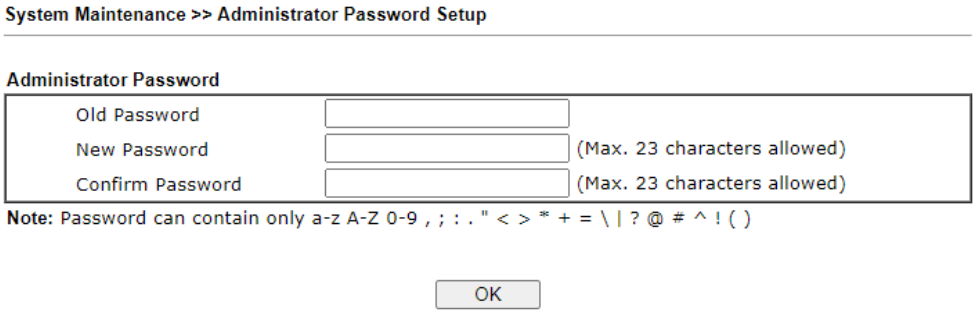
2.2 Changing Password

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

1. Access into the web user interface of Vigor130. The **Main Screen** will appear as below.



2. Go to **System Maintenance** page and choose **Administrator Password/User Password**.



3. Enter the login password (the default is blank) on the field of **Old Password**. Type **New Password**. Then click **OK** to continue.

4. Now, the password has been changed. Next time, use the new password to access the Web User Interface for this modem.

2.3 Quick Start Wizard

Notice: Quick Start Wizard for user operation is the same as for administrator's operation.

The configuration provide here can help you to deploy and use the modem quickly.

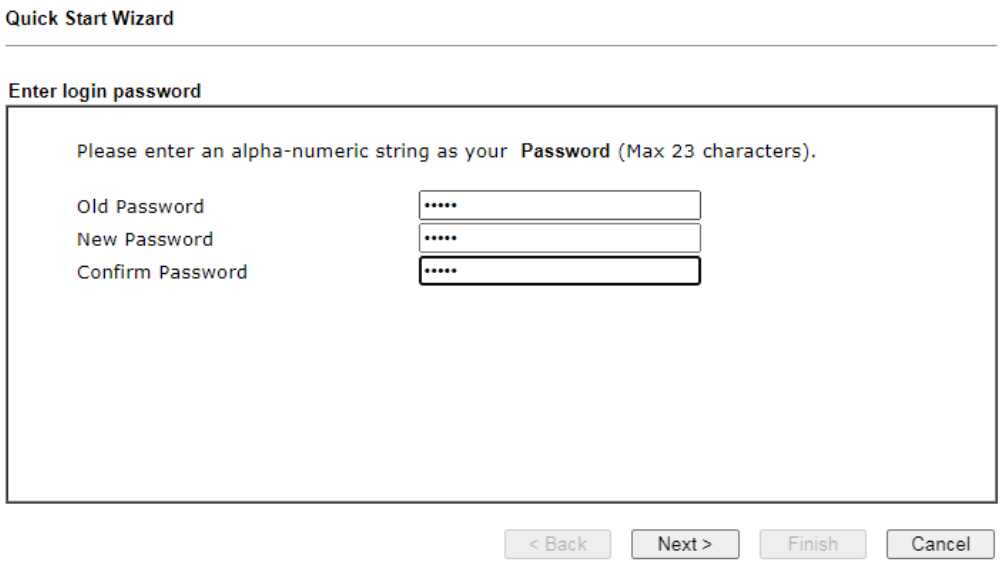
2.3.1 Setting PPPoE/PPPoA Connection

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

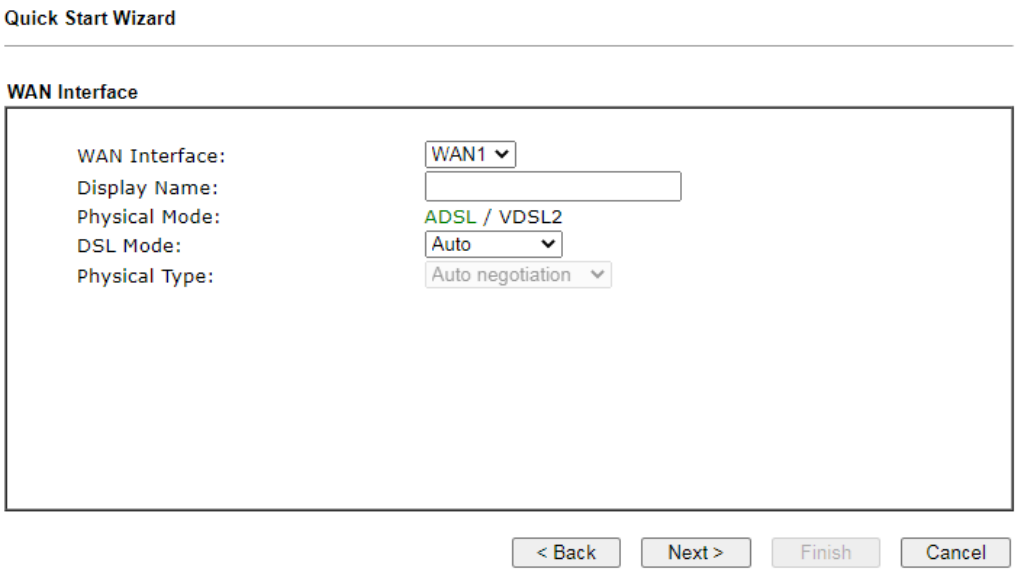
PPPoE is used for most of DSL modem users. All local users can share one PPPoE connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode.

If your ISP provides you the **PPPoE** connection, please select **PPPoE** for this modem.

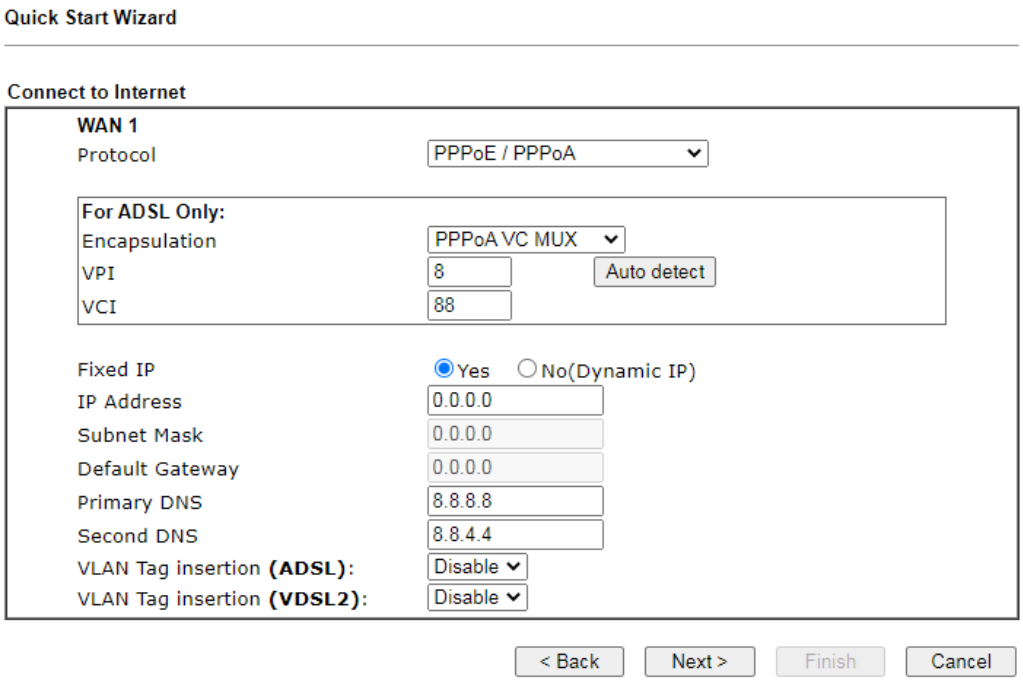
1. Click **Quick Start wizard**.
2. The first screen of **Quick Start Wizard** is entering login password of the web user interface. After typing the password, please click **Next**.



3. On the next page, please select the WAN interface (at present, only WAN1 is available) that you use and specify the DSL mode.



4. You can configure the modem to access the Internet with different protocol/modes such as **PPPoE/PPPoA** or **MPoA/Static or Dynamic IP**. The modem supports the ADSL WAN interface for Internet access. In this case, choose **PPPoE/PPPoA**.

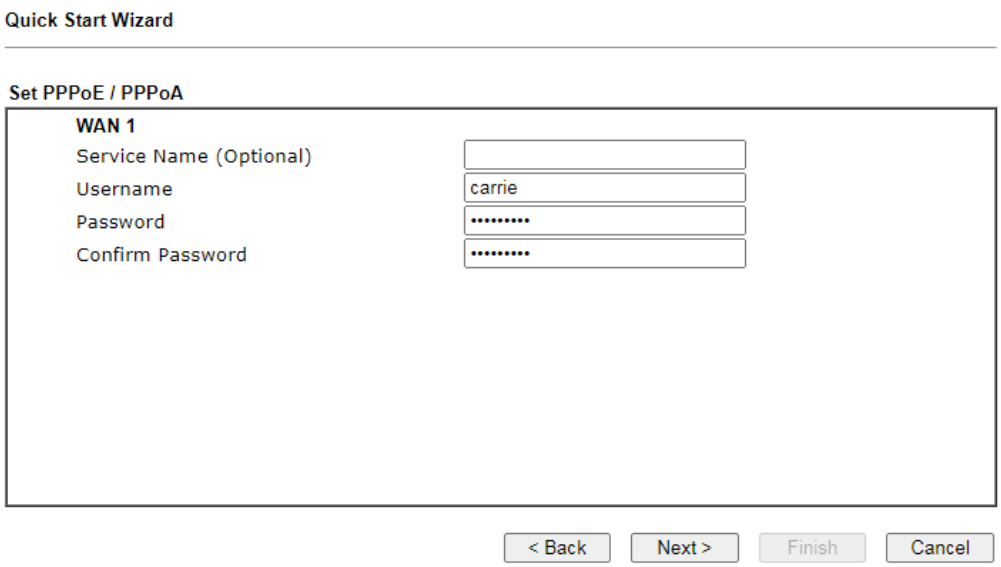


Available parameters are listed below:

Item	Description
For ADSL Only	You have to select an appropriate WAN connection type for connecting to the Internet through this modem according to the settings that your ISP provided. **Auto detect** – Click it to detect suitable values below by the modem automatically.

Item	Description
Encapsulation	Select an IP mode for this WAN interface. There are several available modes for Internet access such as **PPPoE**, **PPPoA.**
VPI	Stands for **Virtual Path Identifier**. It is an 8-bit header inside each ATM cell that indicates where the cell should be routed. The ATM, is a method of sending data in small packets of fixed sizes. It is used for transferring data to client computers.
VCI	Stands for **Virtual Channel Identifier.** It is a 16-bit field inside ATM cell's header that indicates the cell's next destination as it travels through the network. A virtual channel is a logical connection between two end devices on the network.
Fixed IP	Click **Yes** to specify a fixed IP for the modem. Otherwise, click **No (Dynamic IP)** to allow the modem choosing a dynamic IP. If you choose **No**, the following IP Address, Subnet Mask and Default Gateway will not be changed.
IP Address	Assign an IP address for the protocol that you select.
Subnet Mask	Assign a subnet mask value for the protocol of **MPoA/Static or Dynamic IP**.
Default Gateway	Assign an IP address to the gateway for the protocol of **MPoA/Static or Dynamic IP**.
Primary DNS	Assign an IP address to the primary DNS.
Second DNS	Assign an IP address to the secondary DNS.
VLAN Tag insertion	Determines whether 802.1ad VLAN tags will be added to outbound WAN traffic in ADSL/VDSL 2 mode. Check with your ISP to determine if this is required, and if so, the proper tag and priority values to be used. **Enabled** - Tagging enabled. **Disabled -** Tagging disabled. **Tag value -**Value must be between 1 and 4095. **Priority** - Priority code point (PCP). Value must be between 0 and 7.

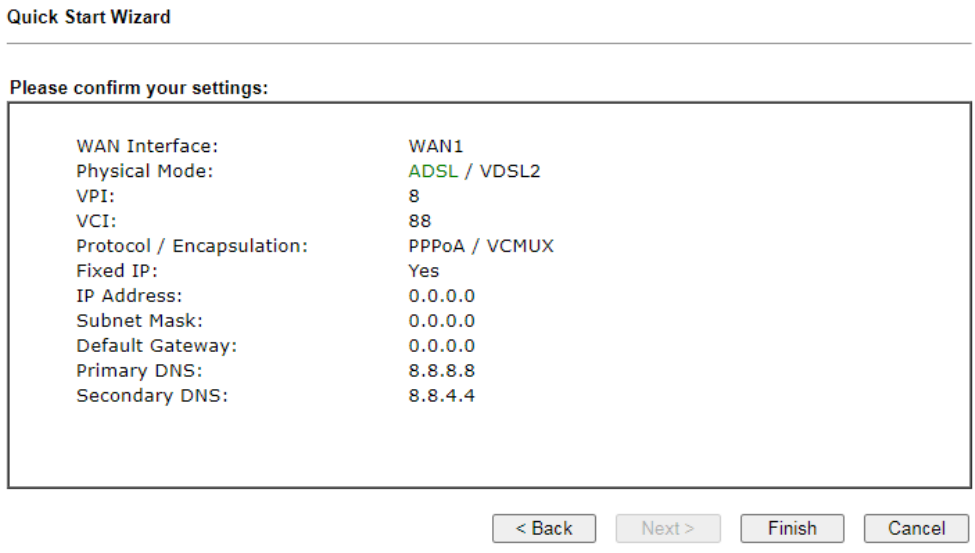
5. After finished the above settings, click **Next** to access into next page.



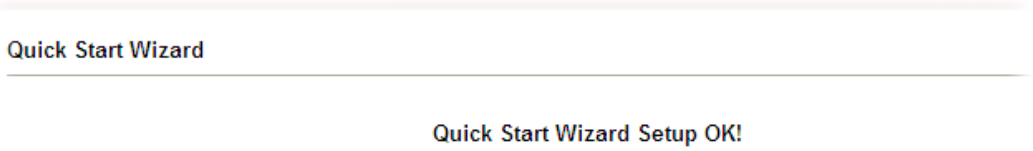
Available parameters are listed below:

Item	Description
User Name	Assign a specific valid user name provided by the ISP. It will be used to access Internet.
Password	Assign a valid password provided by the ISP. It will be used to access Internet.
Confirm Password	Retype the password.

6. Click **Next** for viewing summary of such connection.

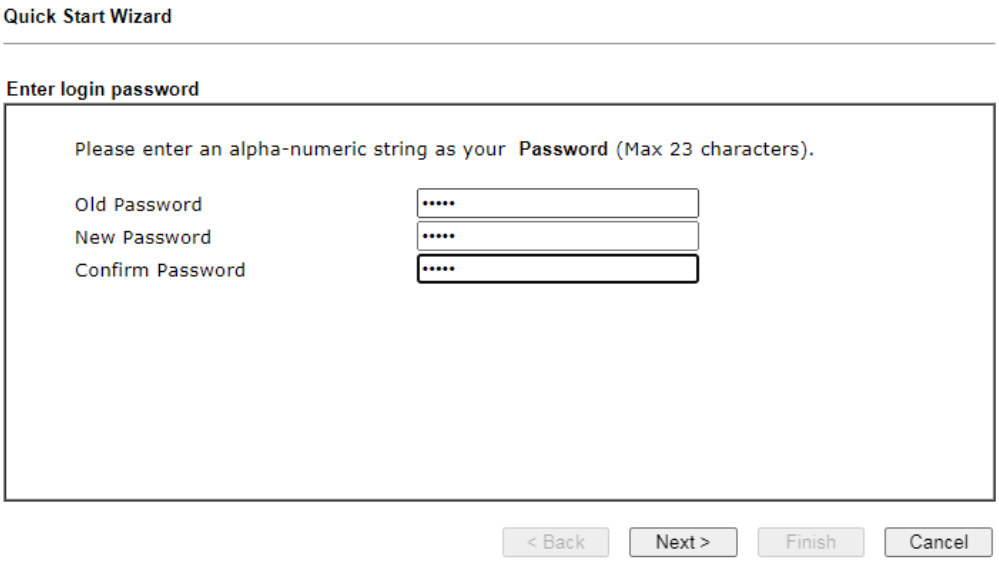


7. Click **Finish.** The Quick Start Wizard Setup OK page will be displayed.

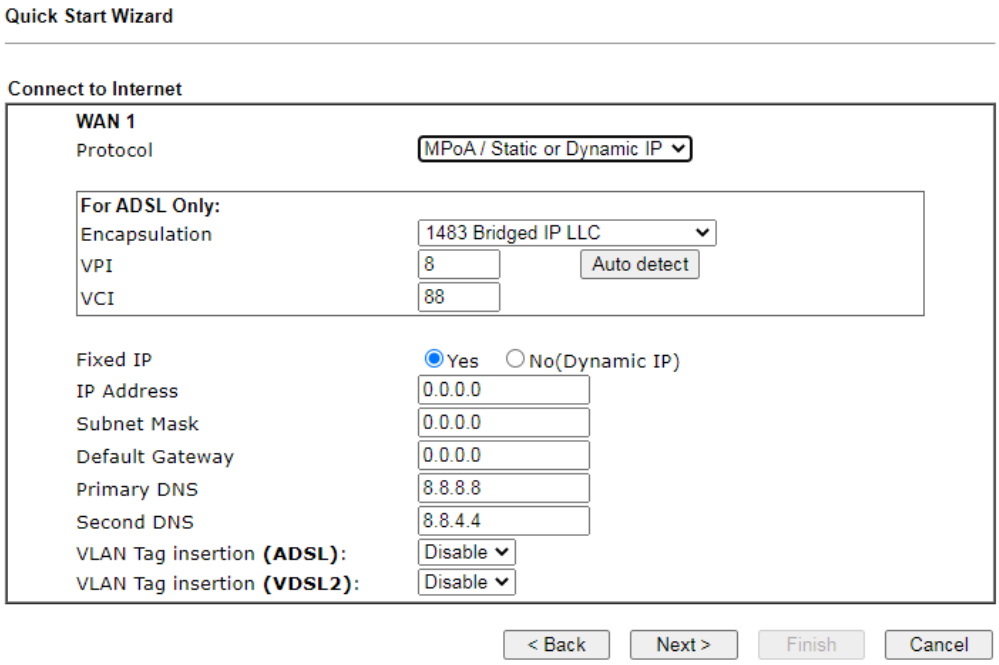


2.3.2 Setting MPoA/Static or Dynamic Connection

1. Click **Quick Start wizard**.
2. The first screen of **Quick Start Wizard** is entering login password of the web user interface. After typing the password, please click **Next**.



3. You can configure the modem to access the Internet with different protocol/modes such as **PPPoE/PPPoA** or **MPoA/Static or Dynamic IP**. The modem supports the ADSL WAN interface for Internet access. In this case, choose MPoA/Static or Dynamic.

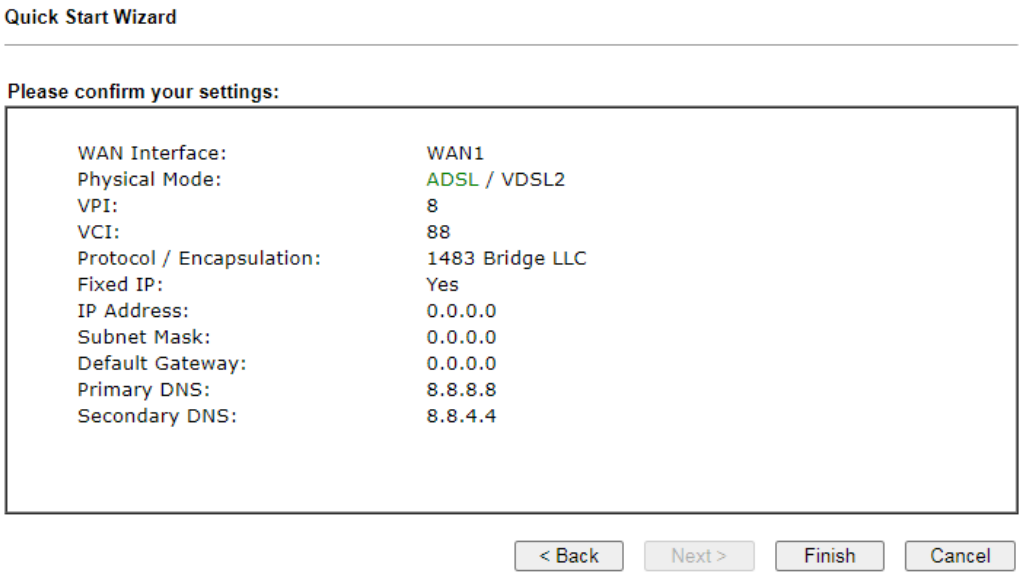


Available parameters are listed below:

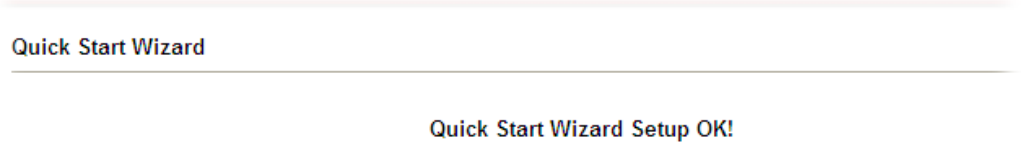
Item	Description
For ADSL Only	You have to select an appropriate WAN connection type for connecting to the Internet through this modem according to the settings that your ISP provided. **Auto detect** – Click it to detect suitable values below by the modem automatically.
Encapsulation	Select an IP mode for this WAN interface. There are several available modes for Internet access such as 1483 Bridged IP or 1483 Routed IP.
VPI	Stands for **Virtual Path Identifier**. It is an 8-bit header inside each ATM cell that indicates where the cell should be routed. The ATM, is a method of sending data in small packets of fixed sizes. It is used for transferring data to client computers.
VCI	Stands for **Virtual Channel Identifier.** It is a 16-bit field inside ATM cell's header that indicates the cell's next destination as it travels through the network. A virtual channel is a logical connection between two end devices on the network.
Fixed IP	Click **Yes** to specify a fixed IP for the modem. Otherwise, click **No (Dynamic IP)** to allow the modem choosing a dynamic IP. If you choose **No**, the following IP Address, Subnet Mask and Default Gateway will not be changed.
IP Address	Assign an IP address for the protocol that you select.

Item	Description
Subnet Mask	Assign a subnet mask value for the protocol of **MPoA/Static or Dynamic IP**.
Default Gateway	Assign an IP address to the gateway for the protocol of **MPoA/Static or Dynamic IP**.
Primary DNS	Assign an IP address to the primary DNS.
Second DNS	Assign an IP address to the secondary DNS.
VLAN Tag insertion	Determines whether 802.1ad VLAN tags will be added to outbound WAN traffic in ADSL/VDSL 2 mode. Check with your ISP to determine if this is required, and if so, the proper tag and priority values to be used. **Enabled** - Tagging enabled. **Disabled** - Tagging disabled. **Tag value** -Value must be between 1 and 4095. **Priority** - Priority code point (PCP). Value must be between 0 and 7.

4. Click **Next** for viewing summary of such connection.

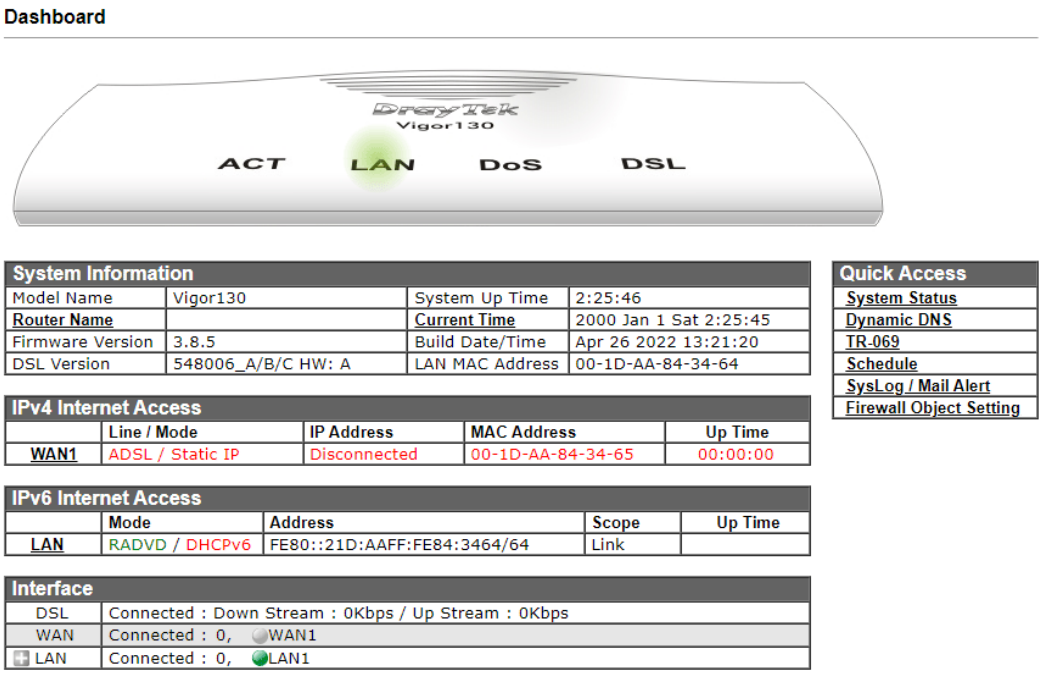


5. Click **Finish.** The Quick Start Wizard Setup OK page will be displayed.



2.4 Introducing Dashboard

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



2.4.1 Virtual Panel

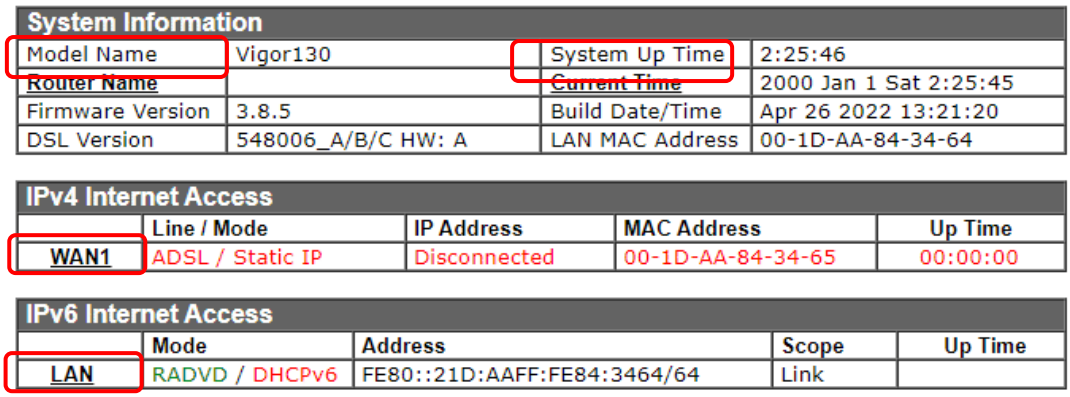
On the top of the Dashboard, a virtual panel (simulating the physical panel of the modem) displays the physical interface connection. It will be refreshed every five seconds.

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

For detailed information about the LED display, refer to **1.2 LED Indicators and Connectors**.

2.4.2 Name with a Link

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



System Information			
Model Name	Vigor130	System Up Time	2:25:46
Router Name		Current Time	2000 Jan 1 Sat 2:25:45
Firmware Version	3.8.5	Build Date/Time	Apr 26 2022 13:21:20
DSL Version	548006_A/B/C HW: A	LAN MAC Address	00-1D-AA-84-34-64

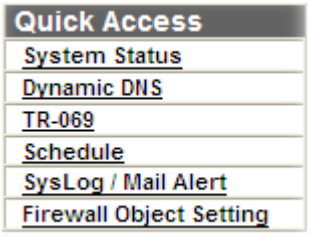
IPv4 Internet Access				
	Line / Mode	IP Address	MAC Address	Up Time
WAN1	ADSL / Static IP	Disconnected	00-1D-AA-84-34-65	00:00:00

IPv6 Internet Access				
	Mode	Address	Scope	Up Time
LAN	RADVD / DHCPv6	FE80::21D:AAFF:FE84:3464/64	Link	

2.4.3 Quick Access for Common Used Menu

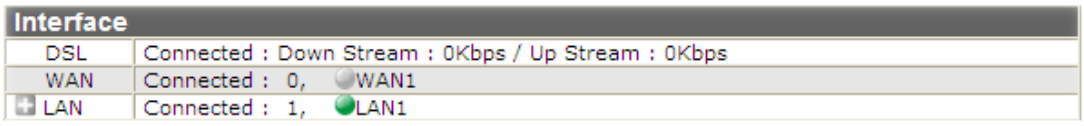
All the menu items can be accessed and arranged orderly on the left side of the main page for your request. However, some **important** and **common** used menu items which can be accessed in a quick way just for convenience.

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



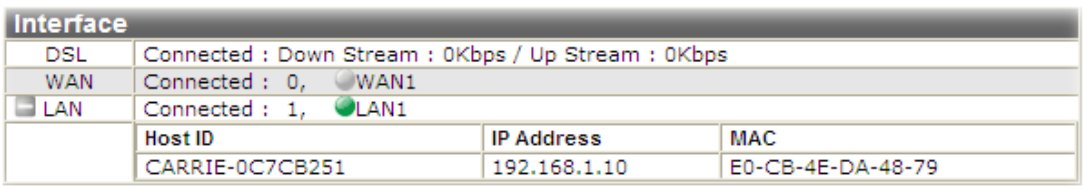
The function links of System Status, Dynamic DNS, TR-069, Schedule, Syslog/Mail Alert, and Firewall Object Setting are displayed here. Move your mouse cursor on any one of the links and click on it. The corresponding setting page will be open immediately.

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



Interface	
DSL	Connected : Down Stream : 0Kbps / Up Stream : 0Kbps
WAN	Connected : 0, WAN1
LAN	Connected : 1, LAN1

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



Interface			
DSL	Connected : Down Stream : 0Kbps / Up Stream : 0Kbps		
WAN	Connected : 0, WAN1		
LAN	Connected : 1, LAN1		
	Host ID	IP Address	MAC
	CARRIE-0C7CB251	192.168.1.10	E0-CB-4E-DA-48-79

2.4.4 GUI Map

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

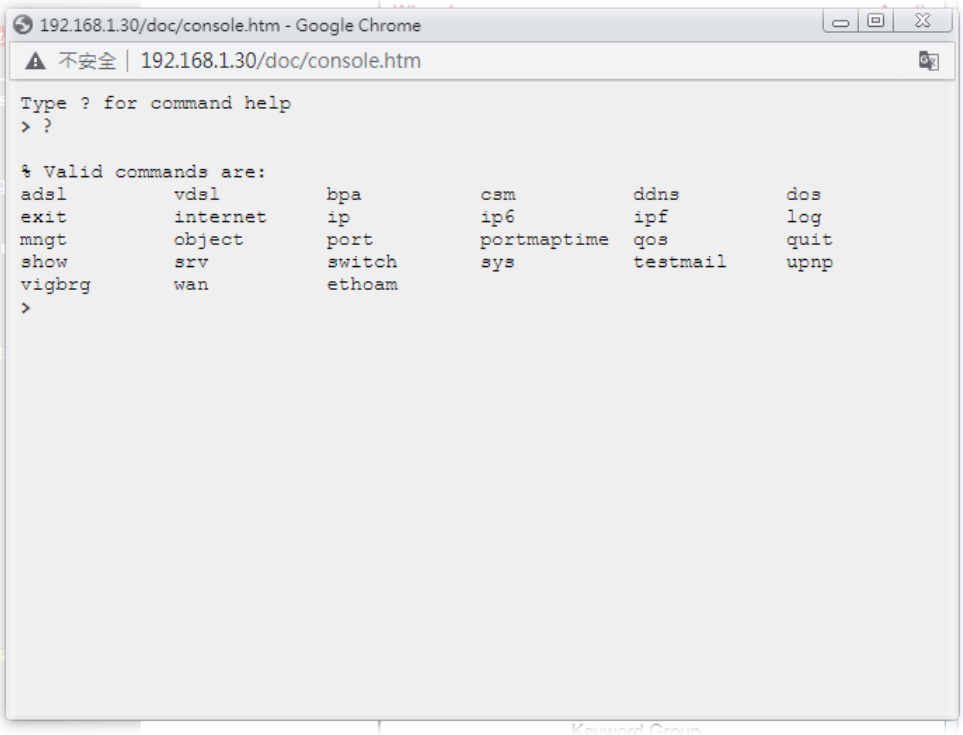
GUI Map

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

2.4.5 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.



2.4.6 Config Backup

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

Simply click the icon on the top of the main screen to save the settings.

2.4.7 Logout

Click the **Logout** icon to exit the web user interface.

2.5 Online Status

2.5.1 Physical Connection

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

If you select **PPPoE** as the protocol, you will find out a link of **Dial PPPoE** or **Drop PPPoE** in the Online Status web page.The online status shows the system status, WAN status, ADSL Information and other status related to this modem within one page. If you select **PPPoE/PPPoA** as the protocol, you will find out a link of **Dial PPPoE** or **Drop PPPoE** in the Online Status web page.

Physical Connection for IPv4 Protocol

Online Status

Physical Connection — System Uptime: 0:2:57

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	1851

WAN Status — >> Renew

Enable	Line	Name	Mode	Up Time	
Yes	ADSL		DHCP Client	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

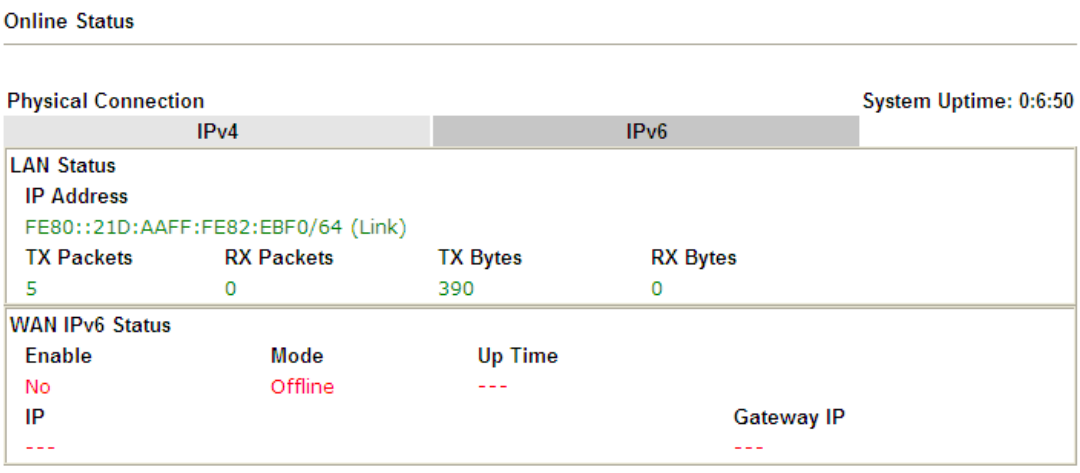
ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
		TRAINING	0	0	0	0

Detailed explanation is shown below:

Item	Description
LAN Status	**Primary DNS**-Display the primary DNS server address for WAN interface. **Secondary DNS** -Display the secondary DNS server address for WAN interface. **IP Address**-Display the IP address of the LAN interface. **TX Packets**-Display the total transmitted packets at the LAN interface. **RX Packets**-Display the total received packets at the LAN interface.
WAN Status	**Enable – Yes** in red means such interface is available but not connected. **Yes** in green means such interface is connected.

Item	Description
	Line – Display the physical connection of this interface. **Name** – Display the name of the modem. **Mode** - Display the type of WAN connection (e.g., PPPoE). **Up Time** - Display the total uptime of the interface. **IP** - Display the IP address of the WAN interface. **GW IP** - Display the IP address of the default gateway. **TX Packets** - Display the total transmitted packets at the WAN interface. **TX Rate** - Display the speed of transmitted octets at the WAN interface. **RX Packets** - Display the total number of received packets at the WAN interface. **RX Rate** - Display the speed of received octets at the WAN interface.
ADSL Information	**ATM Statistics –** Display the ATM layer information. **TX Cells –**Display the total number of ATM transmission cells. **RX Cells –**Display the total number of ATM received cells. **TX CRC errs –** Display the total number of transmission CRC errors. **RX CRC errs –**Display the total number of CRC errors received. **ADSL Status –**Display the ADSL layer information. **Mode –** Display the type of ADSL mode, such as T1.413, G.DMT, ADSL2+(G.992.5), and so on. **State –** Display the ADSL connection status, such as Ready, HANDSHAKING, SHOWTIME and so on. **Up Speed –** Display the upstream rate. **Down Speed –** Display the downstream rate. **SNR Margin –** Display number of SRR Margin. **Loop Att .-** Display the number of Loop Attenuation.

Physical Connection for IPv6 Protocol



Detailed explanation (for IPv6) is shown below:

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

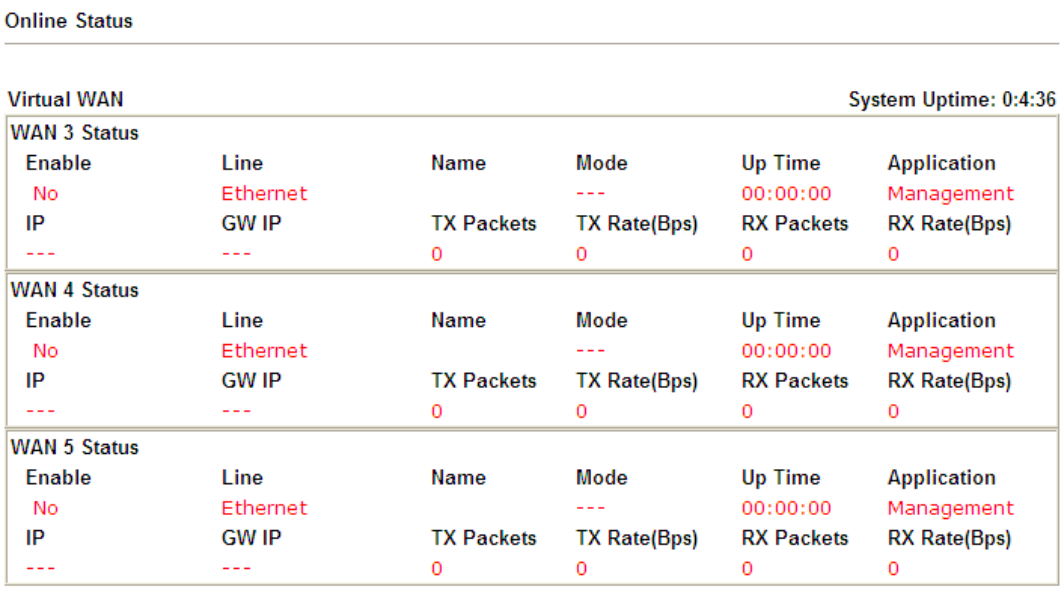
Note: The words in green mean that the WAN connection of that interface (WAN1) is ready for accessing Internet; the words in red mean that the WAN connection of that interface (WAN1) is not ready for accessing Internet.

2.5.2 Virtual WAN

Such page displays the virtual WAN connection information.

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

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



Detailed explanation is shown below:

Item	Description
WAN Status	**Enable – Yes** in red means such interface is available but not enabled. **Yes** in green means such interface is enabled. **Line** – Display the physical connection (Ethernet, or USB) of this interface. **Name** – Display the name of the modem. **Mode** - Display the type of WAN connection (e.g., PPPoE). **Up Time** - Display the total uptime of the interface. **IP** - Displays the IP address of the WAN interface. **GW IP** - Display the IP address of the default gateway. **TX Packets** - Display the total transmitted packets at the WAN interface. **TX Rate** - Display the speed of transmitted octets at the WAN interface. **RX Packets** - Display the total number of received packets at the WAN interface. **RX Rate** - Display the speed of received octets at the WAN interface.

2.6 Saving Configuration

Each time you click **OK** on the web page for saving the configuration, you can find messages showing the system interaction with you.

Ready indicates the system is ready for you to input settings.

Settings Saved means your settings are saved once you click **Finish** or **OK** button.

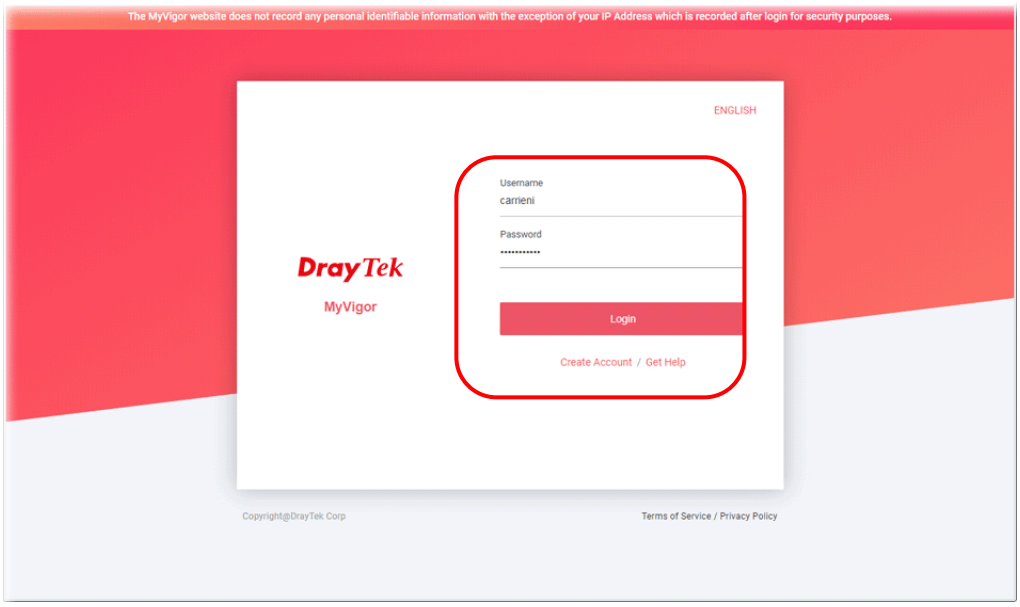
2.7 Registering Vigor130

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

1 Again, login the web configuration interface of Vigor modem by typing "**admin/admin**" as User Name / Password.

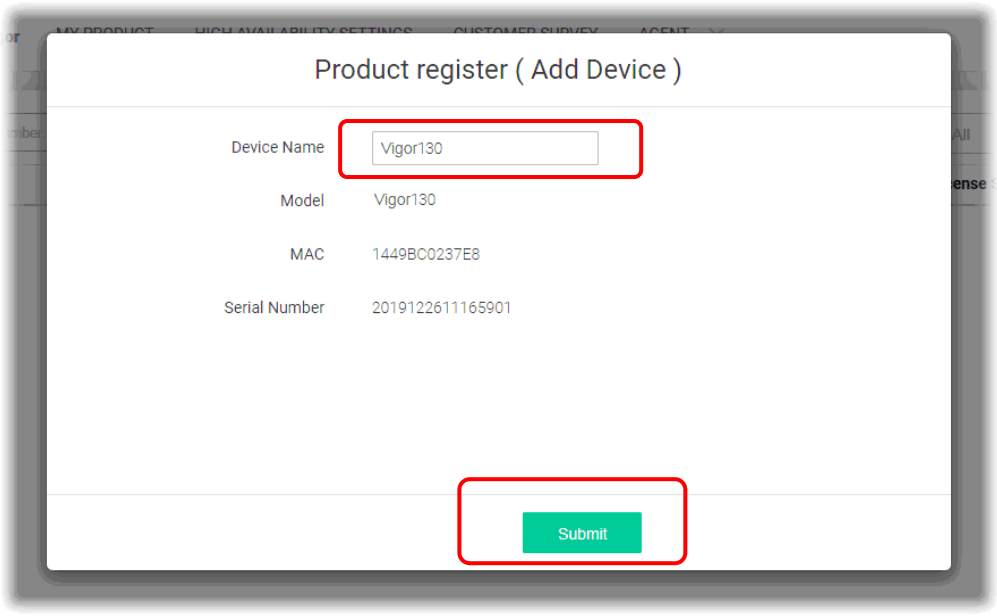
2 Click **Support Area>>Production Registration** from the home page.

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

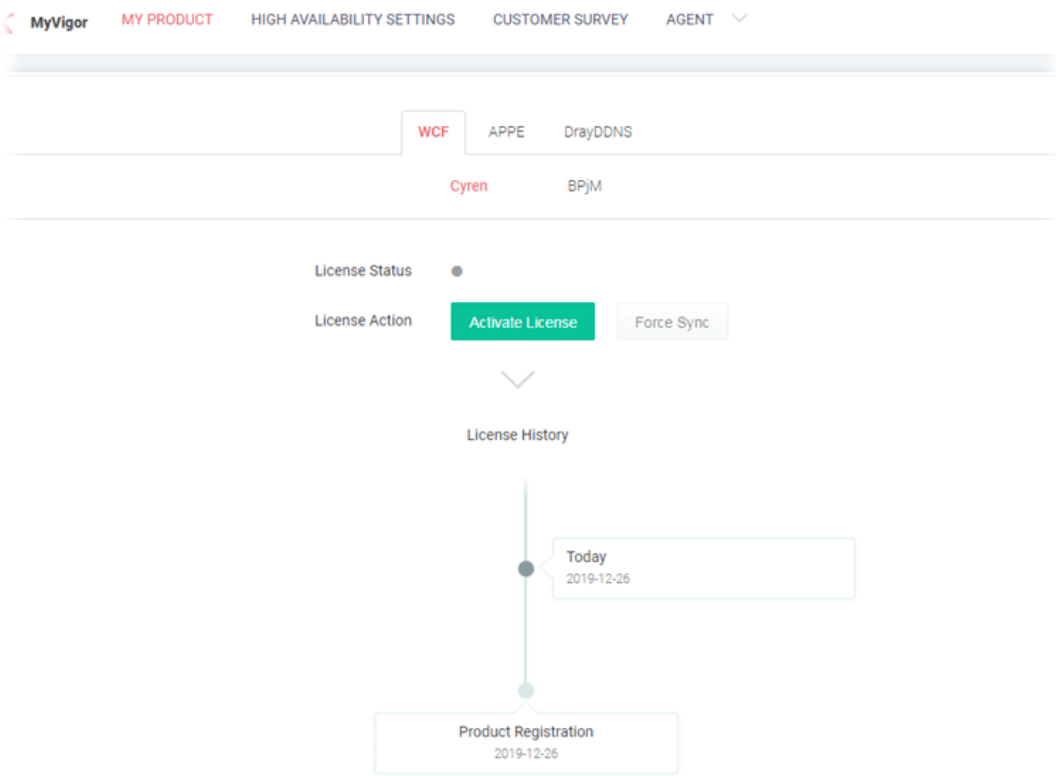


If you haven't an accessing account, please refer to section Creating an Account for MyVigor to create your own one. Please read the articles on the Agreement regarding user rights carefully while creating a user account.

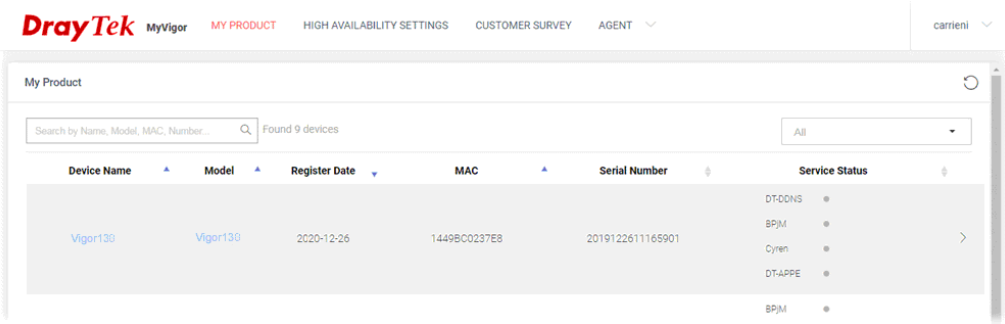
4 The following page will be displayed after you logging in MyVigor. Type a nickname for the router, then click **Submit**.



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



6 Clicking **MYPRODUCT** for viewing the general information of the registered router on MyVigor website.



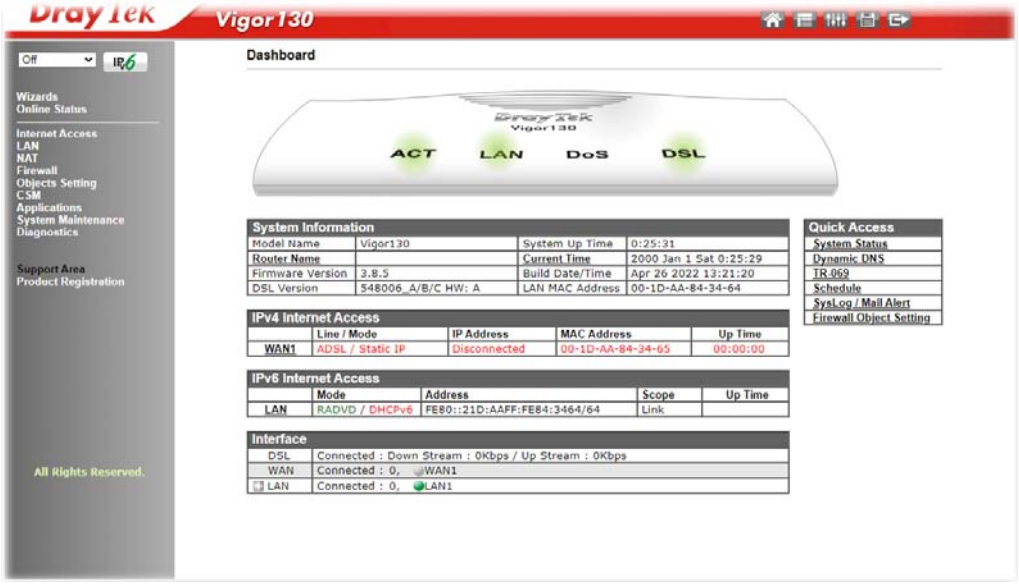
This page is left blank.

3 Web Configuration

This chapter will guide users to execute advanced (full) configuration. As for other examples of application, please refer to chapter 5.

1. Open a web browser on your PC and type **http://192.168.1.1.** The window will ask for typing username and password.
2. Please type “admin/admin” on Username/Password for administration operation.

Now, the **Main Screen** will appear. Note that “Admin mode” will be displayed on the bottom left side.



3.1 Internet Access

Quick Start Wizard offers user an easy method to quick setup the connection mode for the modem. Moreover, if you want to adjust more settings for different WAN modes, please go to **WAN** group and click the **Internet Access** link.

3.1.1 Basics of Internet Protocol (IP) Network

IP means Internet Protocol. Every device in an IP-based Network including modems, 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 modem 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

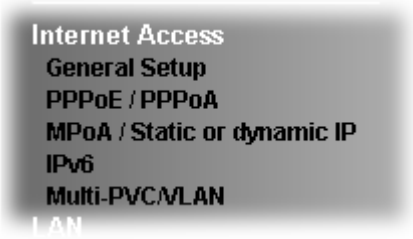
As the modem plays a role to manage and further protect its LAN, it interconnects groups of host PCs. Each of them has a private IP address assigned by the built-in DHCP server of the Vigor modem. The modem itself will also use the default **private IP** address: 192.168.1.1 to communicate with the local hosts. Meanwhile, Vigor modem 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 modem 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.

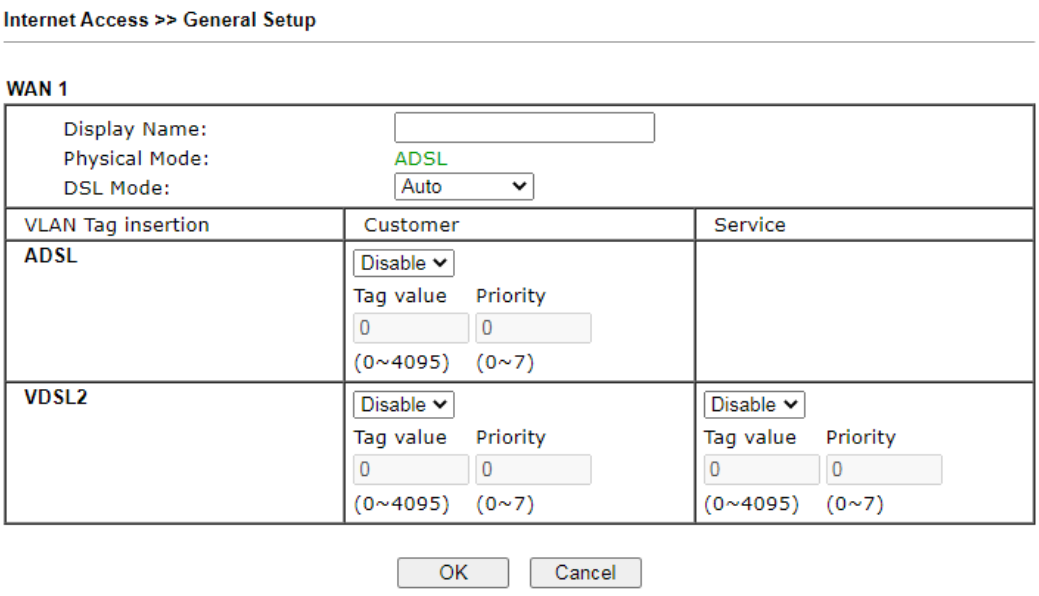
When a modem begins to connect to your ISP, a serial of discovery process will occur to ask for a connection. Then a session will be created. Your user ID and password is authenticated via **PAP** or **CHAP** with **RADIUS** authentication system. And your IP address, DNS server, and other related information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

Below shows the menu items for Internet Access.

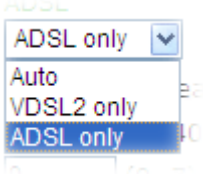


3.1.2 General Setup

This section will introduce some general settings of Internet.



Available settings are explained as follows:

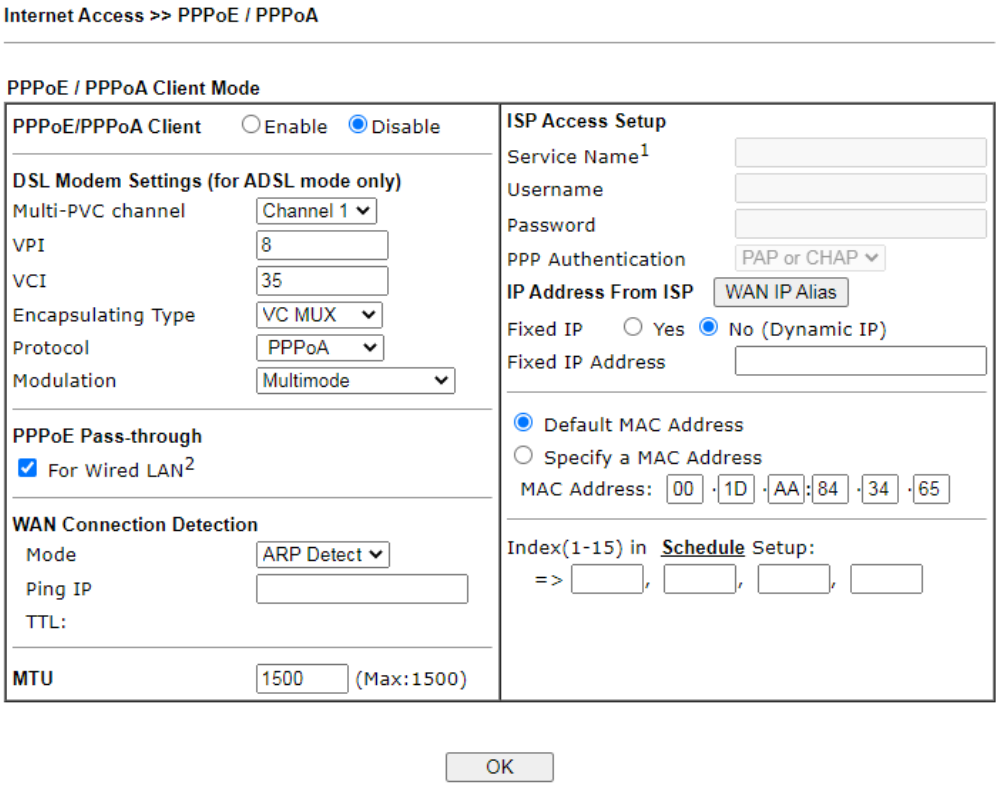
Item	Description
Display Name	Type the description for such WAN interface.
Physical Mode	Display the physical mode of such WAN interface.
DSL Mode	Specify which DSL mode can be used for such WAN connection. **Auto** – The system will choose the suitable one automatically. 
Line Speed	If your choose **According to Line Speed** as the **Load Balance Mode**, please type the line speed for downloading and uploading for such WAN interface. The unit is kbps.
VLAN Tag insertion	**Enable** – Enable the function of VLAN with tag. The modem 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.

3.1.3 PPPoE/PPPoA

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

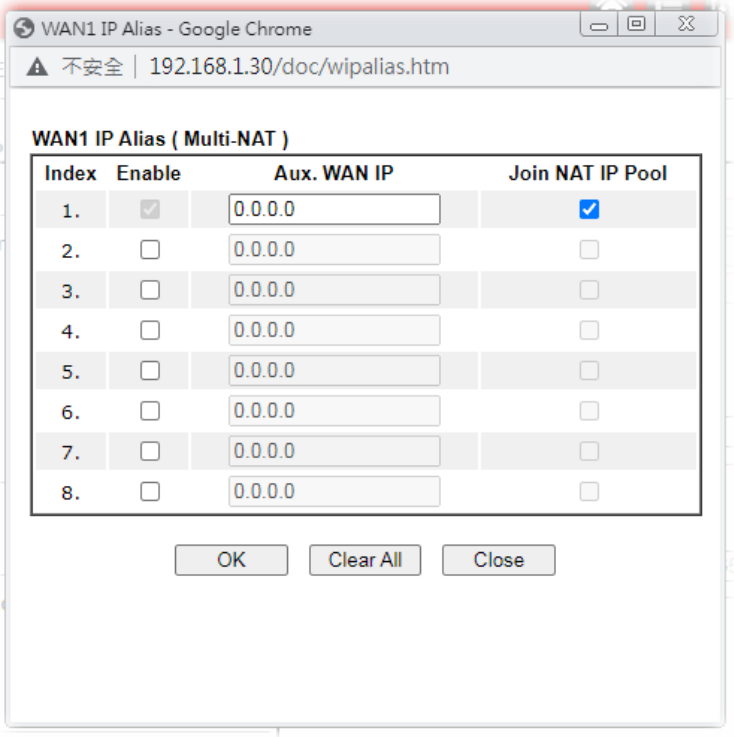
To choose PPPoE or PPPoA as the accessing protocol of the internet, please select **PPPoE/PPPoA** from the **Internet Access** menu. The following web page will be shown.



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.
DSL Modem Settings	Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP. **Multi-PVC channel** - The selections displayed here are determined by the page of **Internet Access** >> **Multi-PVC/VLAN**. **VPI** - Type in the value provided by ISP. **VCI** - Type in the value provided by ISP. **Encapsulating Type** - Drop down the list to choose the type provided by ISP. **Protocol** - Drop down the list to choose the protocol, PPPoE or PPPoA. **Modulation** – Choose a suitable method for PPPoE/PPoA connection.
PPPoE Pass-through	The modem offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor modem. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction. **For Wired LAN** – If you check this box, PCs on the same network can use another set of PPPoE session (different with

	the Host PC) to access into Internet. However, if this box is checked in PPPoA protocol, only PPPoE clients on the LAN will be served and only one session is allowed.
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. **Ping IP** – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. **TTL (Time to Live)** – Displays value for your reference. TTL value is set by telnet command.
MTU	It means Max Transmit Unit for packet. The default setting will be 1500.
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP. If you want to connect to Internet all the time, you can check **Always On**. **ISP Name –** Type the name of the ISP if required. **Username** – Type in the username provided by ISP in this field. **Password** – Type in the password provided by ISP in this field. **PPP Authentication** – Select **PAP only** or **PAP or CHAP** for PPP. **Always On** - If you want to connect to Internet all the time, check the **Always On** box. **Idle Timeout** – Set the timeout for breaking down the Internet after passing through the time without any action. This setting is active only when the **Active on demand** option for Active Mode is selected in **WAN>> General Setup** page.
IP Address From ISP	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. **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.



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

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

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

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

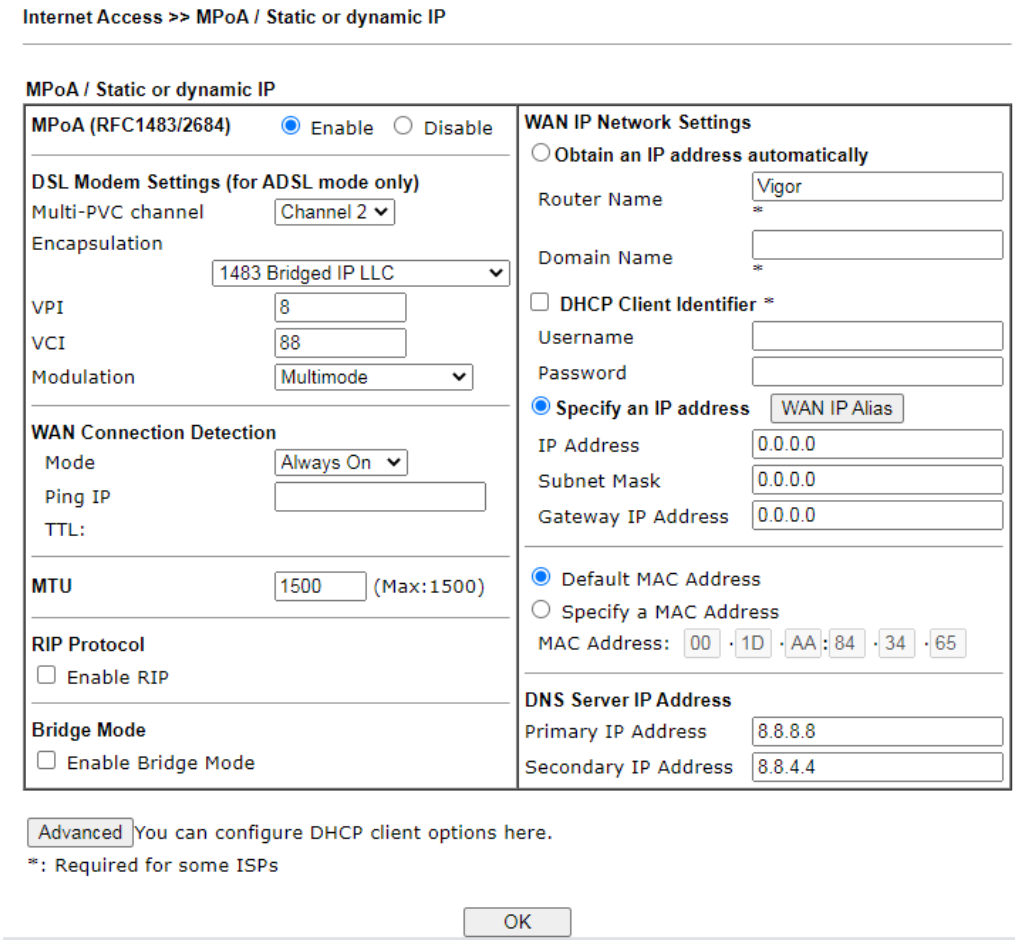
After finishing all the settings here, please click **OK** to activate them.

3.1.4 MPoA /Static or dynamic IP

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

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

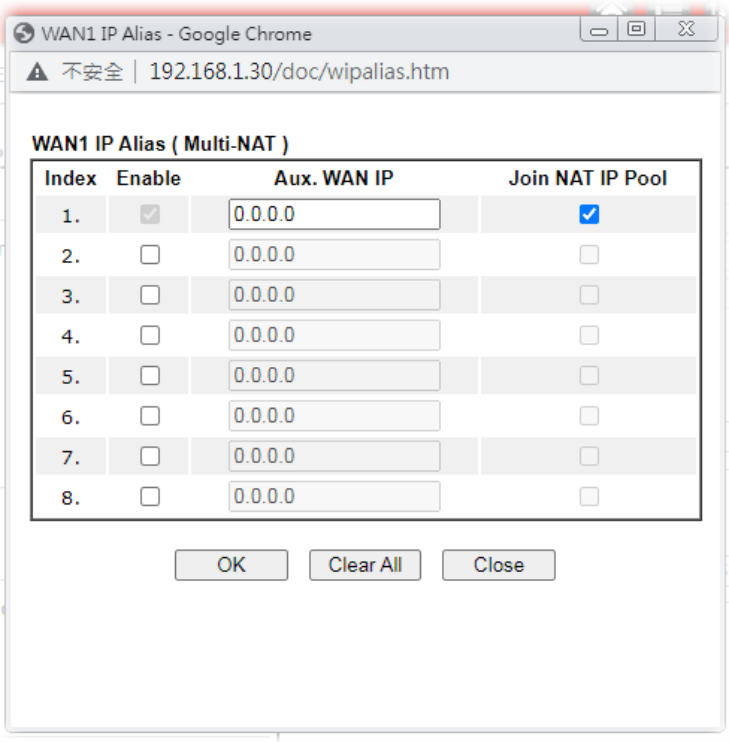
To use **MPoA /Static or dynamic IP** as the accessing protocol of the Internet, select **MPoA** mode. The following web page will appear.



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.
DSL Modem Settings	Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP. **Multi-PVC channel** - The selections displayed here are determined by the page of **Internet Access** – **Multi PVCs**. **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** – Choose a suitable method for such connection.
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. **Ping IP** – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. **TTL (Time to Live)** – Displays value for your reference. TTL

	value is set by telnet command.
MTU	It means Max Transmit Unit for packet.
RIP Protocol	Routing Information Protocol is abbreviated as RIP(RFC1058) specifying how modems exchange routing tables information. Click **Enable RIP** for activating this function.
Bridge Mode	If you choose **Bridged IP** as the protocol, you can check this box to invoke the function. The modem 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. **Obtain an IP address automatically** – Click this button to obtain the IP address automatically. **Modem Name** – Type in the modem name provided by ISP. **Domain Name** – Type in the domain name that you have assigned.
DHCP Client Identifier for some ISP	This feature is offered for certain ISP with special request. **Enable** – Check this box to enable the function of DHCP client identifier for some ISP. **Username** – Type a username used for such function. **Password** – Type a password used for such function.
Specify an IP address	Click this radio button to specify some data. **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.

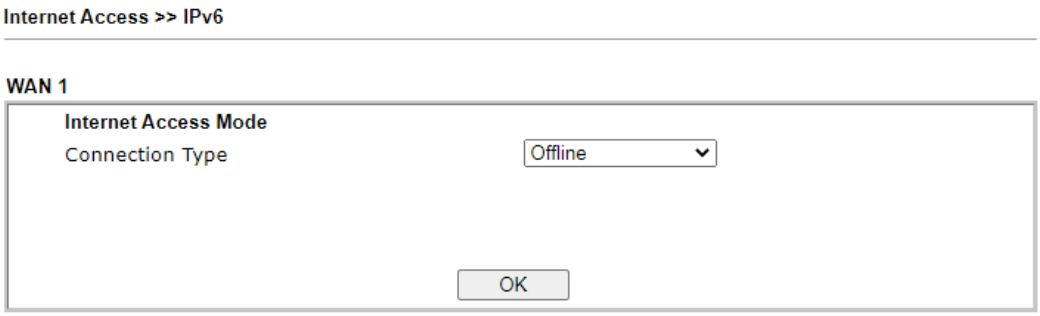
	 **IP Address** – Type in the private IP address. **Subnet Mask** – Type in the subnet mask. **Gateway IP Address** – Type in gateway IP address.
Default MAC Address	Type in MAC address for the modem. You can use **Default MAC Address** or specify another MAC address for your necessity. **MAC Address** – Type in the MAC address for the modem manually.
DNS Server IP Address	Type in the primary IP address for the modem. If necessary, type in secondary IP address for necessity in the future.

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

3.1.5 IPv6

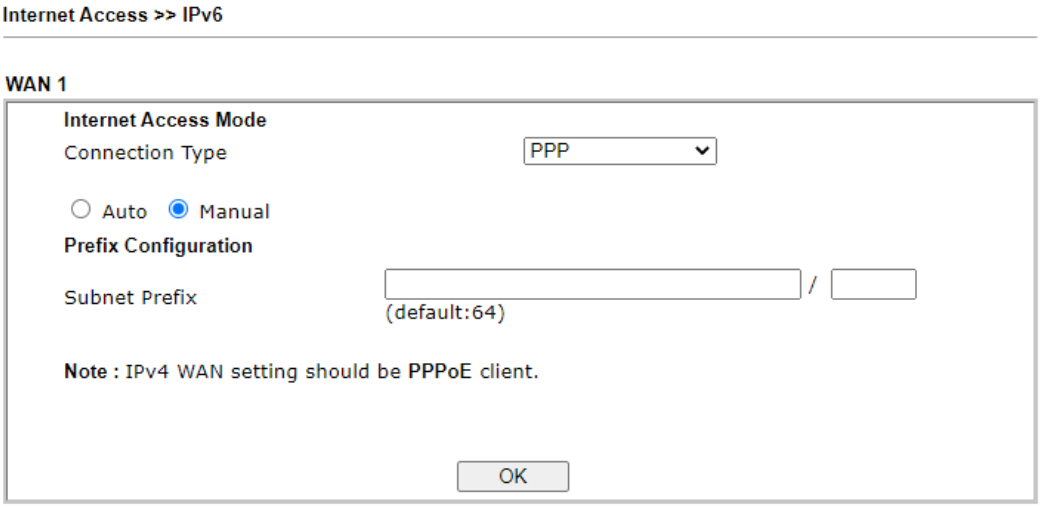
Offline

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



PPP

During the procedure of IPv4 PPPoE connection, we can get the IPv6 Link Local Address between the gateway and Vigor modem 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.



Available settings are explained as follows:

Item	Description
Auto	No need to type any other information for PPP mode.
Manual	**Subnet Prefix** - Enter the subnet prefix address obtained from service provider.

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

Note: 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.

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.

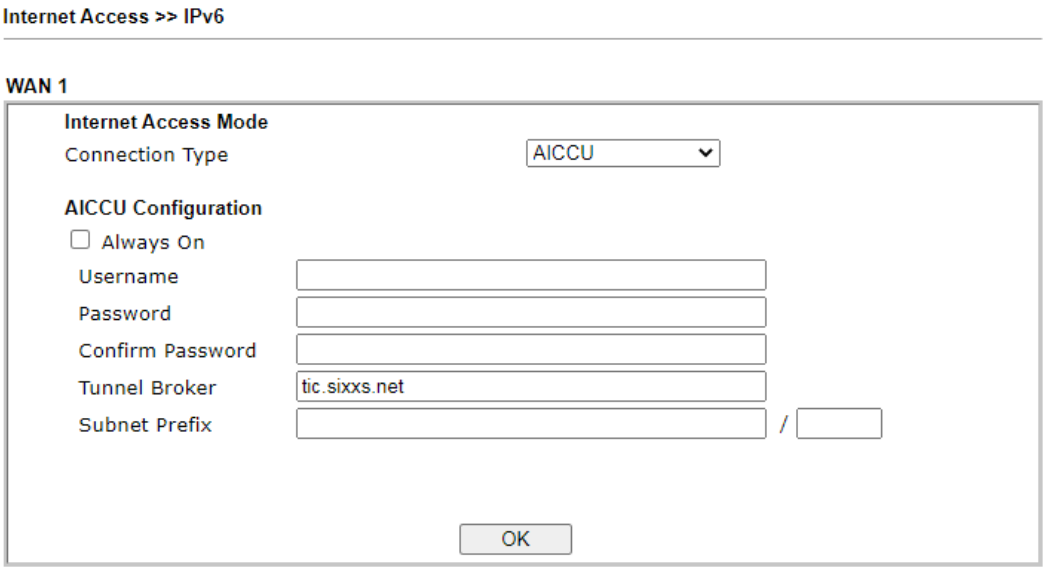
After getting the IPv6 prefix and starting modem advertisement daemon (RADVD), the PC behind this modem can directly connect to IPv6 the Internet.

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.
Password	Type the password assigned with the user name.
Confirm Password	Type the password again to make the confirmation.
Tunnel Broker	Type the address for the tunnel broker IP, FQDN or an optional port number.

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

AICCU



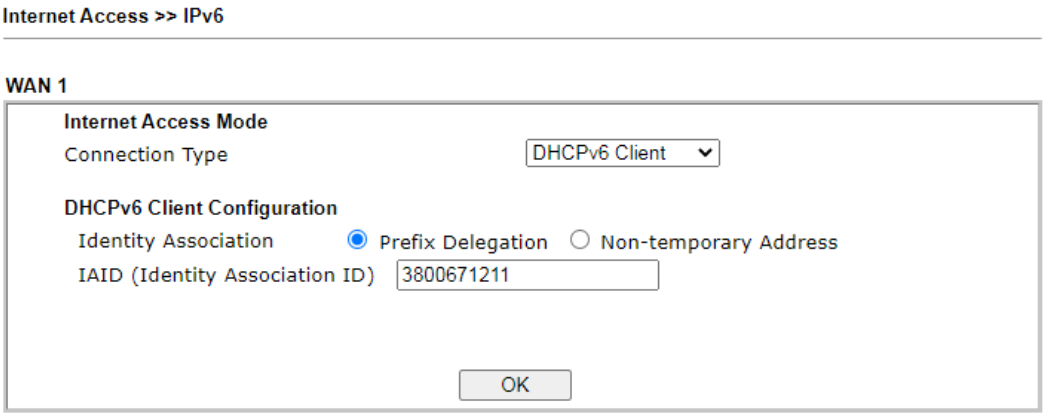
Available settings are explained as follows:

Item	Description
Always	The IPv6 network connection will be always on when this box is checked.
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.
Password	Type the password assigned with the user name.
Confirm Password	Type the password again to make the confirmation.
Tunnel Broker	Type the address for the tunnel broker IP, FQDN or an optional port number.
Subnet Prefix	Type the subnet prefix address getting from service provider

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

DHCPv6 Client

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



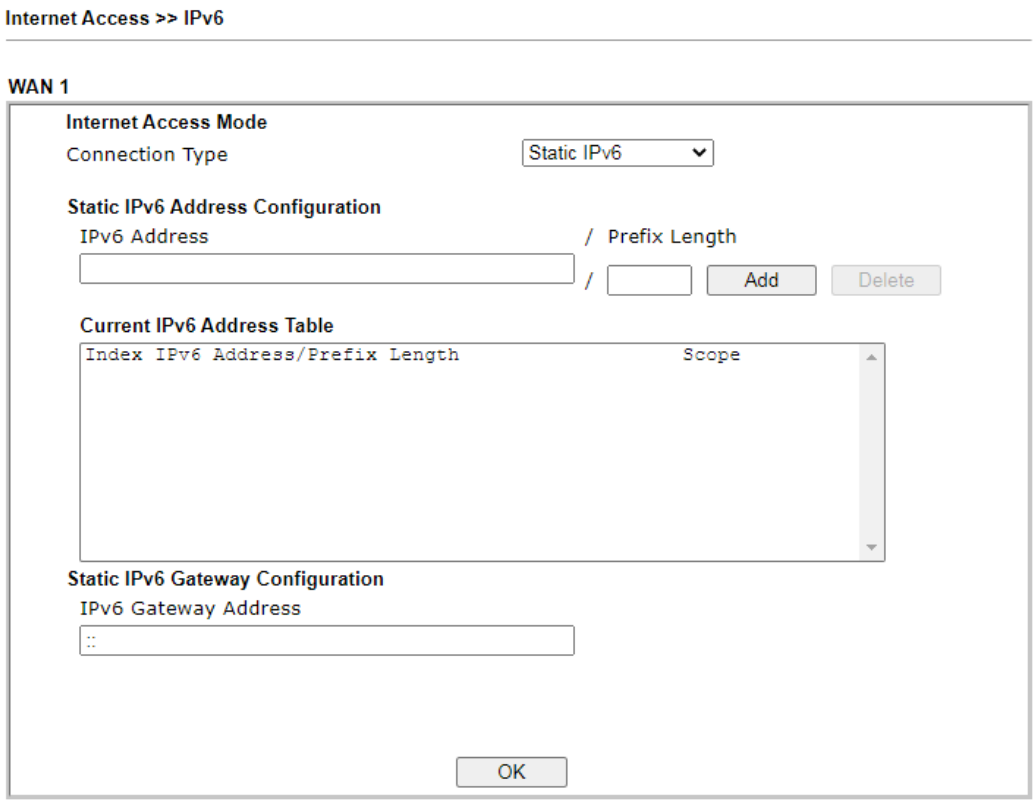
Available settings are explained as follows:

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

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

Static IPv6

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



Available settings are explained as follows:

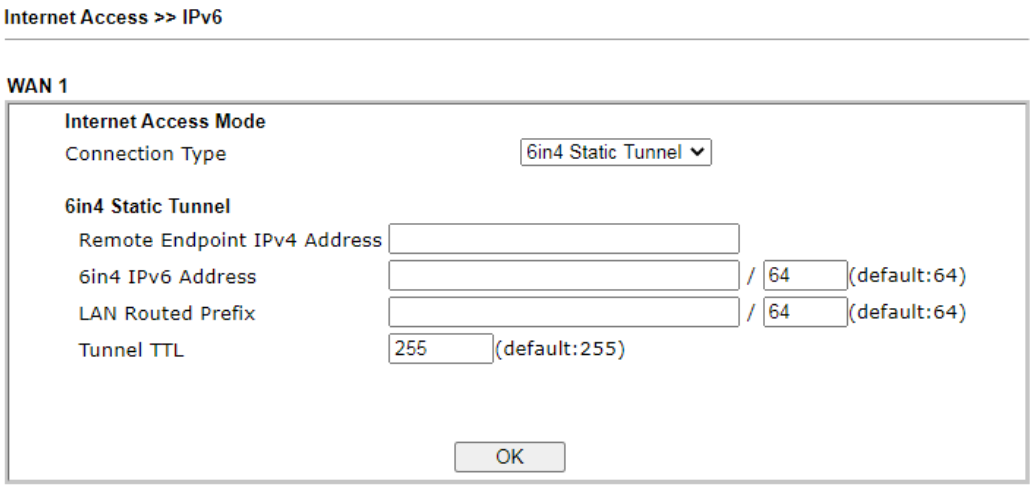
Item	Description
Static IPv6 Address configuration	**IPv6 Address –** Type the IPv6 Static IP Address. **Prefix Length –** Type the fixed value for prefix length. **Add –** Click it to add a new entry. **Delete –** Click it to remove an existed entry.
Current IPv6 Address Table	Display current interface IPv6 address.
Static IPv6 Gateway Configuration	**IPv6 Gateway Address -** Type your IPv6 gateway address here.

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

6in4 Static Tunnel

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

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



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)

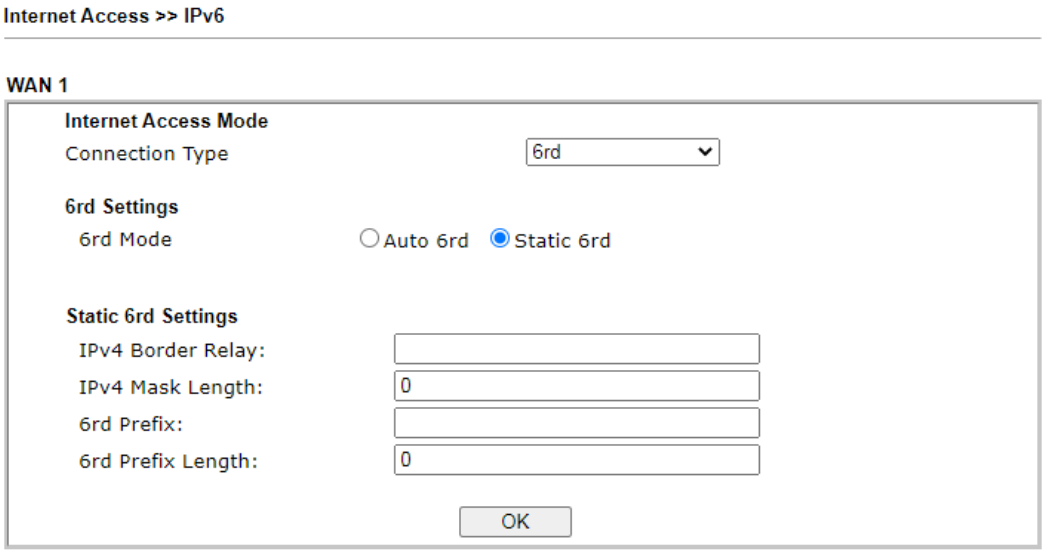
TX Packets	RX Packets	TX Bytes	RX Bytes
14	80	1244	6815

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

6rd

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



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.

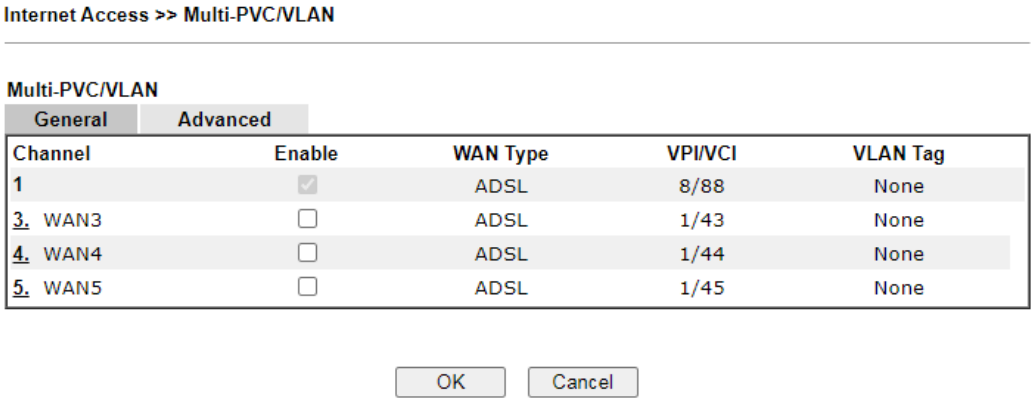
After finished the above settings, click **OK** to save the settings.

3.1.6 Multi-PVC/VLAN

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

General

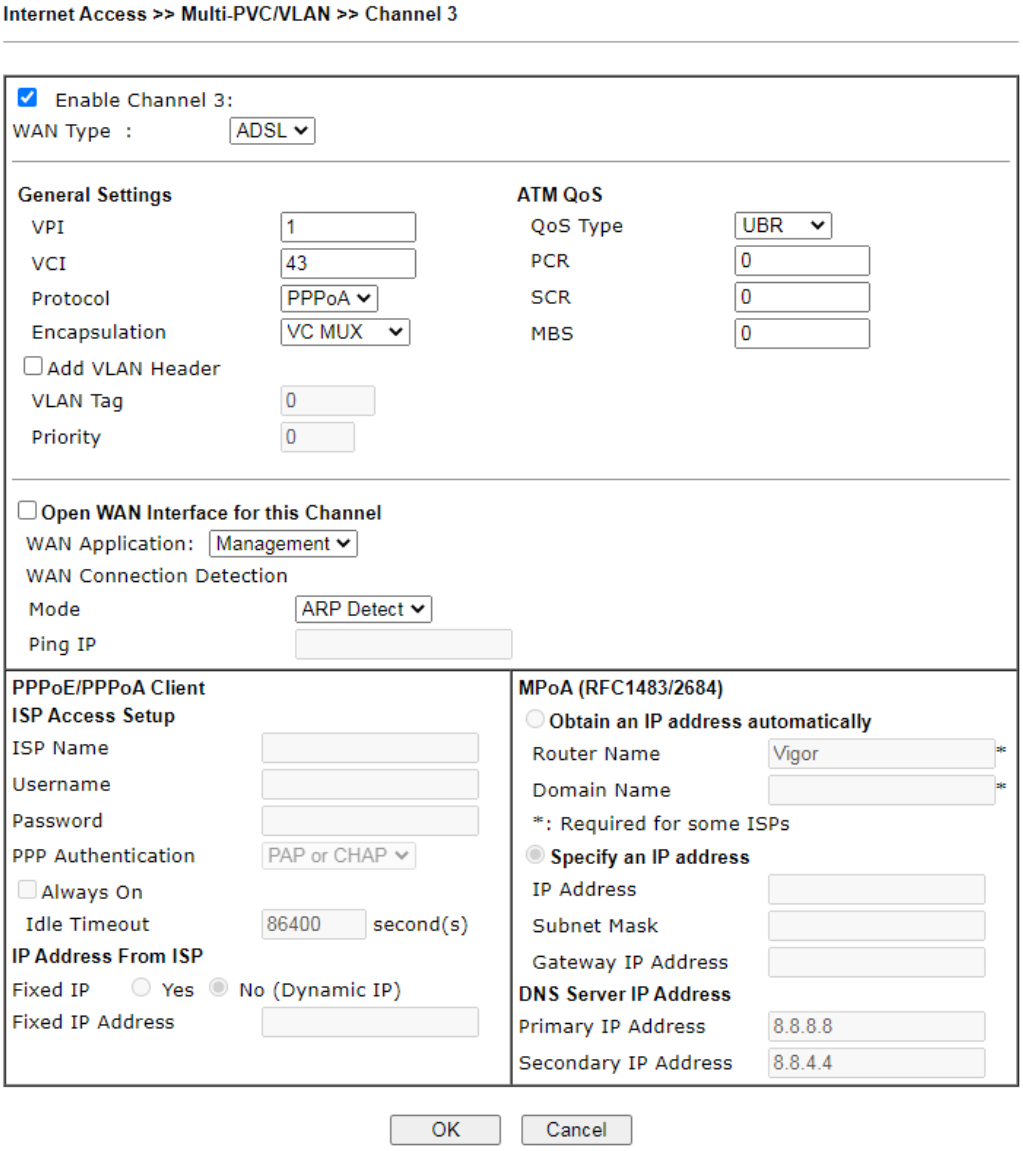
This page shows the basic configurations used by every channel.



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 ~ 8 are configurable.
Enable	Enable or disable the settings for this channel.
WAN Type	Displays the physical medium that the channel will use.
VLAN Tag	Displays the VLAN tag value that will be used for the packets traveling on this channel.

Click any index (3, 4 and 5) to get the following web page:



Available settings are explained as follows:

Item	Description
Multi-PVC/VLAN Channel 3/4/5	**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.
General Setting	**VPI** - Type in the value provided by your ISP. **VCI** - Type in the value provided by your ISP. **Protocol** - Select a proper protocol for this channel. **Encapsulation** - Choose a proper type for this channel. The types will be different according to the protocol setting that you choose. **Add VLAN Header –** Check the box to enable VLAN tag configuration. **VLAN Tag –** Type the value as the VLAN ID number. Valid

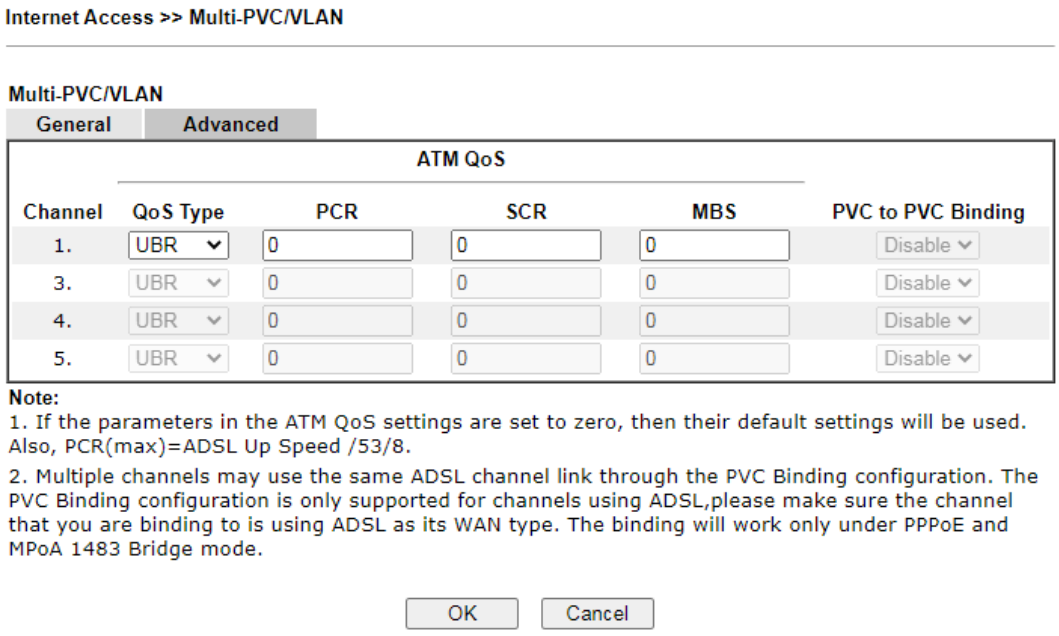
	settings are in the range from 1 to 4095. The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value. **Priority –** Choose the number to determine the packet priority for such VLAN. The range is from 0 to 7.
ATM QoS	Such configuration is applied to upstream packets. Such information will be provided by ISP. Please contact with your ISP for detailed information. **QoS Type -** Select a proper QoS type for the channel. **PCR** - It represents Peak Cell Rate. The default setting is "0". **SCR** - It represents Sustainable Cell Rate. The value of SCR must be smaller than PCR. **MBS** - It represents Maximum Burst Size. The range of the value is 10 to 50.
Open WAN Interface for this Channel	Check the box to enable relating function. **WAN Application –** **Management** – It can be specified for general management (Web configuration/telnet/TR069). If you choose Management, the configuration for this VLAN will be effective for Web configuration/telnet/TR069. **IPTV** - The IPTV configuration will allow the WAN interface to send IGMP packets to IPTV servers.
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. **Ping IP** – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. **TTL (Time to Live)** – Displays value for your reference. TTL value is set by telnet command.
PPPoE/PPPoA Client	Enter your allocated username, password and authentication parameters according to the information provided by your ISP. **ISP Access Setup** ● **ISP Name** – Type in the name of your ISP. ● **Username** – Type in the username provided by ISP in this field. The maximum length of the name you can set is 80 characters. ● **Password** – Type in the password provided by ISP in this field. The maximum length of the password you can set is 48 characters. ● **PPP Authentication** – Select **PAP only** or **PAP or CHAP** for PPP. ● **Always On** – Check it to keep the network connection always. **Idle Timeout** – Set the timeout for breaking down the Internet after passing through the time without any action.

	IP Address From ISP ● **Fixed IP** – Click **Yes** to use this function and type in a fixed IP address in the box of **Fixed IP Address**.
MPoA (RFC1483/2684)	**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. **DNS Server IP Address -** Type in the primary IP address for the router if you want to use **Static IP** mode. If necessary, type in secondary IP address for necessity in the future.

WAN link for Channel 3, 4 and 5 are provided for modem-borne application such as TR-069 and IPTV. The settings must be applied and obtained from your ISP. For your special request, please contact with your ISP and then click WAN link of Channel 3 or 4 to configure your modem.

Advanced

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



Available settings are explained as follows:

Item	Description

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

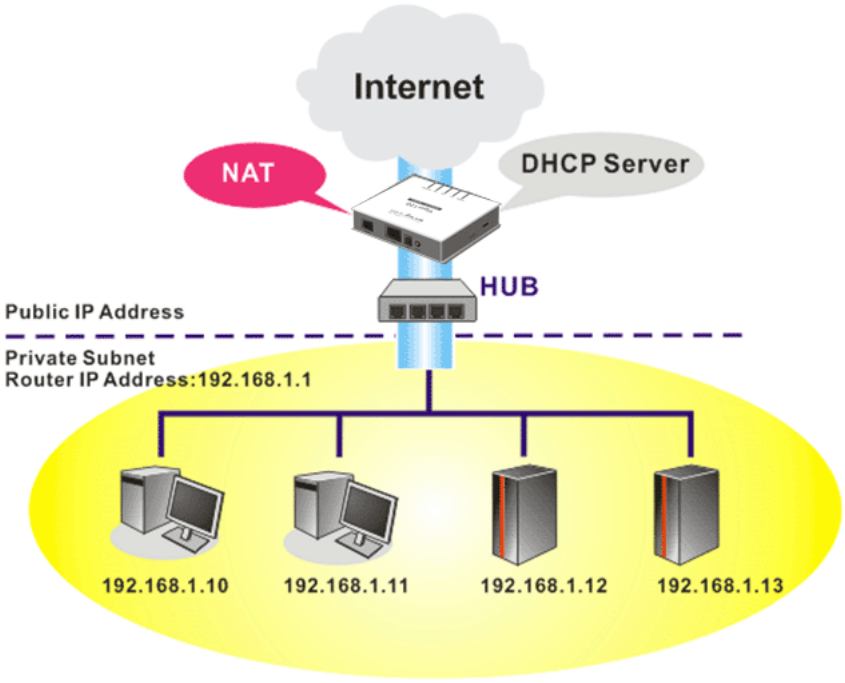
After finished the above settings, click **OK** to save the settings.

3.2 LAN

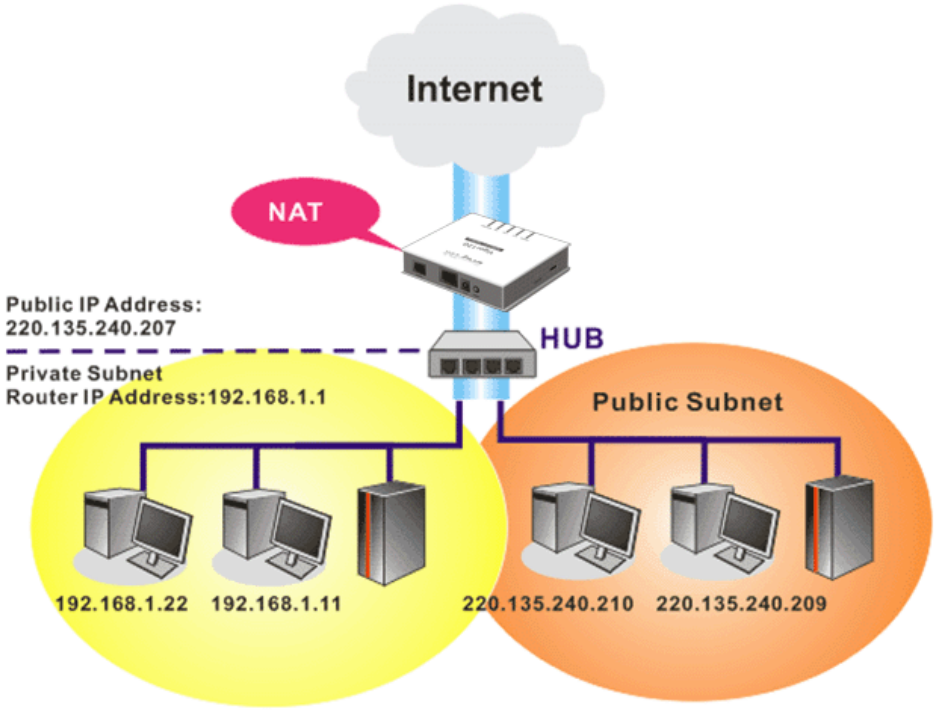
Local Area Network (LAN) is a group of subnets regulated and ruled by modem. The design of network structure is related to what type of public IP addresses coming from your ISP.

3.2.1 Basics of LAN

The most generic function of Vigor modem is NAT. It creates a private subnet of your own. As mentioned previously, the modem 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 modem 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 modem will serve for IP routing to help hosts in the public subnet to communicate with other public hosts or servers outside. Therefore, the modem should be set as the gateway for public hosts.

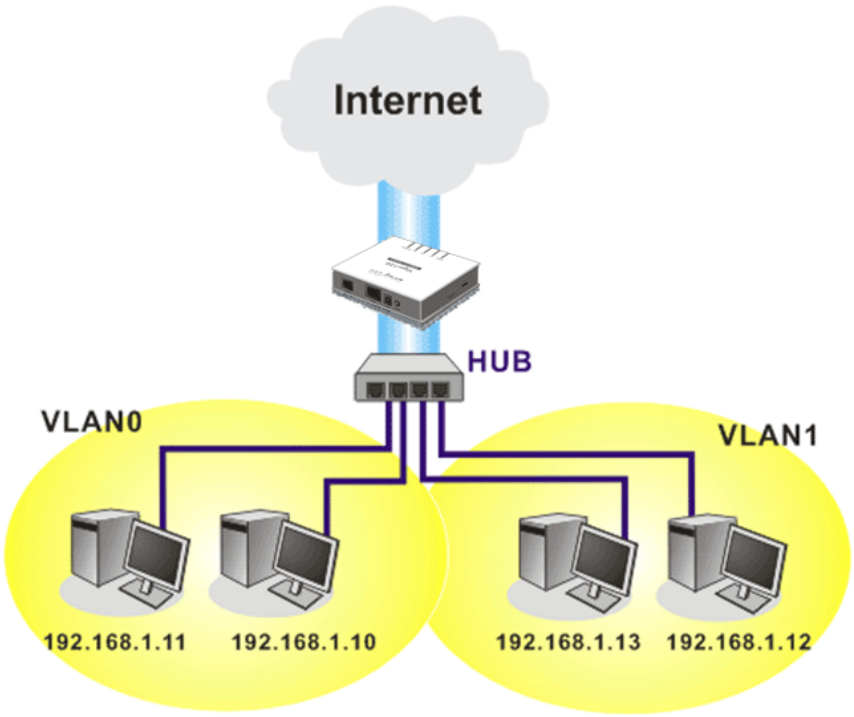


What is Routing Information Protocol (RIP)

Vigor modem will exchange routing information with neighboring modems using the RIP to accomplish IP routing. This allows users to change the information of the modem such as IP address and the modems 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.

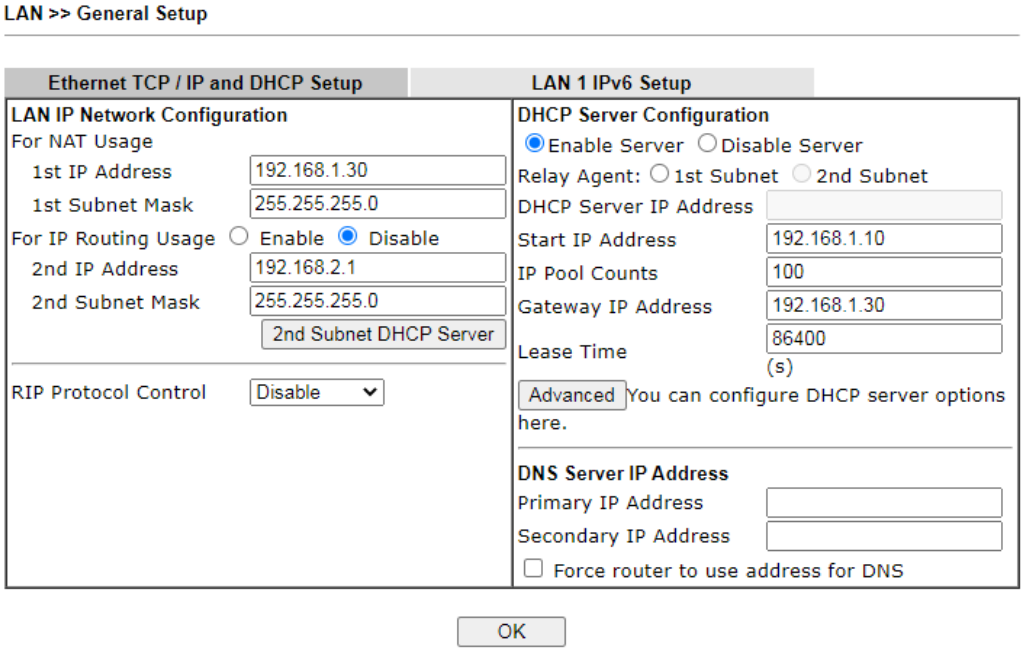


3.2.2 General Setup

This page provides you the general settings for LAN. Open **LAN>>General Setup**.

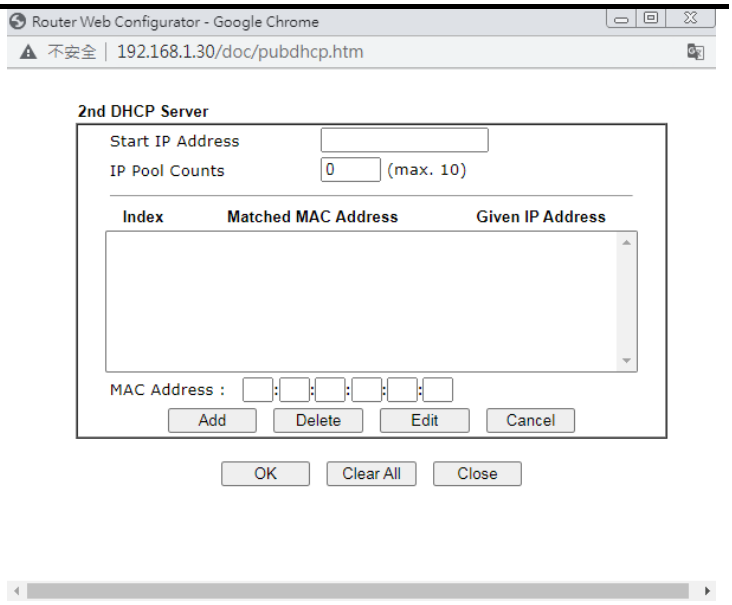
Details Page for LAN1 – Ethernet TCP/IP and DHCP Setup

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



Available settings are explained as follows:

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



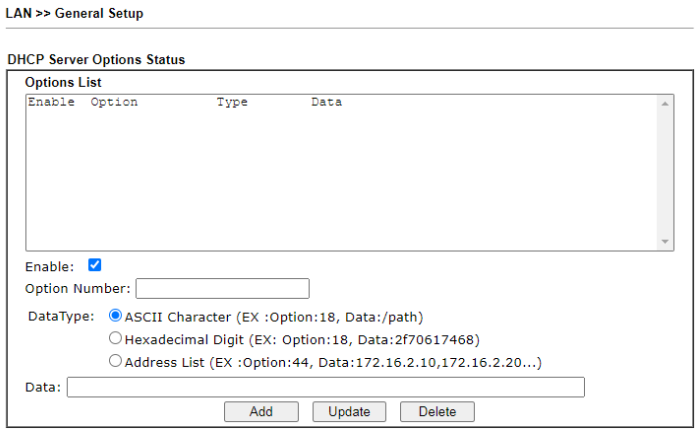
- **Start IP Address:** Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 2nd IP address of your modem is 220.135.240.1, the starting IP address must be 220.135.240.2 or greater, but smaller than 220.135.240.254.
- **IP Pool Counts:** Enter the number of IP addresses in the pool. The maximum is 10. For example, if you type 3 and the 2nd IP address of your modem is 220.135.240.1, the range of IP address by the DHCP server will be from 220.135.240.2 to 220.135.240.11.
- **MAC Address:** Enter the MAC Address of the host one by one and click **Add** to create a list of hosts to be assigned, deleted or edited IP address from above pool. Set a list of MAC Address for 2nd DHCP server will help modem to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2nd subnet won't get an IP address belonging to 1st subnet.

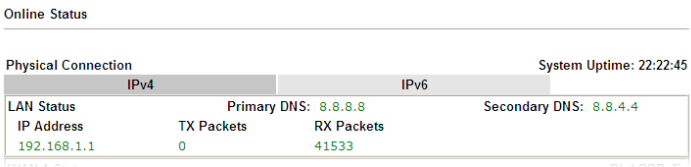
RIP Protocol Control,

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

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

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

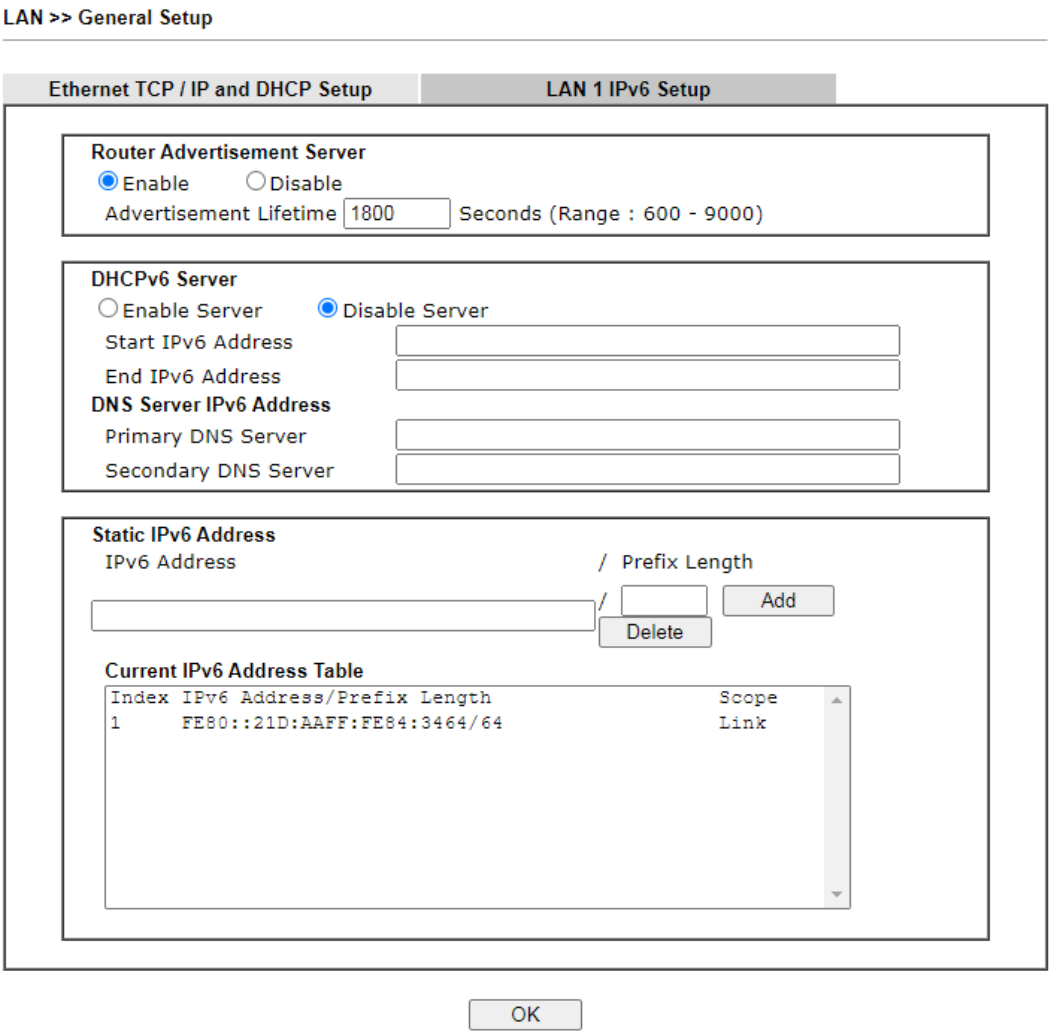
	network. If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location. **Enable Server -** Let the modem assign IP address to every host in the LAN. **Disable Server –** Let you manually assign 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 –**Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server. **Start IP Address -** Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your modem is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254. **IP Pool Counts -** Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253. **Gateway IP Address -** Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the modem, which means the modem is the default gateway. **Lease Time –** Enter the time to determine how long the IP address assigned by DHCP server can be used. – If required, click it to set option number for DHCP.
Advanced	DHCP packets can be processed by adding option number and data information when such function is enabled.  **Enable/Disable** – Enable/Disable the function of DHCP Option. This modem allows you to add up to five Option Numbers. 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 function. Different number means different meaning. Please contact with your ISP for obtaining the correct number value. **DataType** – Choose the type (ASCII or Hex) for the data to be calculated. **Data** – Type the content of the data to be processed by the function of DHCP option.
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 modem 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 modem will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field. The default DNS Server IP address can be found via Online Status:  If both the Primary IP and Secondary IP Address fields are left empty, the modem 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 modem will resolve the domain name immediately. Otherwise, the modem 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 modem to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).

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

Details Page for LAN1 – IPv6 Setup

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



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

Available settings are explained as follows:

Item	Description
Router Advertisement Server	**Enable** – Click it to enable RADVD server. The modem 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. **Disable** – Click it to disable RADVD server. **Advertisement Lifetime** - The lifetime associated with the default modem 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 modem is not a default modem and should not appear on the default modem list.
DHCPv6 Server	**Enable Server** –Click it to enable DHCPv6 server. DHCPv6 Server could assign IPv6 address to PC according to the Start/End IPv6 address configuration.

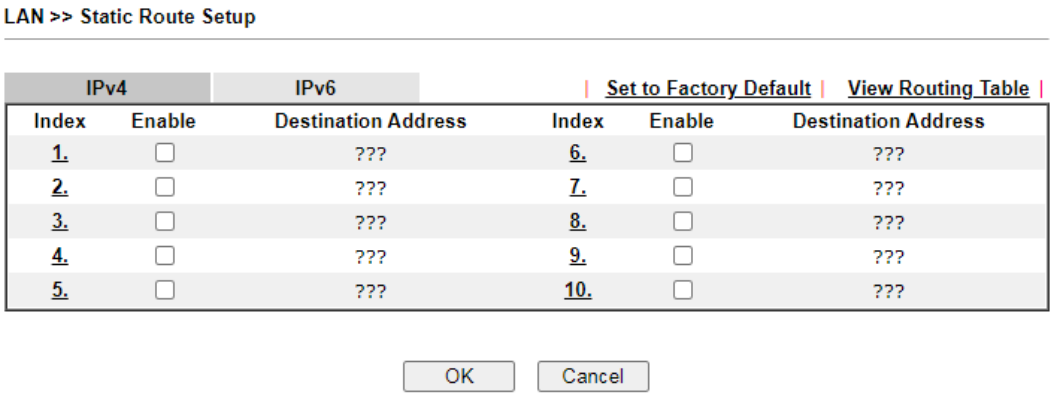
	Disable Server –Click it to disable DHCPv6 server. **Start IPv6 Address** / **End IPv6 Address** –Type the start and end address for IPv6 server.
DNS Server IPv6 Address	**Primary DNS Sever** – Type the IPv6 address for Primary DNS server. **Secondary DNS Server** –Type another IPv6 address for DNS server if required.
Static IPv6 Address	**IPv6 Address** –Type static IPv6 address for LAN. **Prefix Length –** Type the fixed value for prefix length. **Add –** Click it to add a new entry. **Delete –** Click it to remove an existed entry.
Current IPv6 Address Table	Display current used IPv6 addresses.

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

3.2.3 Static Route

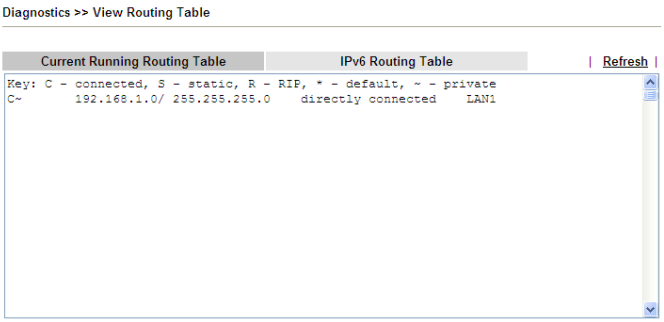
Go to **LAN** to open setting page and choose **Static Route**. The modem offers IPv4 and IPv6 for you to configure the static route. Both protocols bring different web pages.

Static Route for IPv4



Available settings are explained as follows:

Item	Description
Index	The number (1 to 10) 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.

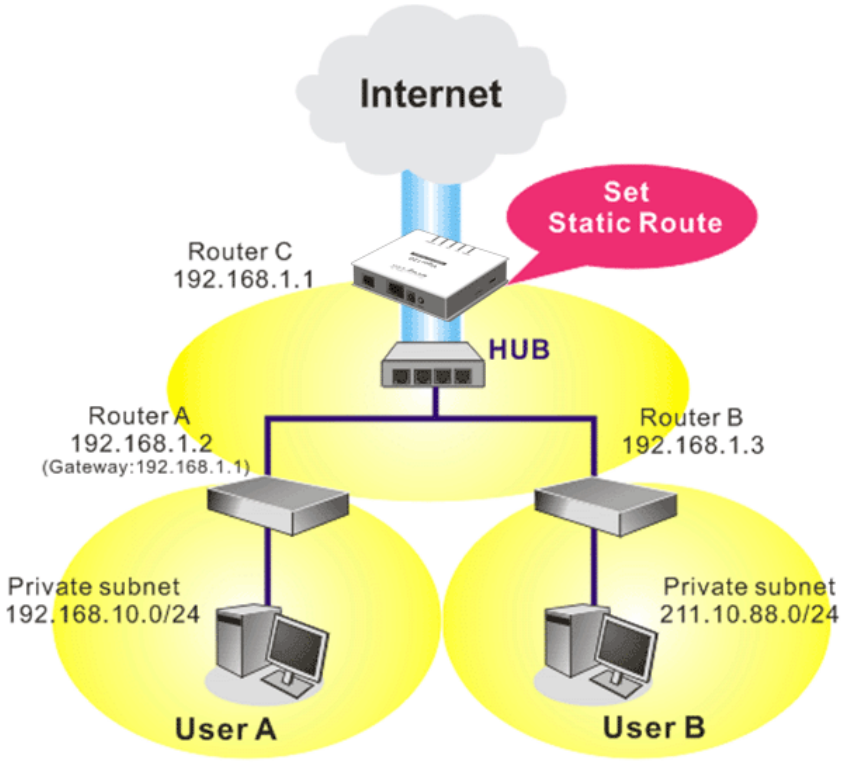
Viewing Routing Table	Displays the routing table for your reference. 

Add Static Routes to Private and Public Networks (based on IPv4)

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

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

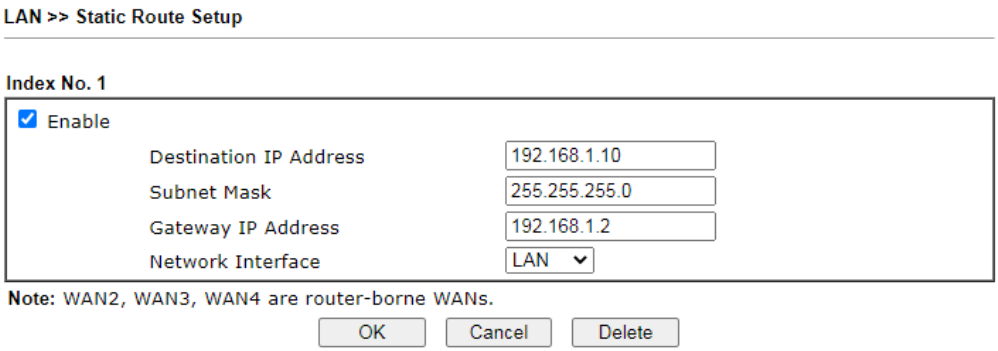
Before setting Static Route, user A cannot talk to user B for Modem A can only forward recognized packets to its default gateway Main Modem.



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

Note: 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 modems 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 modem, and continuously exchange of IP routing information with different subnets.

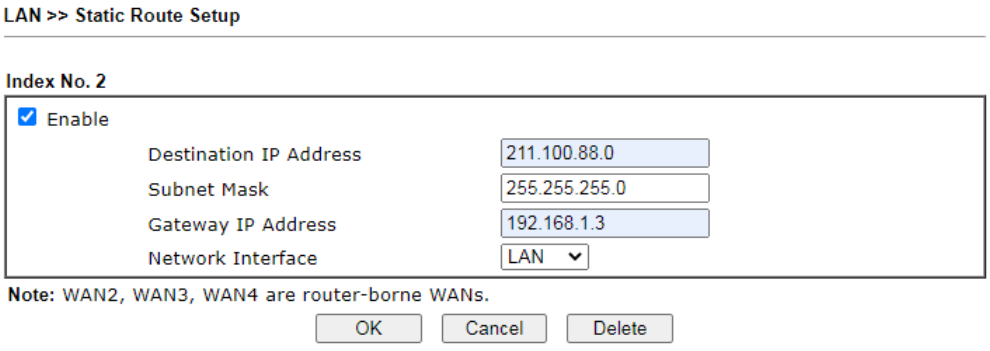
2. Click the **LAN - Static Route** and click on the **Index Number 1.** Check the **Enable** box. Please add a static route as shown below, which regulates all packets destined to 192.168.10.0 will be forwarded to 192.168.1.2. Click **OK**.



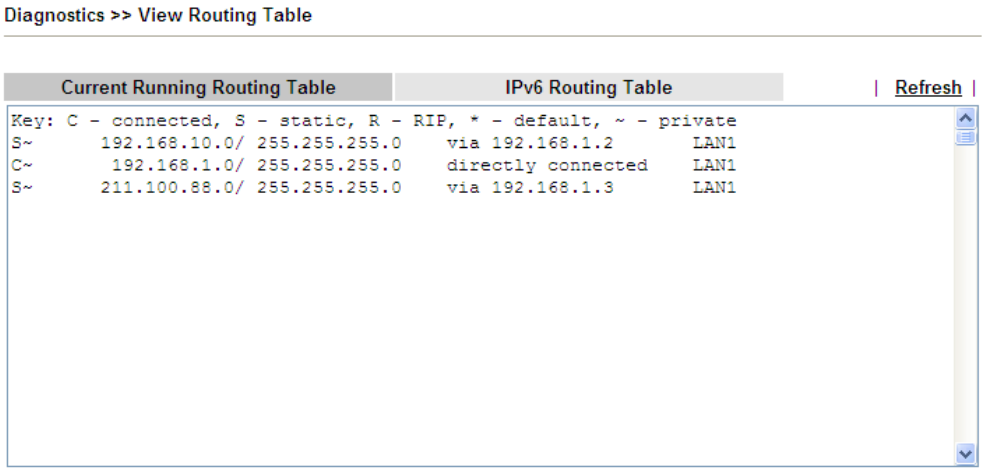
Available settings are explained as follows:

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.

3. 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.

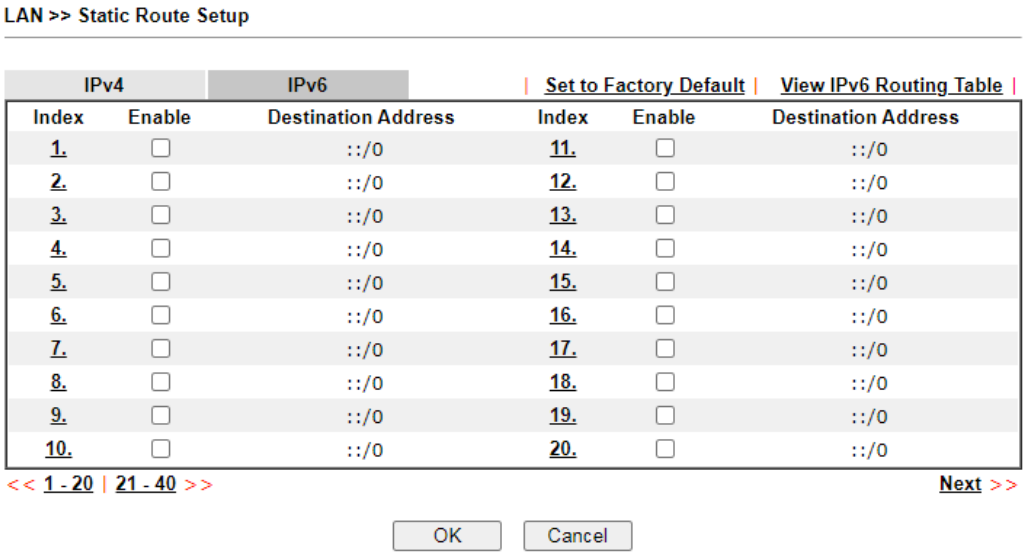


4. Go to **Diagnostics** and choose **Routing Table** to verify current routing table.



Static Route for IPv6

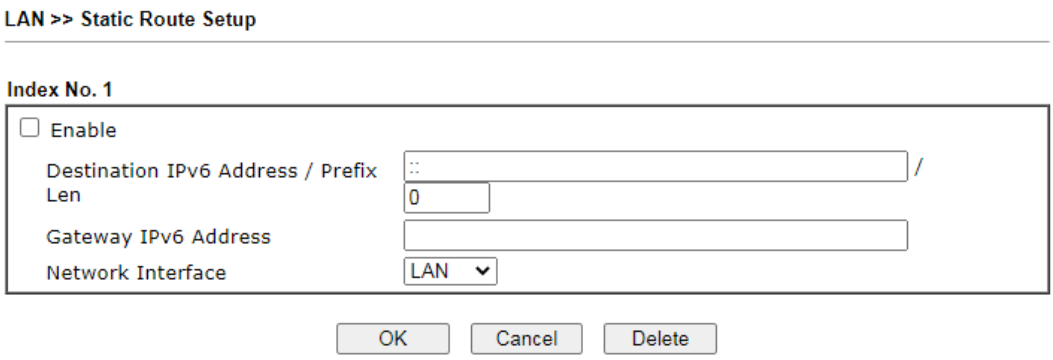
You can set up to 40 profiles for IPv6 static route. Click the IPv6 tab to open the following page:



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.



Available settings are explained as follows:

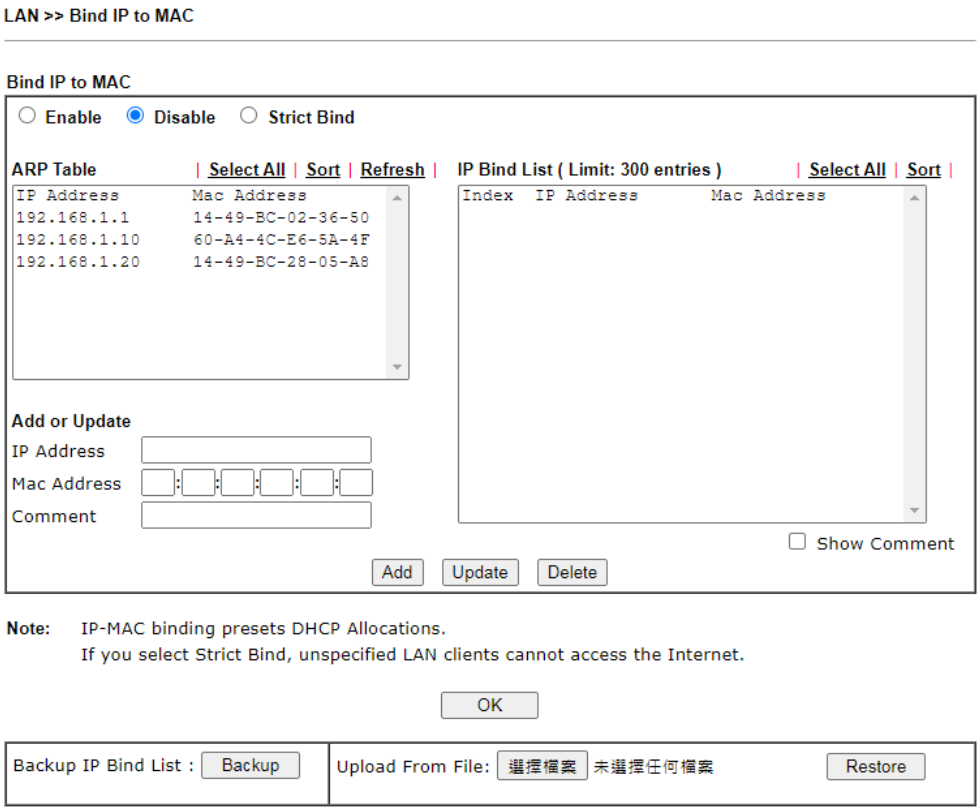
Item	Description
Enable	Click it to enable this profile.
Destination IPv6 Address / Prefix Len	Type the IP address with the prefix length for this entry.
Gateway IPv6 Address	Type the gateway address for this entry.
Network Interface	Use the drop down list to specify an interface for this static route.

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

3.2.4 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.



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 modem. 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	**IP Address** – Type the IP address that will be used for the specified MAC address. **Mac Address** – Type the MAC address that is used to bind with the assigned IP address. **Comment** – Type a brief description for the entry. **Show Comment** – Check this box to display the comment on IP Bind List box.
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 or Update** 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.

Note: 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 modem might not be accessed.

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

3.3 NAT

Usually, the modem serves as an NAT (Network Address Translation) modem. 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.

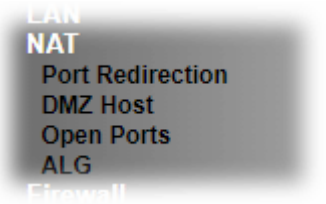
When the outgoing packets destined to some public server on the Internet reach the NAT modem, the modem will change its source address into the public IP address of the modem, select the available public port, and then forward it. At the same time, the modem shall list an entry in a table to memorize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

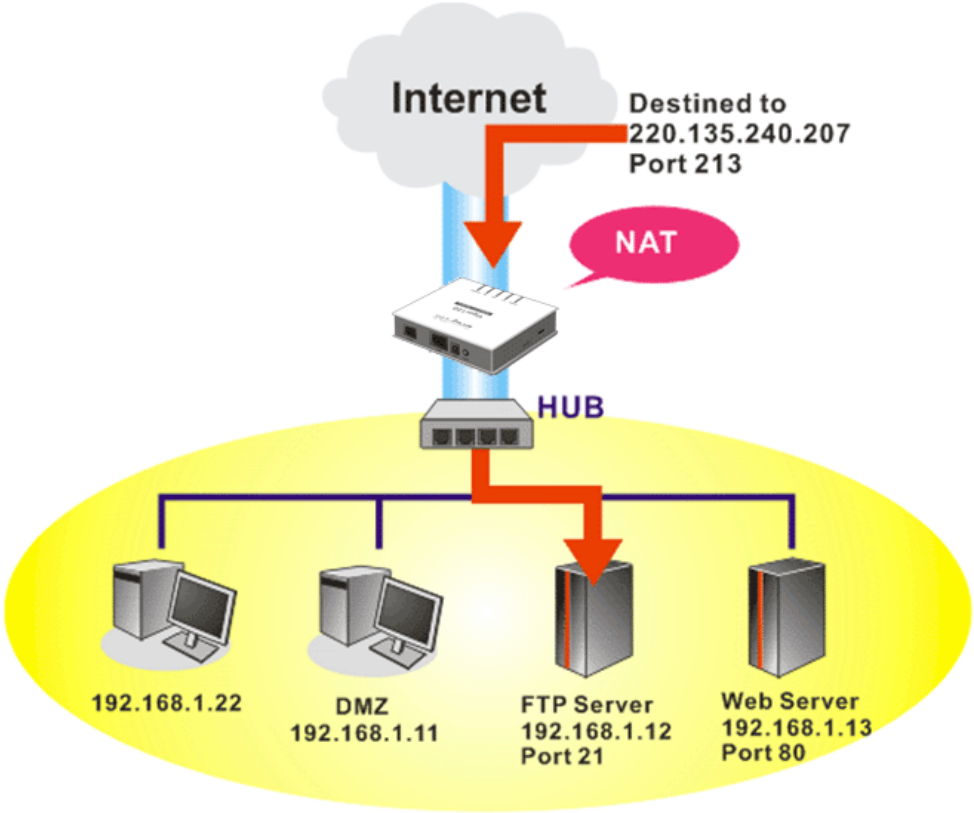
On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the modem. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by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

Below shows the menu items for NAT.



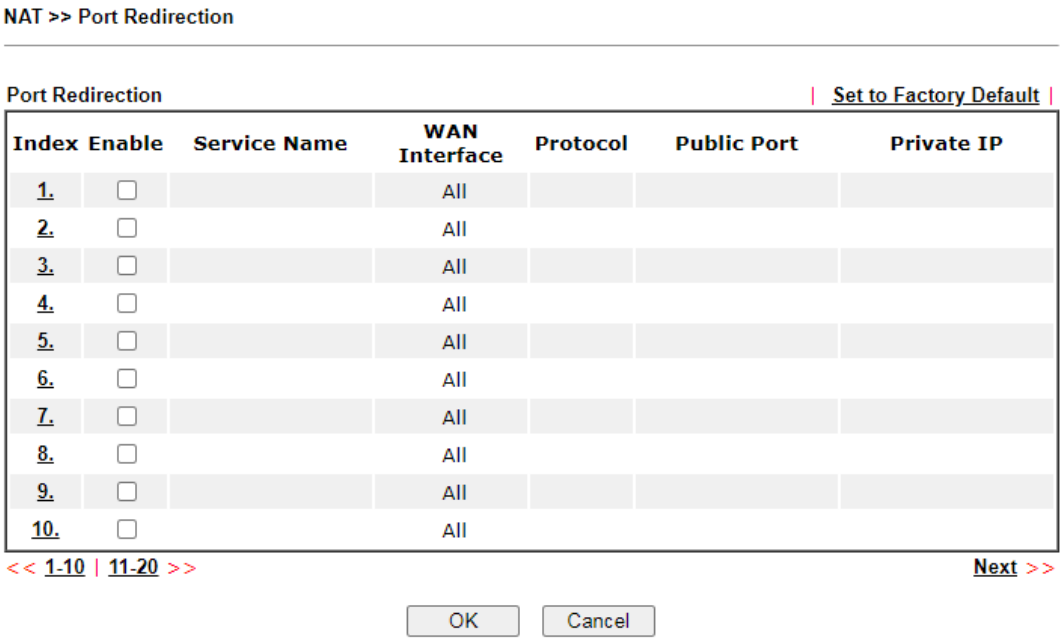
3.3.1 Port Redirection

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 modem, 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.

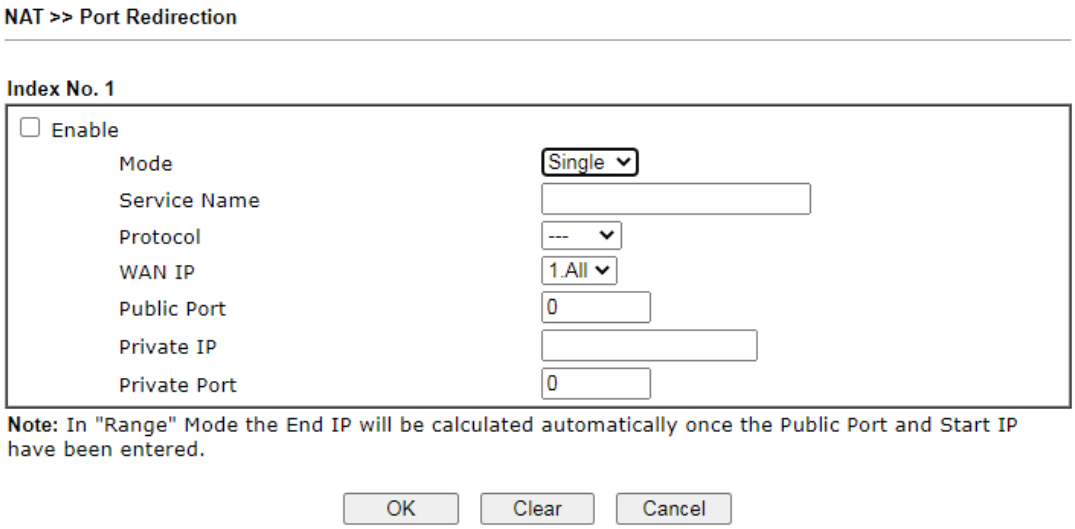
To use this function, please go to **NAT** page and choose **Port Redirection** web page. The **Port Redirection Table** provides 20 port-mapping entries for the internal hosts.



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 or interface 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.



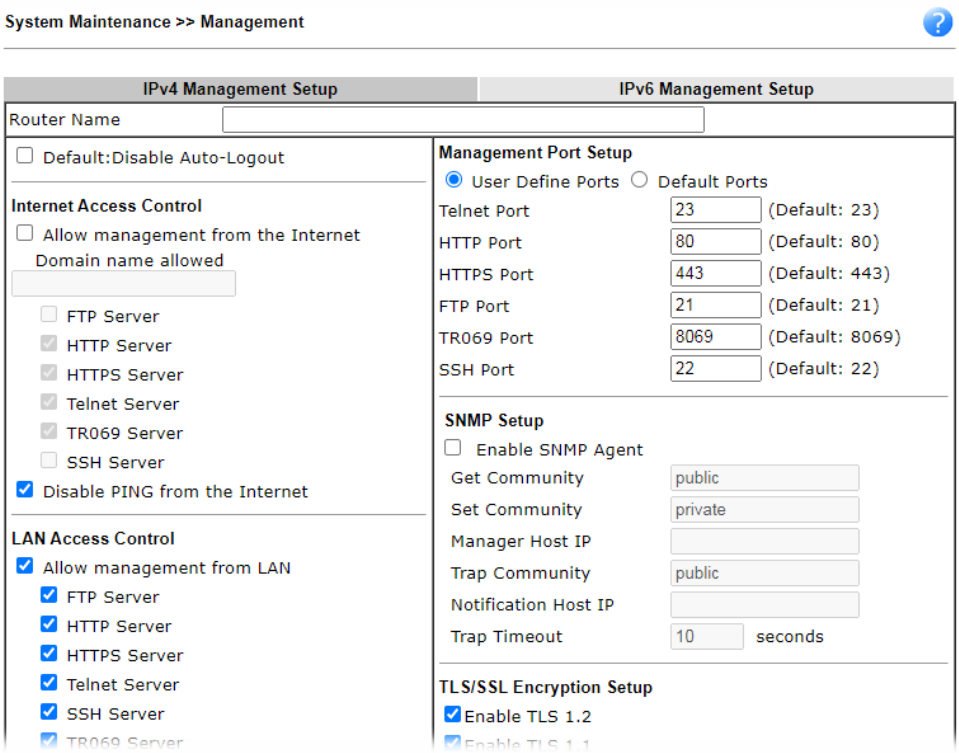
Available settings are explained as follows:

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. Simply type the required number on the first box. The second one will be assigned automatically later.
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) and the fourth digits in the second box (as the end point).
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.

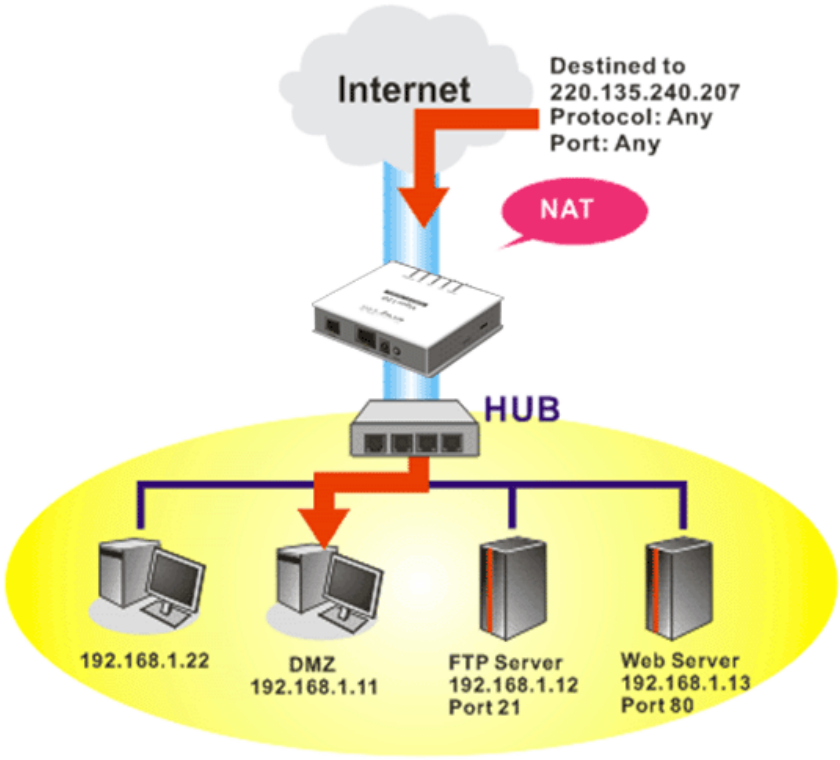
Note that the modem has its own built-in services (servers) such as Telnet, HTTP and FTP etc. Since the common port numbers of these services (servers) are all the same, you may need to reset the modem in order to avoid confliction.

For example, the built-in Web User Interface in the modem 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 modem'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.



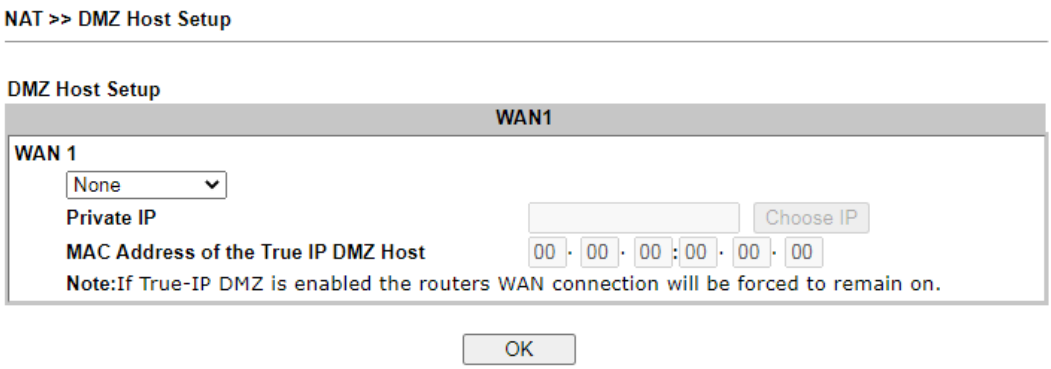
3.3.2 DMZ Host

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 modem 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.



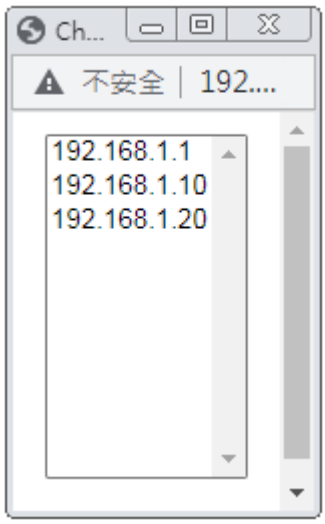
The inherent security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

Click **DMZ Host** to open the following page:



Available settings are explained as follows:

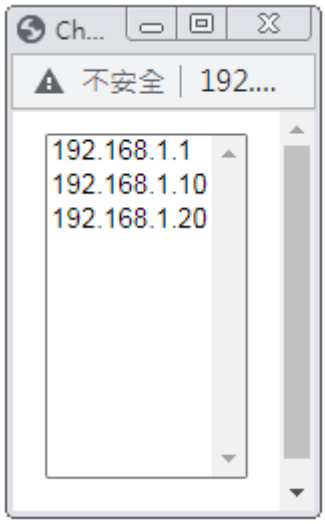
Item	Description
WAN 1 None None Private IP Active True IP	Choose Private IP or Active True IP first. Active True IP selection is available for WAN1 only.
Private IP	Enter the private IP address of the DMZ host, or click Choose PC to select one.
Choose PC	Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select

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

If you previously have set up **WAN Alias** for **PPPoE/PPPoA** or **MPoA** mode**,** you will find them in **Aux. WAN IP** for your selection.

Available settings are explained as follows:

Item	Description
Enable	Check to enable the DMZ Host function.
Private IP	Enter the private IP address of the DMZ host, or click Choose PC to select one.

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

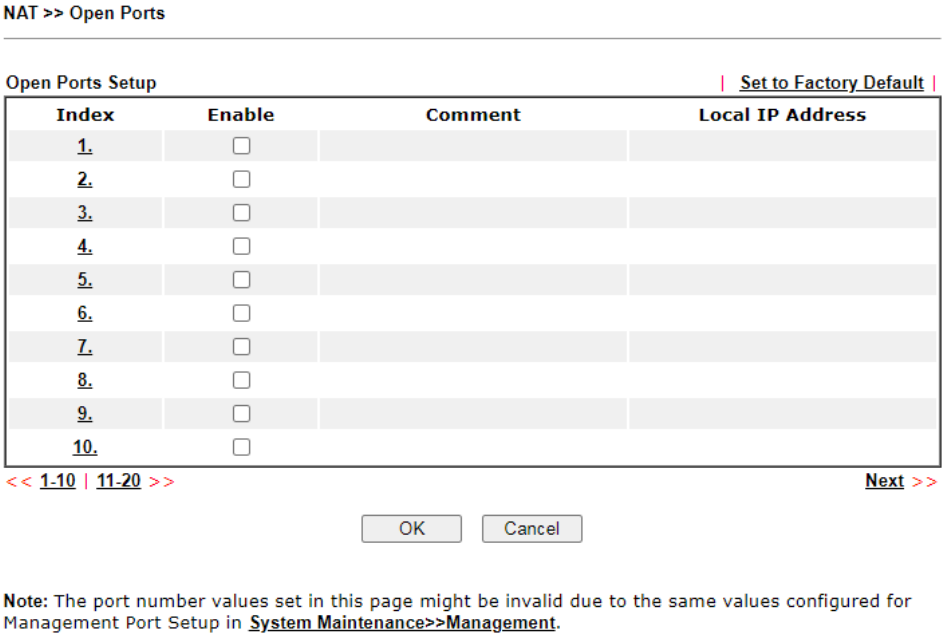
After finishing all the settings here, please click **OK** to save the configuration.

3.3.3 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.

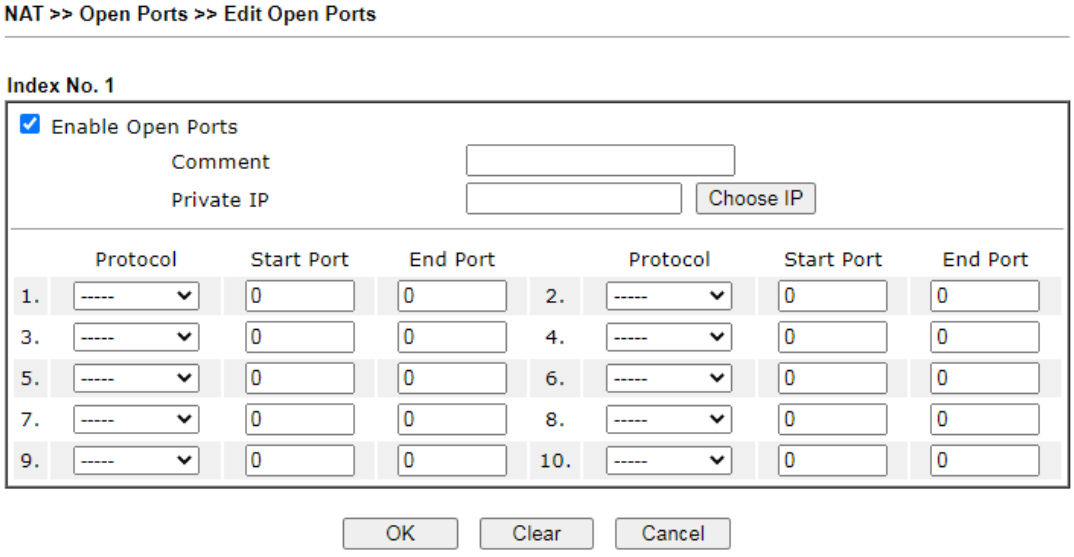
Click **Open Ports** to open the following page:



Available settings are explained as follows:

Item	Description
Index	Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.
Enable	Check to enable the entry.
Comment	Specify the name for the defined network service.
Aux. WAN IP	Display the IP address defined in **WAN Alias** for **PPPoE/PPPoA** or **MPoA** mode.
Local IP Address	Display the private IP address of the local host offering the service.

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



Available settings are explained as follows:

Item	Description
Enable Open Ports	Check to enable this entry.
Comment	Make a name for the defined network application/service.
WAN IP	Specify the WAN IP address that will be used for this entry. This setting is available when WAN IP Alias is configured.
Private IP	Enter the private IP address of the local host or click **Choose IP** to select one. **Choose IP -** Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select the appropriate IP address of the local host in the list.
Protocol	Specify the transport layer protocol. It could be **TCP**, **UDP**, or ----- (none) for selection.

Start Port	Specify the starting port number of the service offered by the local host.
End Port	Specify the ending port number of the service offered by the local host.

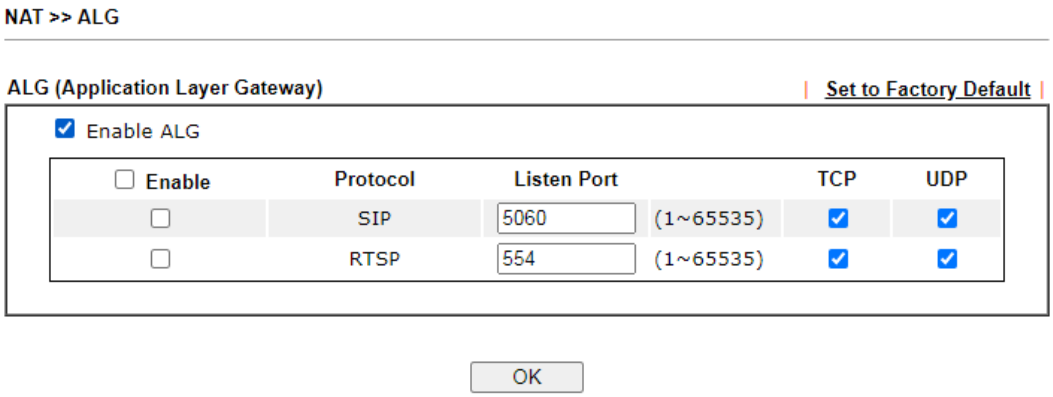
After finishing all the settings here, please click **OK** to save the configuration.

3.3.4 ALG

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

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

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



Available settings are explained as follows:

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

3.4 Firewall

3.4.1 Basics for 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 modem 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 modem to build an unwanted outgoing connection.

Firewall Facilities

The users on the LAN are provided with secured protection by the following firewall facilities:

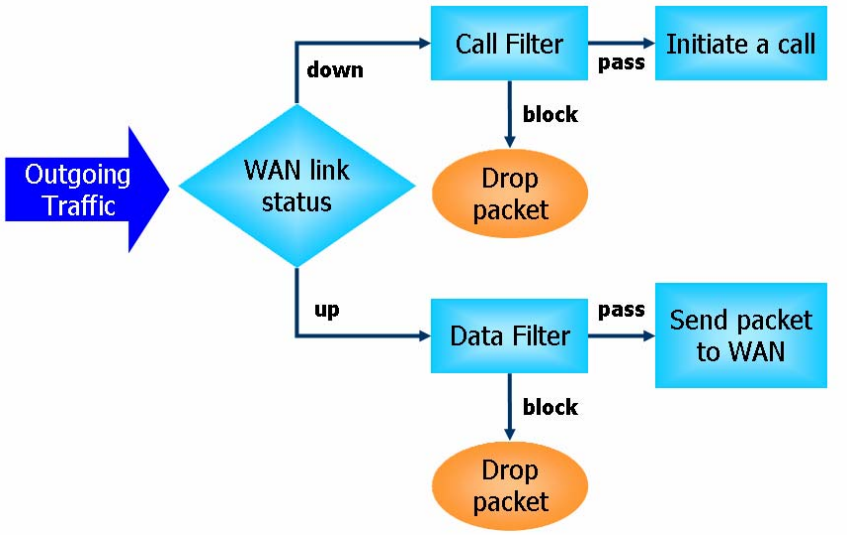
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

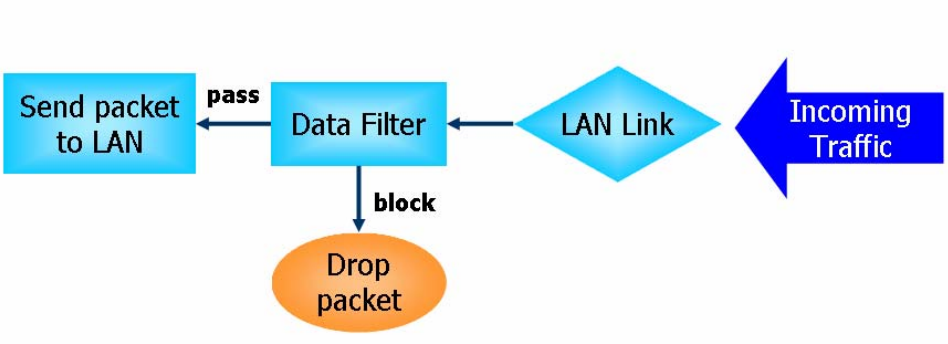
IP Filters

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 modem 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 modem.

The following illustrations are flow charts explaining how modem 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 modem not just examine the header information also monitor 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.

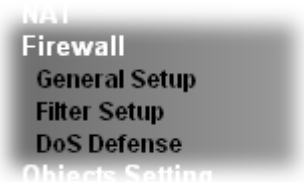
The **DoS Defense** function enables the Vigor modem to inspect every incoming packet based on the attack signature database. Any malicious packet that might duplicate itself to paralyze the host in the secure LAN will be strictly blocked and a Syslog message will be sent as warning, if you set up Syslog server.

Also the Vigor modem 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 modem 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
2. UDP flood attack
3. ICMP flood attack
4. Port Scan attack
5. IP options
6. Land attack
7. Smurf attack
8. Trace route
9. SYN fragment
10. Fraggle attack
11. TCP flag scan
12. Tear drop attack
13. Ping of Death attack
14. ICMP fragment
15. Unknown protocol

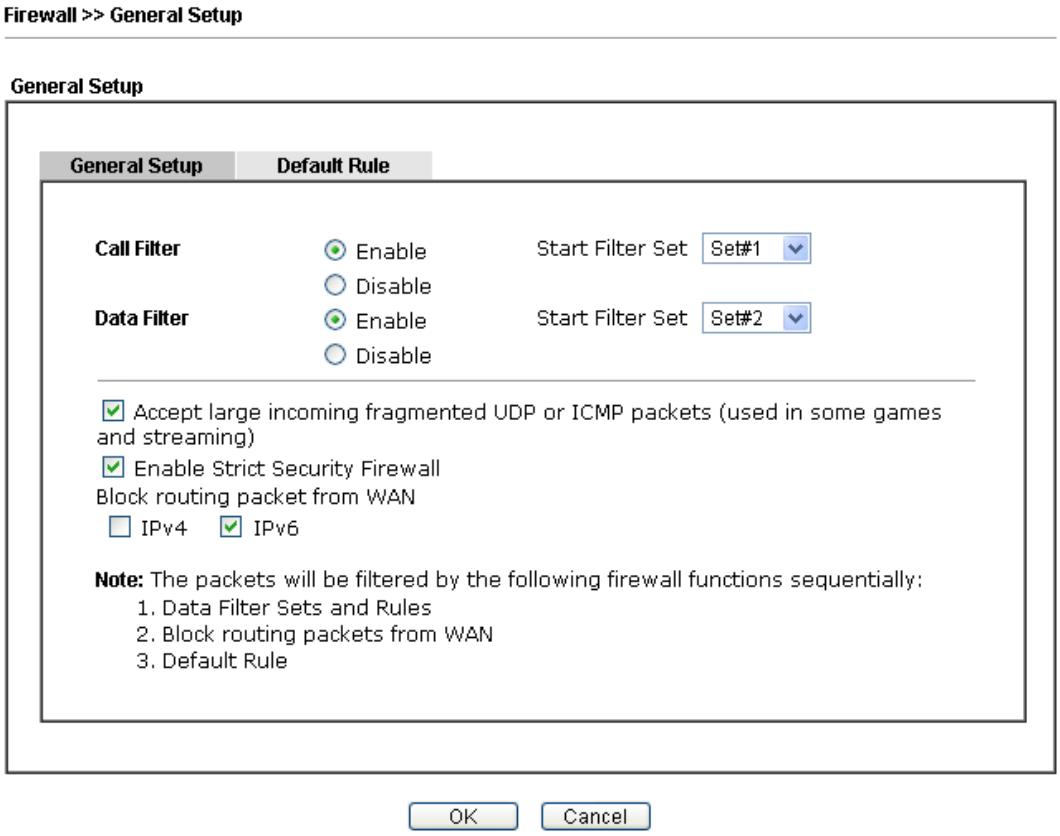
Below shows the menu items for Firewall.

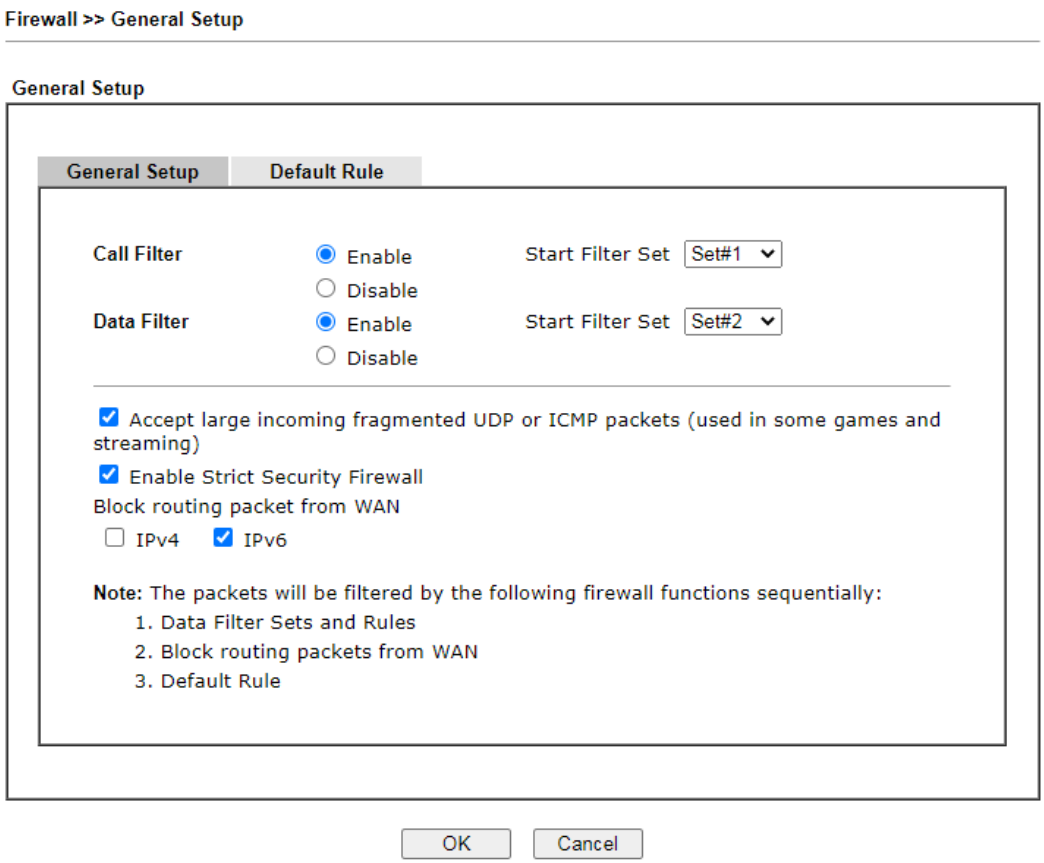


3.4.2 General Setup

General Setup allows you to adjust settings of IP Filter and common options. Here you can enable or disable the **Call Filter** or **Data Filter**. Under some circumstance, your filter set can be linked to work in a serial manner. So here you assign the **Start Filter Set** only. Also you can configure the **Log Flag** settings, **Apply IP filter to VPN incoming packets**, and **Accept incoming fragmented UDP packets**.

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





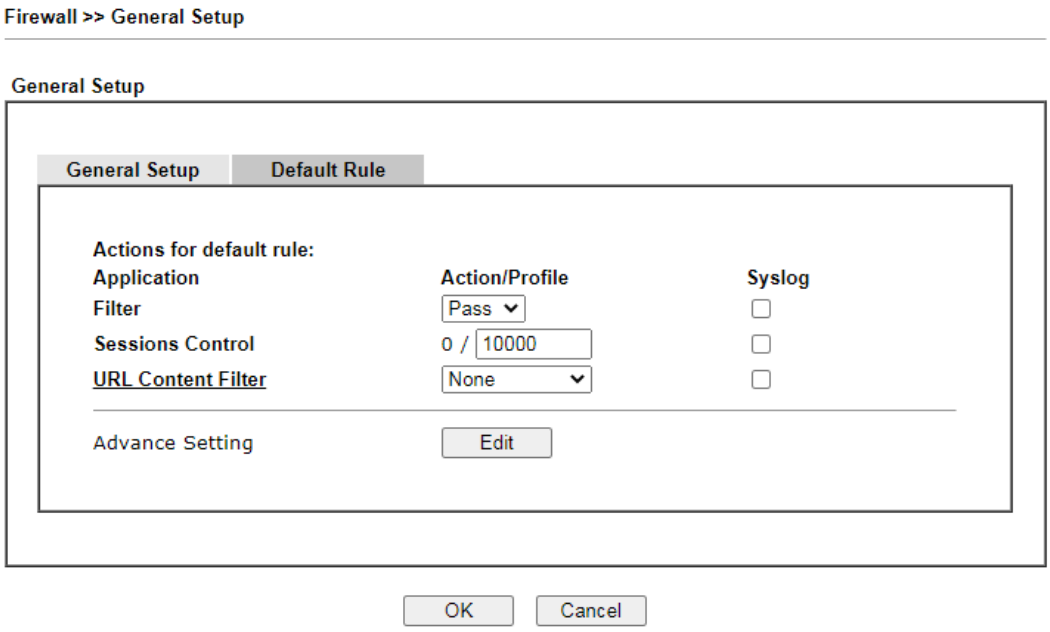
Available settings are explained as follows:

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 modem 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 modem will execute strict security checking for data transmission. Such feature is enabled in default. All the packets, while transmitting through Vigor modem, 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 modem'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.

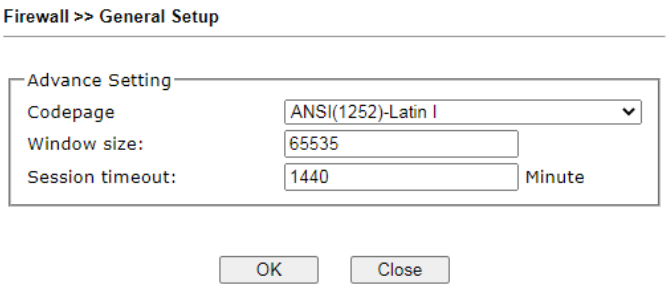
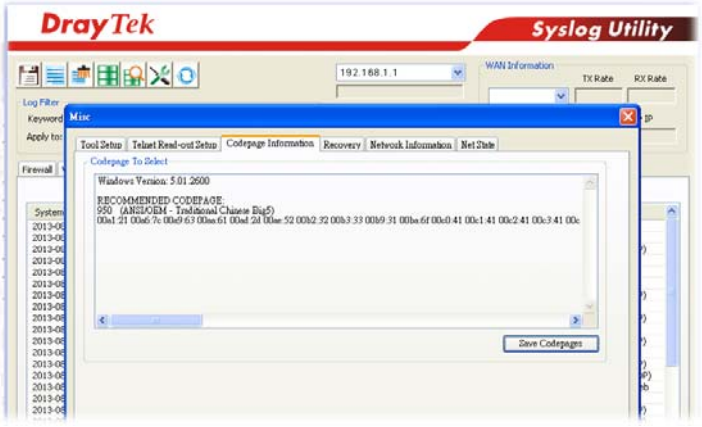
Default Rule Page

Such page allows you to choose filtering profiles including QoS, Load-Balance policy, WCF, APP Enforcement, URL Content Filter, for data transmission via Vigor modem.



Available settings are explained as follows:

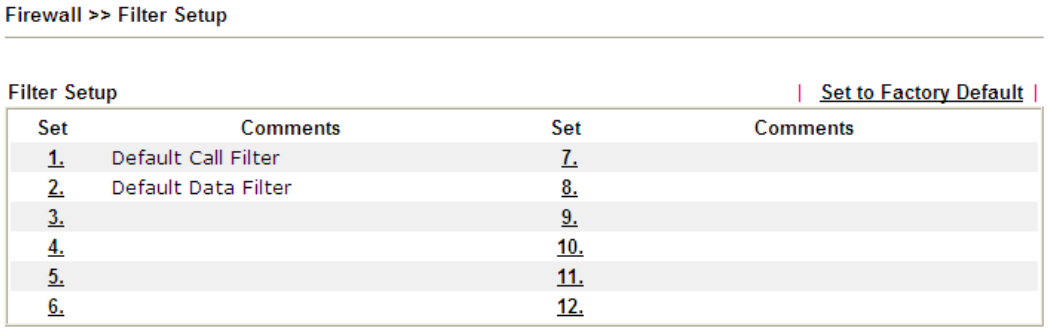
Item	Description
Filter	Select **Pass** or **Block** for the packets that do not match with the filter rules.
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.
URL Content Filter	Select one of the **URL Content Filter** profile settings (created in **CSM>> URL Content Filter**) for applying with this modem. 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.
Advance Setting	Click **Edit** to open the following window. However, it is **strongly recommended** to use the default settings here.  **Codepage** - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage. If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.  **Window size** – It determines the size of TCP protocol (0~65535). The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper. **Session timeout** – Setting timeout for sessions can make the best utilization of network resources.

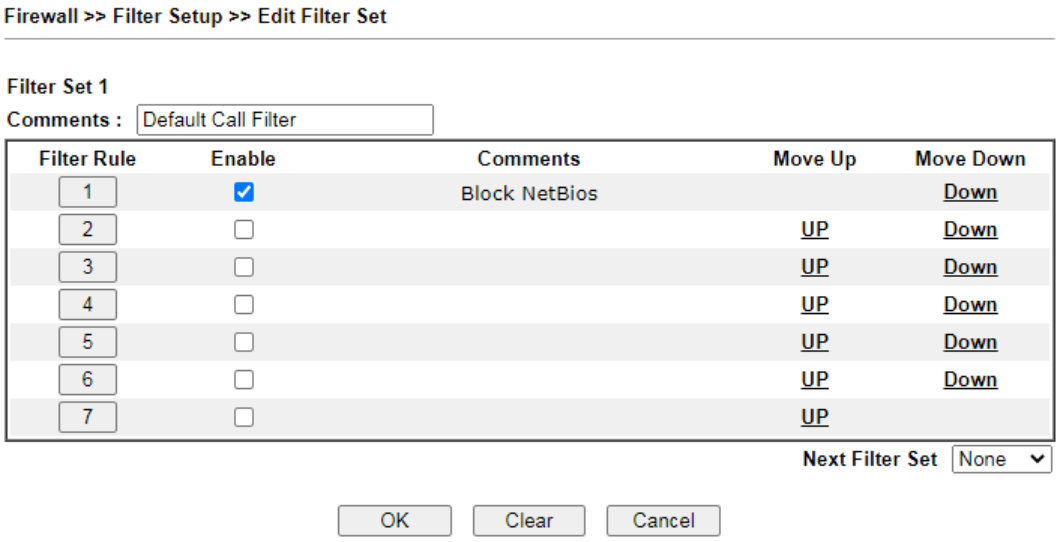
After finishing all the settings here, please click **OK** to save the configuration.

3.4.3 Filter Setup

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



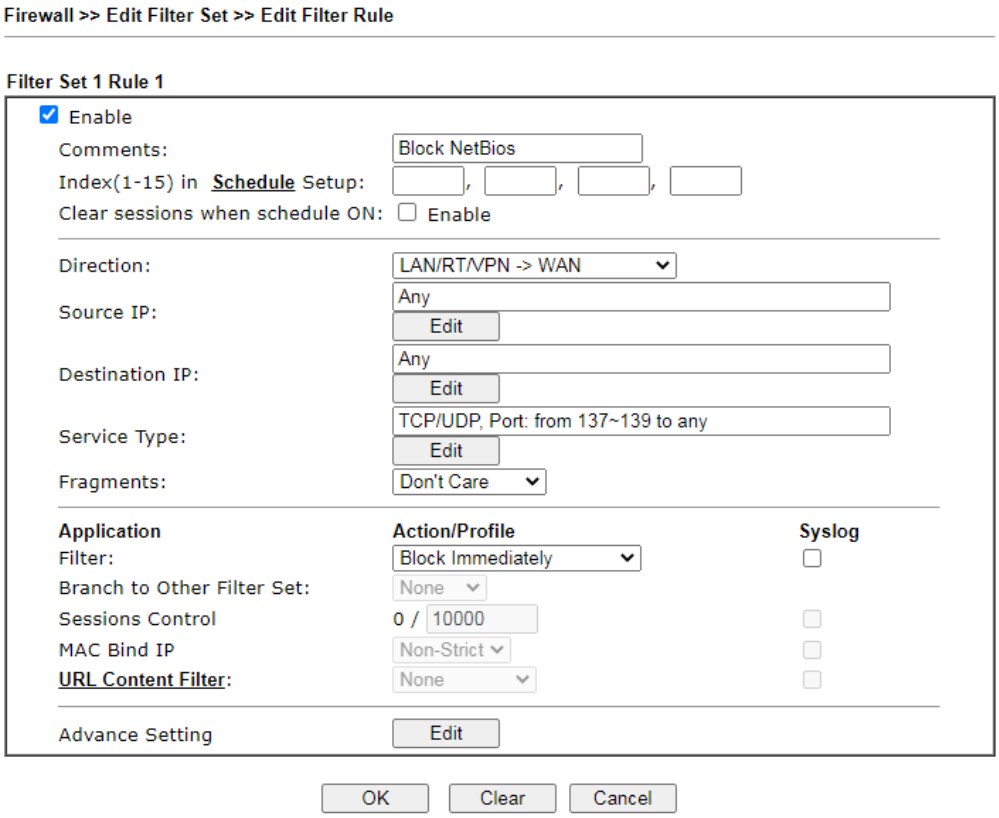
To edit or add a filter, click on the set number to edit the individual set. The following page will be shown. Each filter set contains up to 7 rules. Click on the rule number button to edit each rule. Check **Active** to enable the rule.



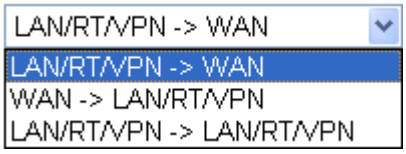
Available settings are explained as follows:

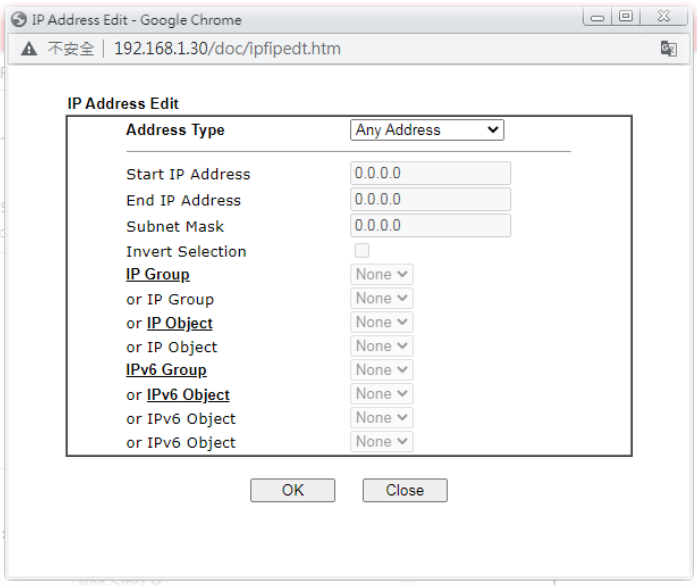
Item	Description
Filter Rule	Click a button numbered (1 ~ 7) to edit the filter rule. Click the button will open Edit Filter Rule web page. For the detailed information, refer to the following page.
Active	Enable or disable the filter rule.
Comment	Enter filter set comments/description. Maximum length 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.



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.  **Note:** RT means routing domain for 2nd subnet or other LAN.
Source/Destination IP	Click **Edit** to access into the following dialog to choose the source/destination IP or IP ranges.

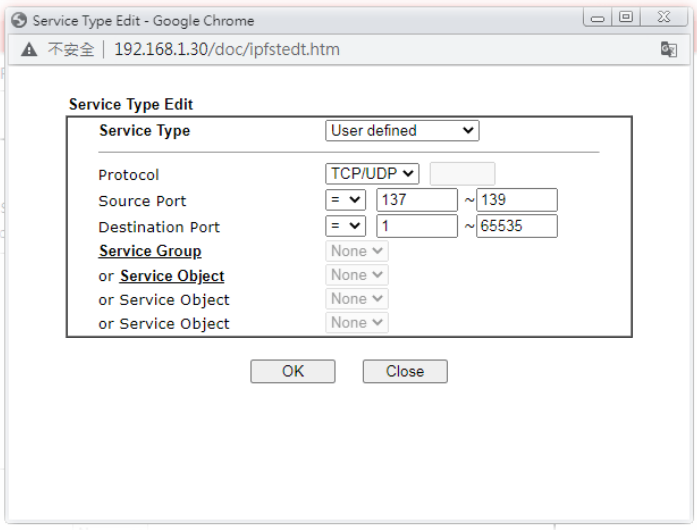


To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose **Group and Objects** as the Address Type.

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

Service Type

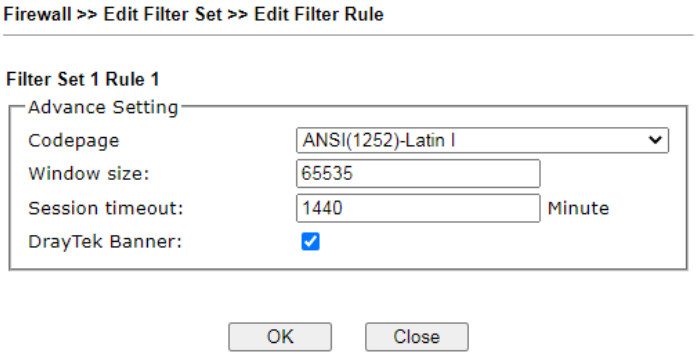
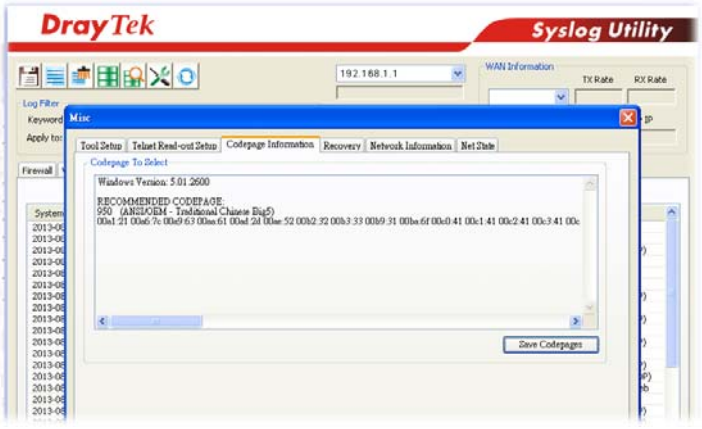
Click **Edit** to access into the following dialog to choose a suitable service type.



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

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

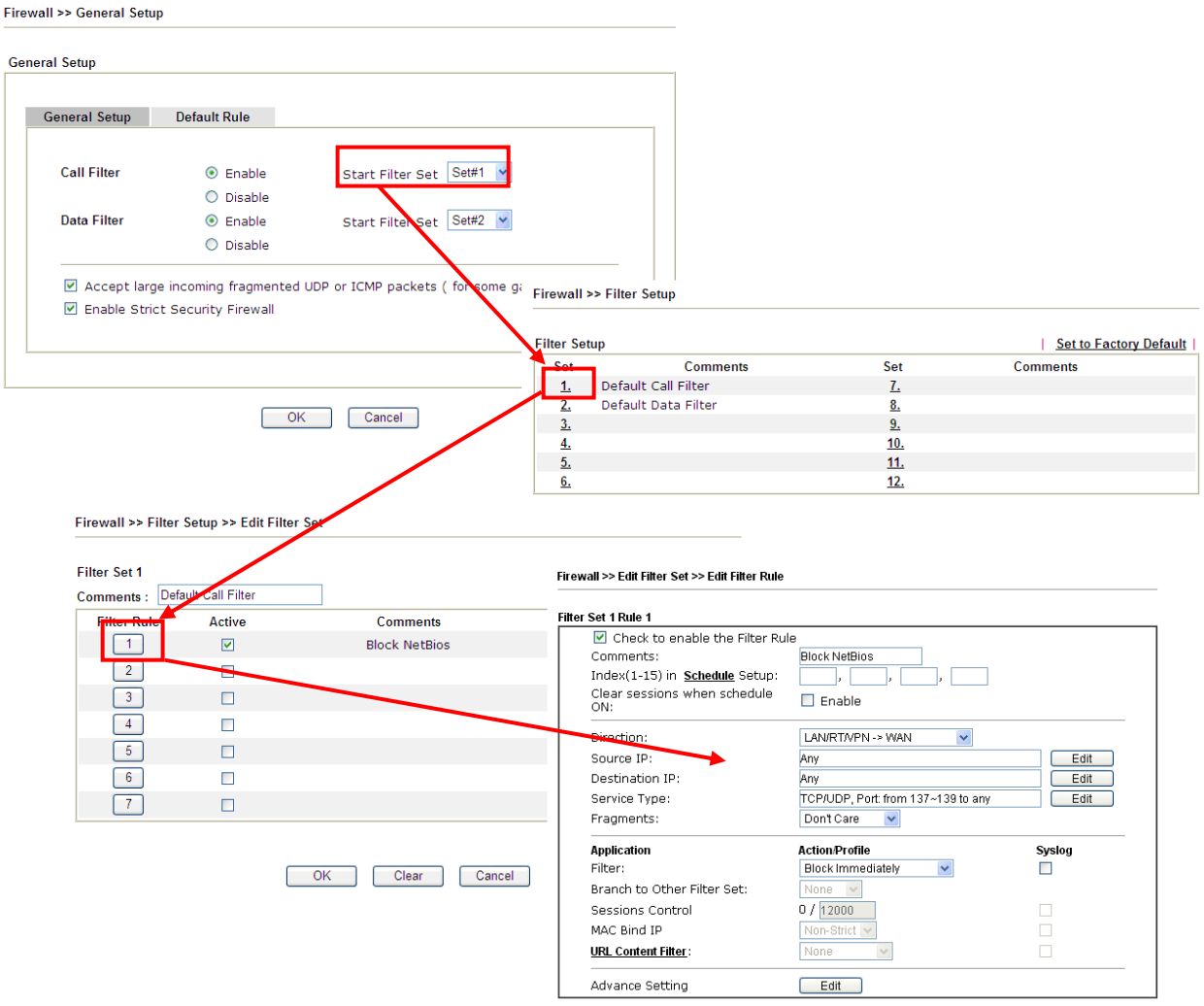
	Source/Destination Port – ***(=)*** – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type. ***(!=)*** – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type. ***(>)*** – the port number greater than this value is available. ***(<)*** – the port number less than this value is available for this profile. **Service Group/Object** - Use the drop down list to choose the one that you want.
Fragments	Specify the action for fragmented packets. And it is used for **Data Filter** only. ***Don't care*** -No action will be taken towards fragmented packets. ***Unfragmented*** -Apply the rule to unfragmented packets. ***Fragmented*** - Apply the rule to fragmented packets. ***Too Short*** - Apply the rule only to packets that are too short to contain a complete header.
Filter	Specifies the action to be taken when packets match the rule. **Block Immediately** - Packets matching the rule will be dropped immediately. **Pass Immediately** - Packets matching the rule will be passed immediately. **Block If No Further Match** - A packet matching the rule, and that does not match further rules, will be dropped. **Pass If No Further Match** - A packet matching the rule, and that does not match further rules, will be passed through.
Branch to other Filter Set	If the packet matches the filter rule, the next filter rule will branch to the specified filter set. Select next filter rule to branch from the drop-down menu. Be aware that the modem will apply the specified filter rule for ever and will not return to previous filter rule any more.
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.
MAC Bind IP	**Strict** – Make the MAC address and IP address settings configured in **IP Object** for **Source IP** and **Destination IP** be bound for applying such filter rule. **No-Strict** - no limitation.
URL Content Filter	Select one of the **URL Content Filter** profile settings (created in **CSM>> URL Content Filter**) for applying with this modem. 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.
Advance Setting	Click **Edit** to open the following window. However, it is **strongly recommended** to use the default settings here.  **Codepage** - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage. If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.  **Window size** – It determines the size of TCP protocol (0~65535). The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper. **Session timeout**–Setting timeout for sessions can make the best utilization of network resources. However, Queue timeout is configured for TCP protocol only; session timeout is configured for the data flow which matched with the firewall rule.

	DrayTek Banner – Please uncheck this box and the following screen will not be shown for the unreachable web page. The default setting is Enabled. 

Example

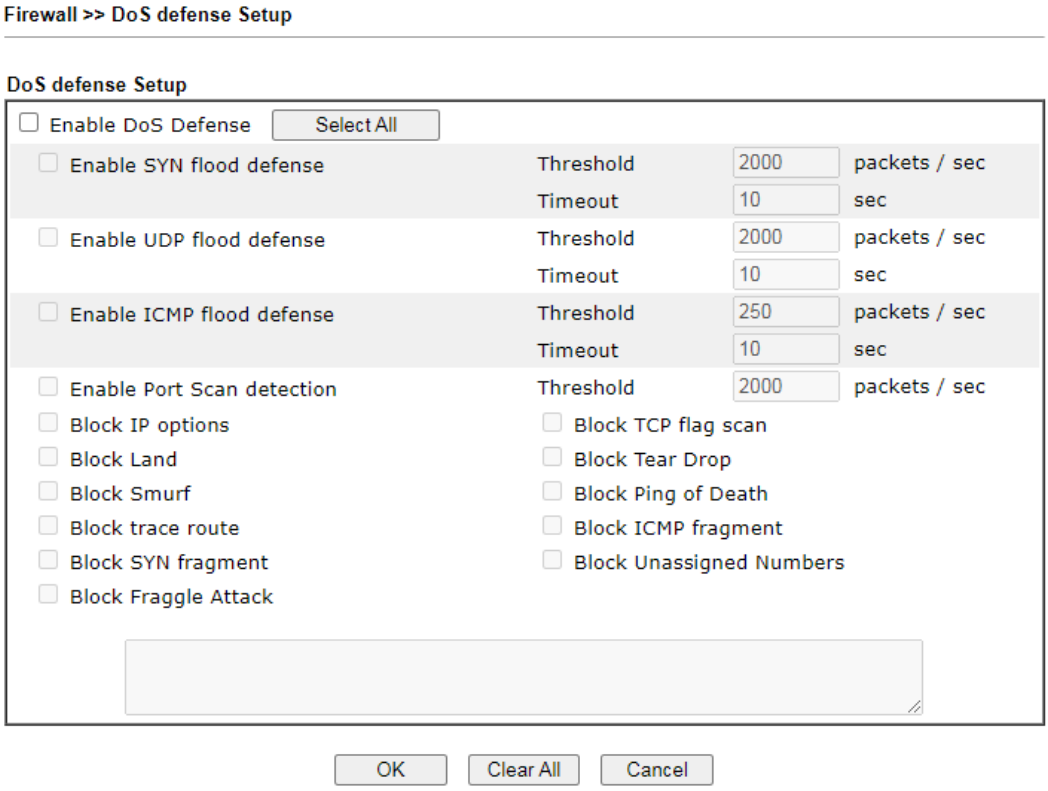
As stated before, all the traffic will be separated and arbitrated using on of two IP filters: call filter or data filter. You may preset 12 call filters and data filters in **Filter Setup** and even link them in a serial manner. Each filter set is composed by 7 filter rules, which can be further defined. After that, in **General Setup** you may specify one set for call filter and one set for data filter to execute first.



3.4.4 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.

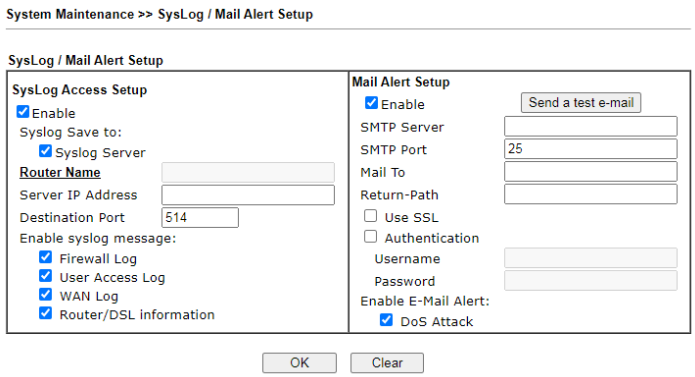
Click **Firewall** and click **DoS Defense** to open the setup page.

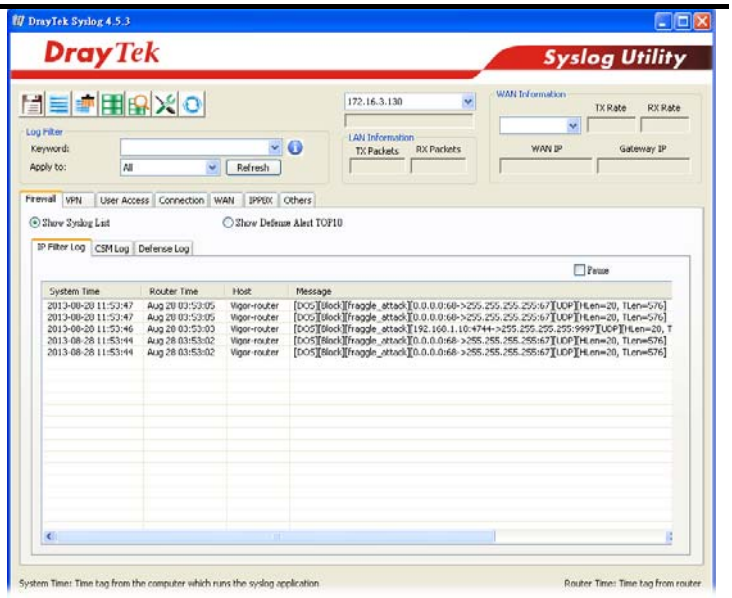


Available settings are explained as follows:

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	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 modem 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 modem. By default, the threshold and timeout values are set to 50 packets per second and 10 seconds, respectively. That means, when 50 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.
Enable UDP flood defense	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 modem will start to randomly discard the subsequent UDP packets for a period defined in Timeout.

	The default setting for threshold and timeout are 150 packets per second and 10 seconds, respectively. That means, when 150 packets per second received, they will be regarded as “attack event” and the session will be paused for 10 seconds.
Enable ICMP flood defense	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 modem will discard the ICMP echo requests coming from the Internet. The default setting for threshold and timeout are 50 packets per second and 10 seconds, respectively. That means, when 50 packets per second received, they will be regarded as “attack event” and the session will be paused for 10 seconds.
Enable PortScan detection	Port Scan attacks the Vigor modem 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 modem will send out a warning. By default, the Vigor modem sets the threshold as 150 packets per second. That means, when 150 packets per second received, they will be regarded as “attack event”.
Block IP options	Check the box to activate the Block IP options function. The Vigor modem 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.
Block Land	Check the box to enforce the Vigor modem 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.
Block Smurf	Check the box to activate the Block Smurf function. The Vigor modem will ignore any broadcasting ICMP echo request.
Block trace router	Check the box to enforce the Vigor modem not to forward any trace route packets.
Block SYN fragment	Check the box to activate the Block SYN fragment function. The Vigor modem will drop any packets having SYN flag and more fragment bit set.
Block Fraggle Attack	Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked.

	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.
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 *no flag scan*, *FIN without ACK scan*, *SYN FINscan*, *Xmas scan* and *full Xmas scan*.
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 modem 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 modems 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 modem should have ability to detect and reject this kind of packets.
Warning Messages	We provide Syslog function for user to retrieve message from Vigor modem. The user, as a Syslog Server, shall receive the report sending from Vigor modem which is a Syslog Client. All the warning messages related to **DoS Defense** will be sent to user and user can review it through Syslog daemon. Look for the keyword **DoS** in the message, followed by a name to indicate what kind of attacks is detected. 

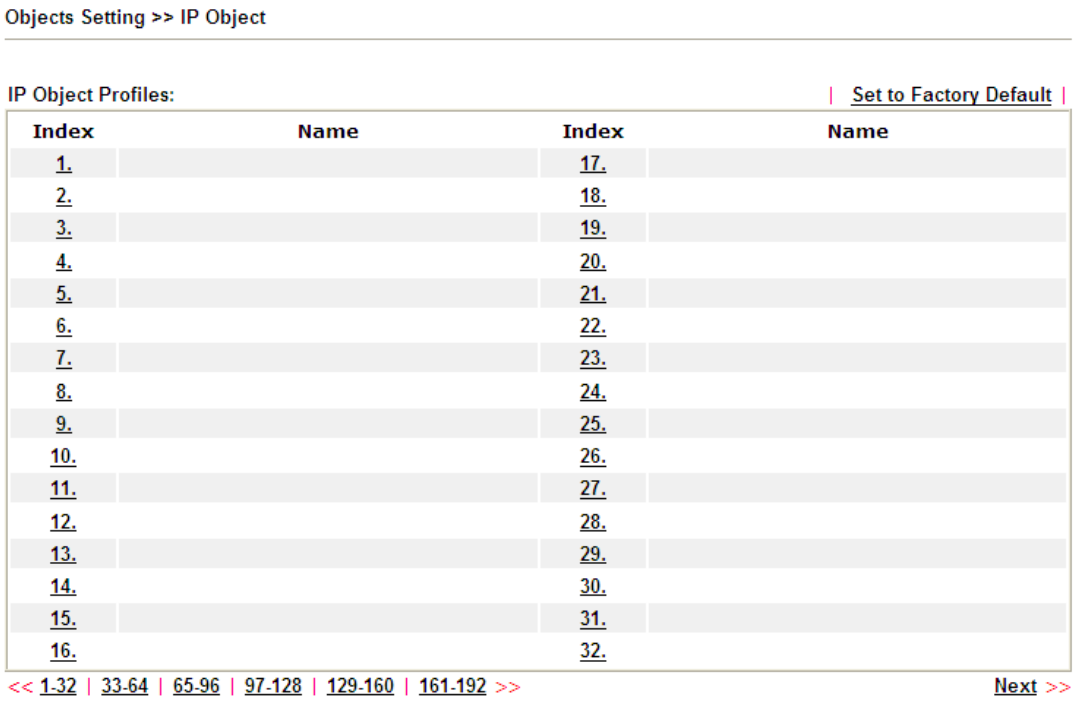

DrayTek Syslog 4.5.3
DrayTek
Syslog Utility
172.16.3.130
WAN Information
TX Rate
RX Rate
Log Filter
Keyword:
Apply to:
All
Refresh
LAN Information
TX Packets
RX Packets
WAN IP
Gateway IP
Firewall
VPN
User Access
Connection
WAN
IPPBX
Others
Show Syslog List
Show Defense Alert TOP10
IP Filter Log
CSM Log
Defense Log
Pause
System Time
Router Time
Host
Message
2013-08-28 11:53:47 Aug 28 03:53:05 Vigor-router [DOS][Block][fraggle_attack][0.0.0.0:68->255.255.255.255:67][UDP][HLen=20, TLen=576]
2013-08-28 11:53:47 Aug 28 03:53:05 Vigor-router [DOS][Block][fraggle_attack][0.0.0.0:68->255.255.255.255:67][UDP][HLen=20, TLen=576]
2013-08-28 11:53:46 Aug 28 03:53:03 Vigor-router [DOS][Block][fraggle_attack][192.168.1.10:4744->255.255.255.255:9997][UDP][HLen=20, T
2013-08-28 11:53:44 Aug 28 03:53:02 Vigor-router [DOS][Block][fraggle_attack][0.0.0.0:68->255.255.255.255:67][UDP][HLen=20, TLen=576]
2013-08-28 11:53:44 Aug 28 03:53:02 Vigor-router [DOS][Block][fraggle_attack][0.0.0.0:68->255.255.255.255:67][UDP][HLen=20, TLen=576]
System Time: Time tag from the computer which runs the syslog application
Router Time: Time tag from router

3.5 Objects Settings

For IPs in a range and service ports in a limited range usually will be applied in configuring modem'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).

3.5.1 IP Object

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



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:

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Interface	Choose a proper interface. For example, the **Direction** setting in **Edit Filter Rule** will ask you specify IP or IP range for WAN or LAN or any IP address. If you choose LAN as the **Interface** here, and choose LAN as the direction setting in **Edit Filter Rule**, then all the IP addresses specified with LAN interface will be opened for you to choose in **Edit Filter Rule** page.
Address Type	Determine the address type for the IP address. Select **Single Address** if this object contains one IP address only. Select **Range Address** if this object contains several IPs within a range. Select **Subnet Address** if this object contains one subnet for IP address. Select **Any Address** if this object contains any IP address. Select **Mac Address** if this object contains Mac address.
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.

3. 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
1.	RD Department	17.
2.	Financial Dept	18.
3.	HR Department	19.
4.		20.
5.		21.
6.		22.

3.5.2 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.	

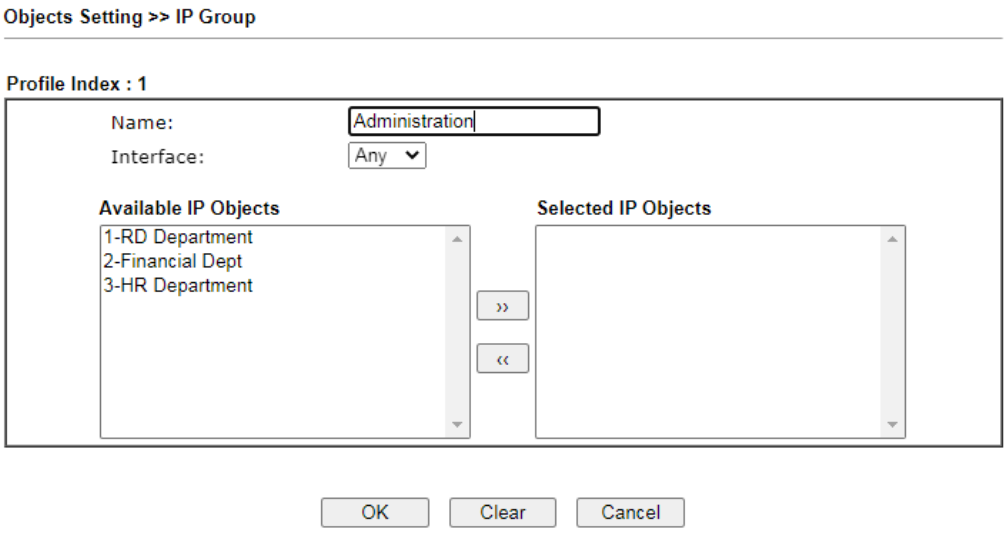
Available settings are explained as follows:

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:



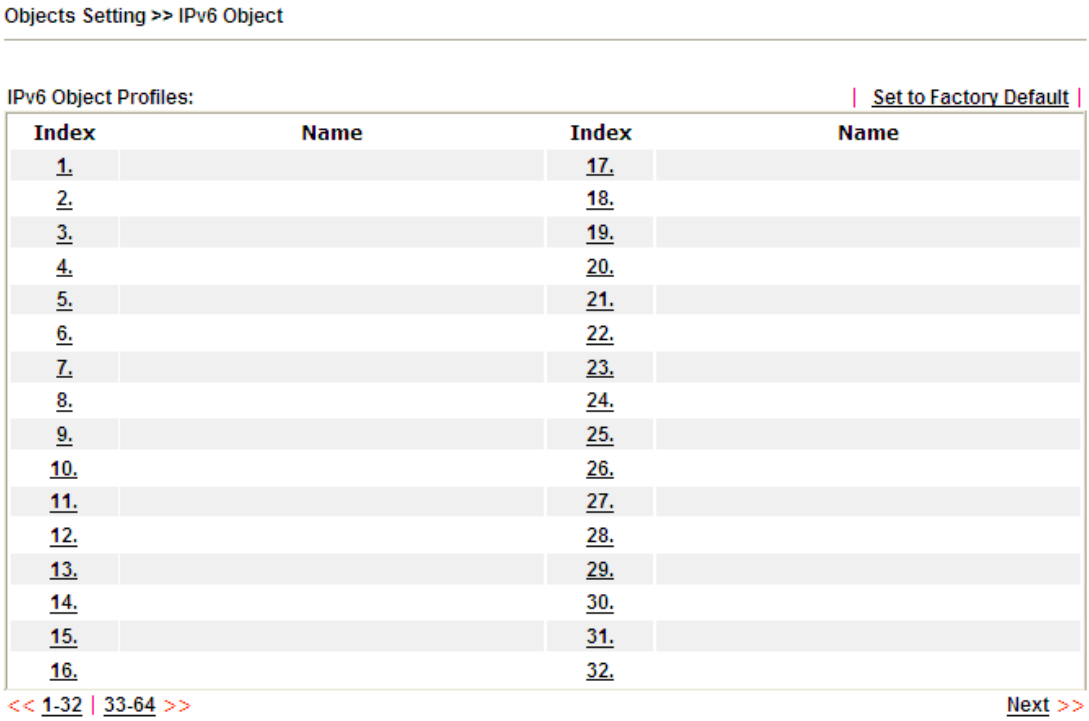
Available settings are explained as follows:

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.

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

3.5.3 IPv6 Object

You can set up to 64 sets of IPv6 Objects with different conditions.

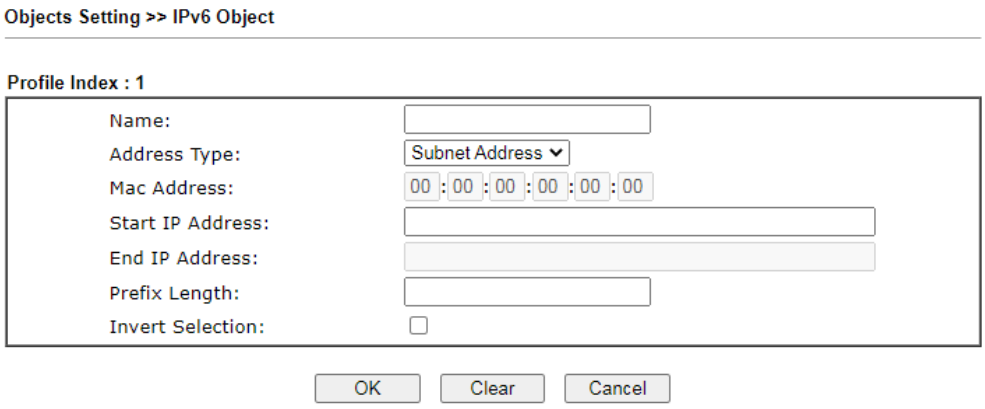


Available settings are explained as follows:

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:



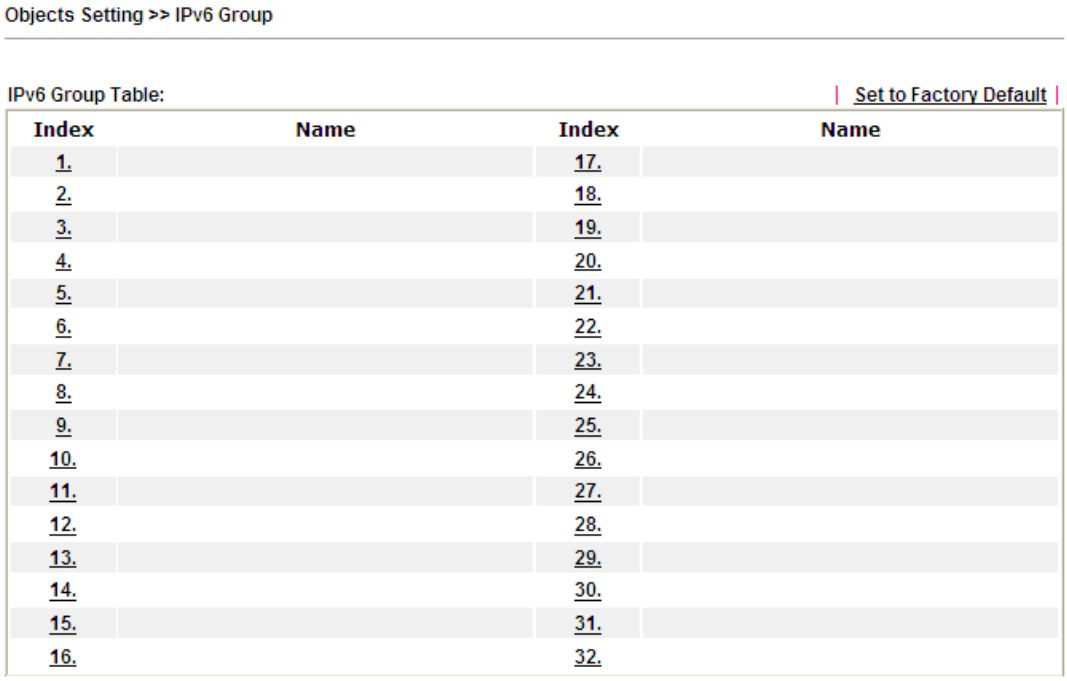
Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Address Type	Determine the address type for the IPv6 address. Select **Single Address** if this object contains one IPv6 address only. Select **Range Address** if this object contains several IPv6s within a range. Select **Subnet Address** if this object contains one subnet for IPv6 address. Select **Any Address** if this object contains any IPv6 address. Select **Mac Address** if this object contains Mac address.
Mac Address	Type the MAC address of the network card which will be controlled.
Start IP Address	Type the start IP address for Single Address type.
End IP Address	Type the end IP address if the Range Address type is selected.
Prefix Len	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.

3.5.4 IPv6 Group

This page allows you to bind several IPv6 objects into one IPv6 group.

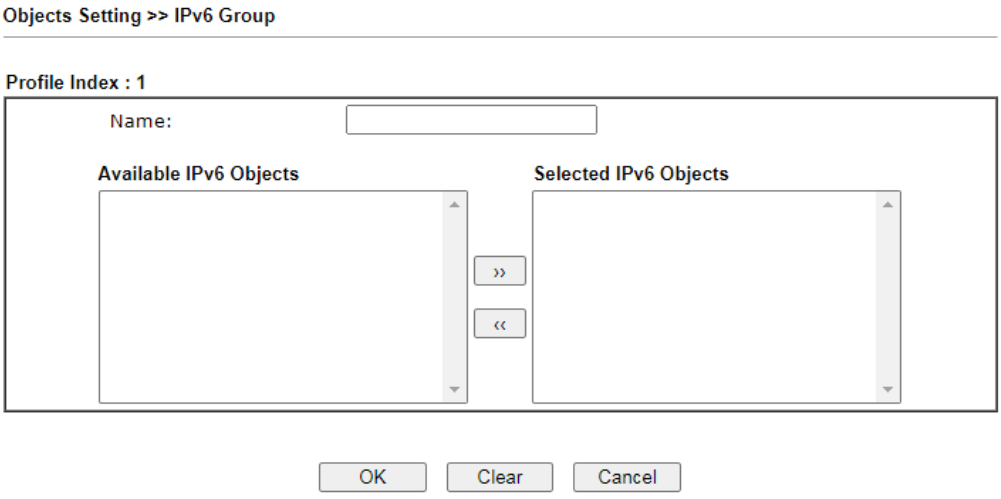


Available settings are explained as follows:

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:



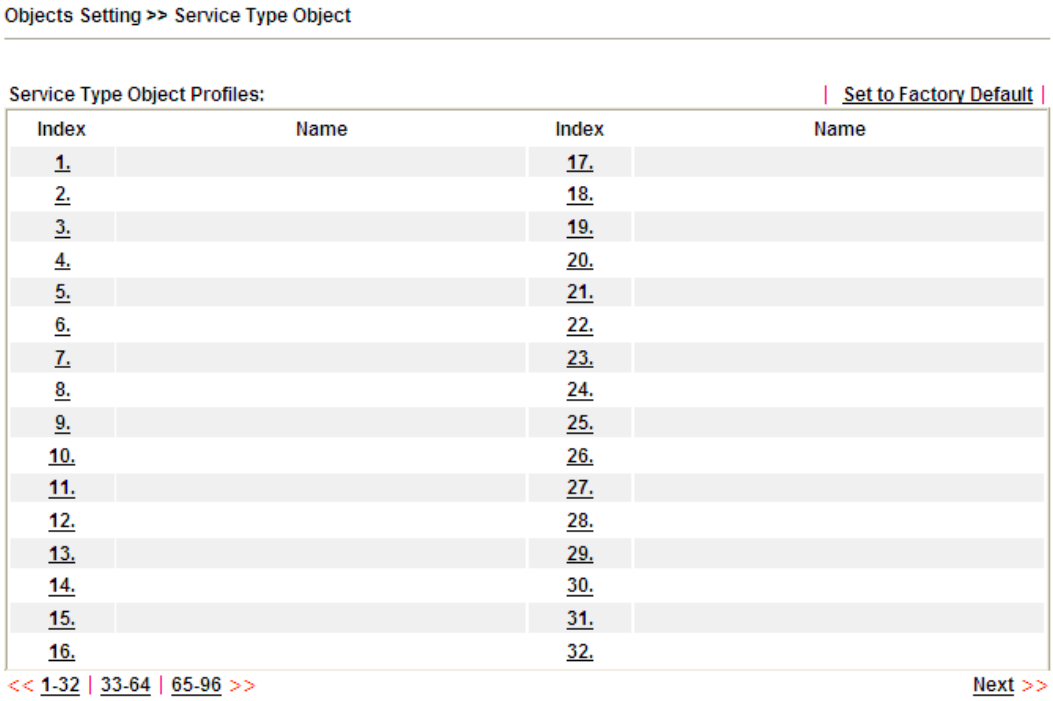
Available settings are explained as follows:

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.

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

3.5.5 Service Type Object

You can set up to 96 sets of Service Type Objects with different conditions.

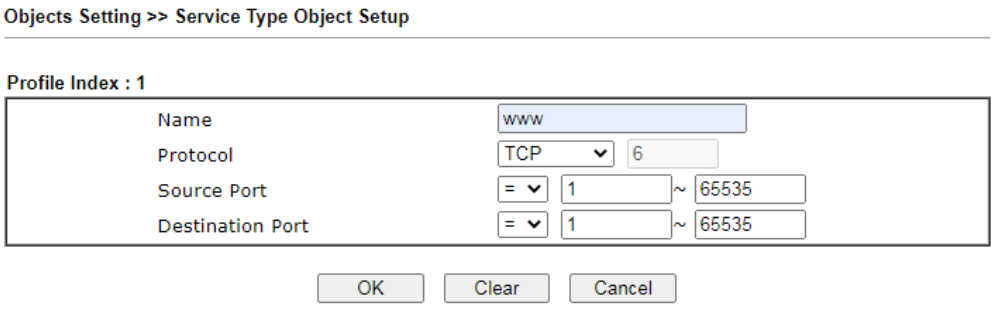


Available settings are explained as follows:

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:

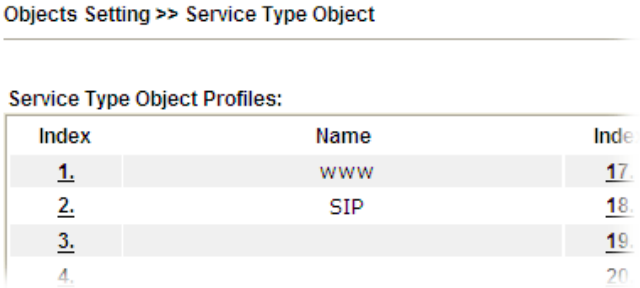
1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:



Available settings are explained as follows:

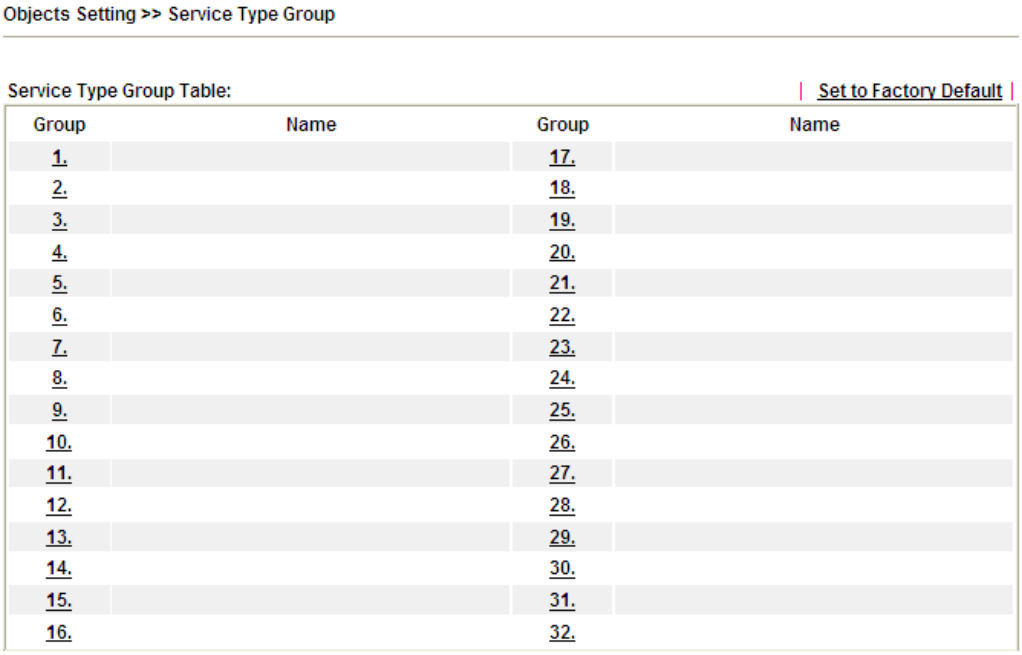
Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Protocol	Specify the protocol(s) which this profile will apply to.
Source/Destination Port	**Source Port** and the **Destination Port** column are available for TCP/UDP protocol. It can be ignored for other protocols. 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.

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



3.5.6 Service Type Group

This page allows you to bind several service types into one group.

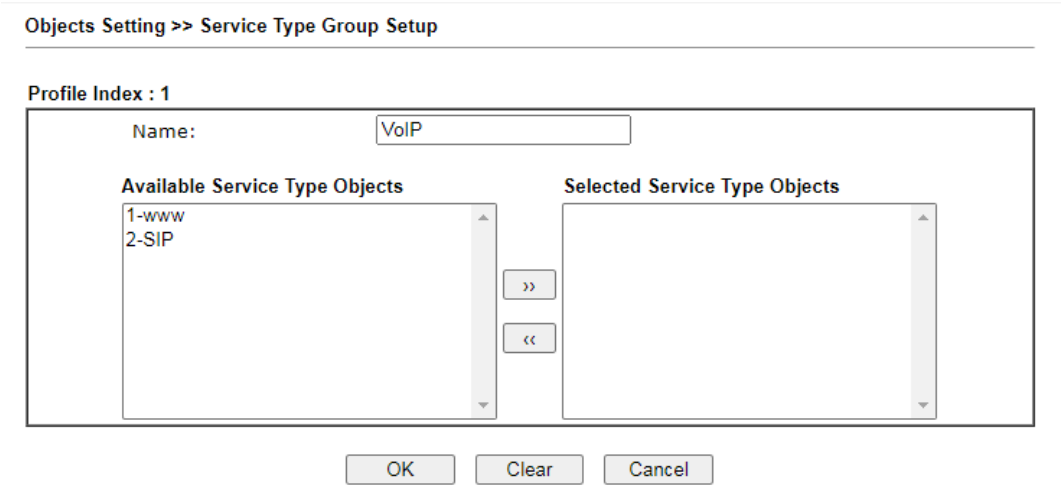


Available settings are explained as follows:

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:



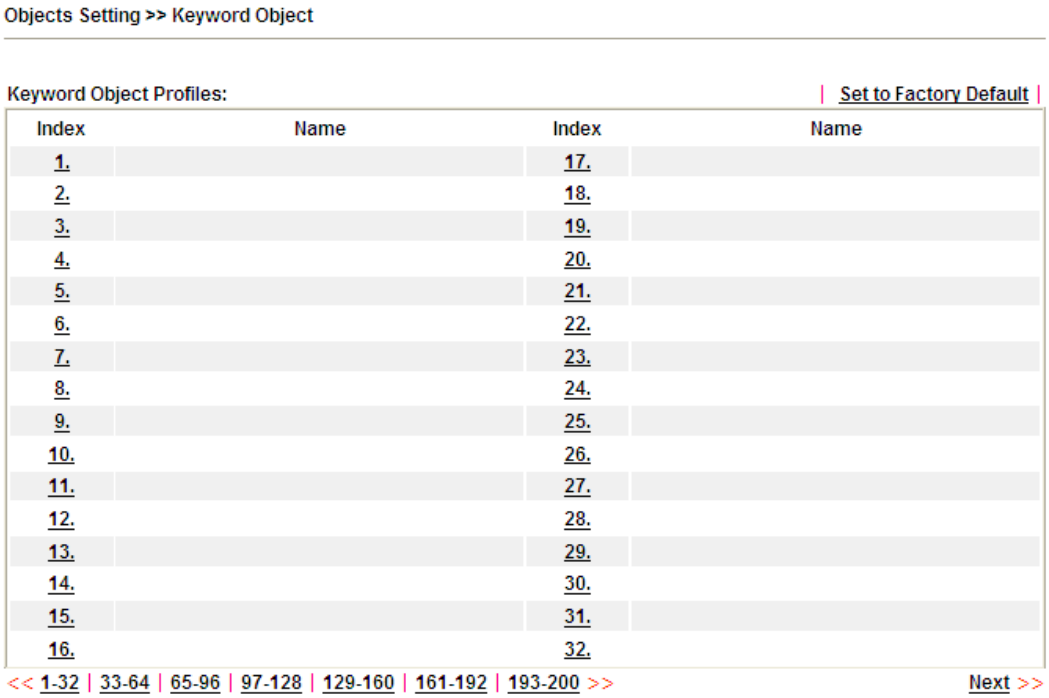
Available settings are explained as follows:

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.

3.5.7 Keyword Object

You can set 200 keyword object profiles for choosing as black /white list in **CSM >>URL Web Content Filter Profile.**

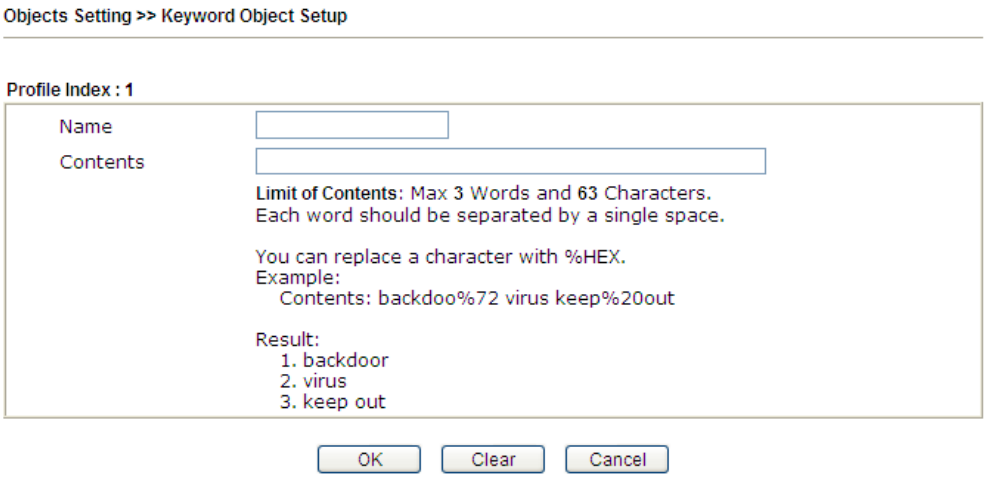


Available settings are explained as follows:

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:



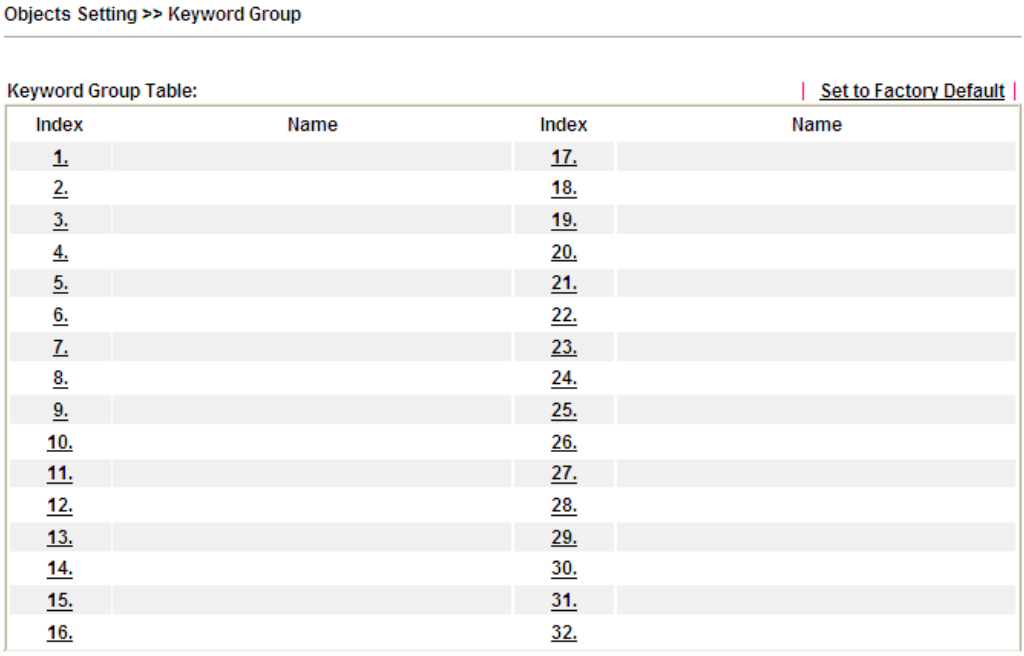
Available settings are explained as follows:

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 *gambling* 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.

3.5.8 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**.

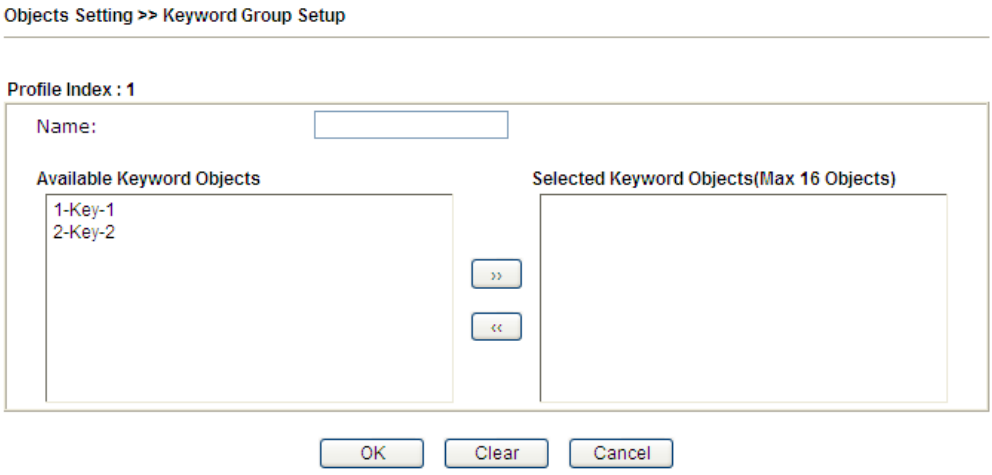


Available settings are explained as follows:

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:



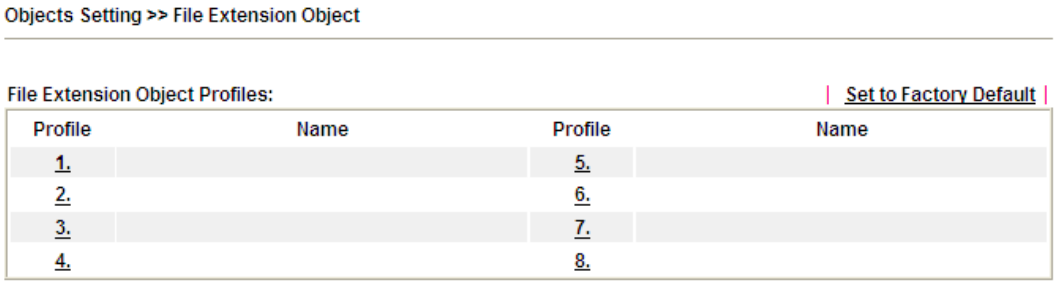
Available settings are explained as follows:

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

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

3.5.9 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.

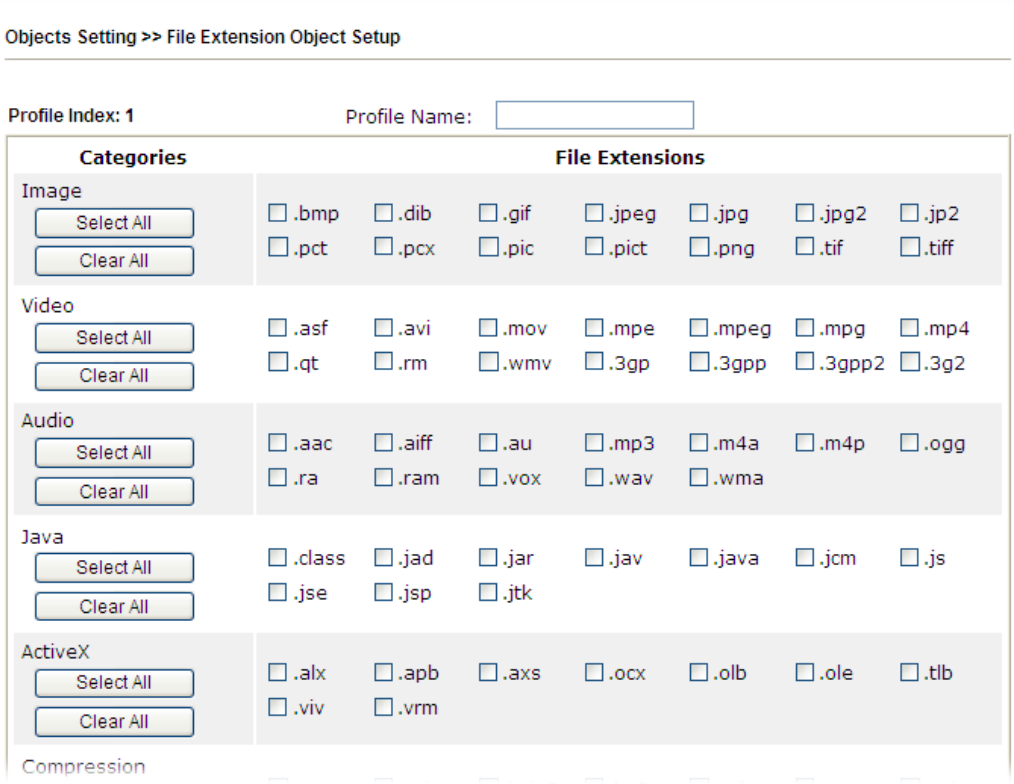


Available settings are explained as follows:

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:



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 modem. Finally, click **OK** to save this profile.

3.6 CSM Profile

Content Security Management (CSM)

CSM is an abbreviation of **Content Security Management** which is used to control IM/P2P usage, filter the web content and URL content to reach a goal of security management.

URL Content Filter

To provide an appropriate cyberspace to users, Vigor modem 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

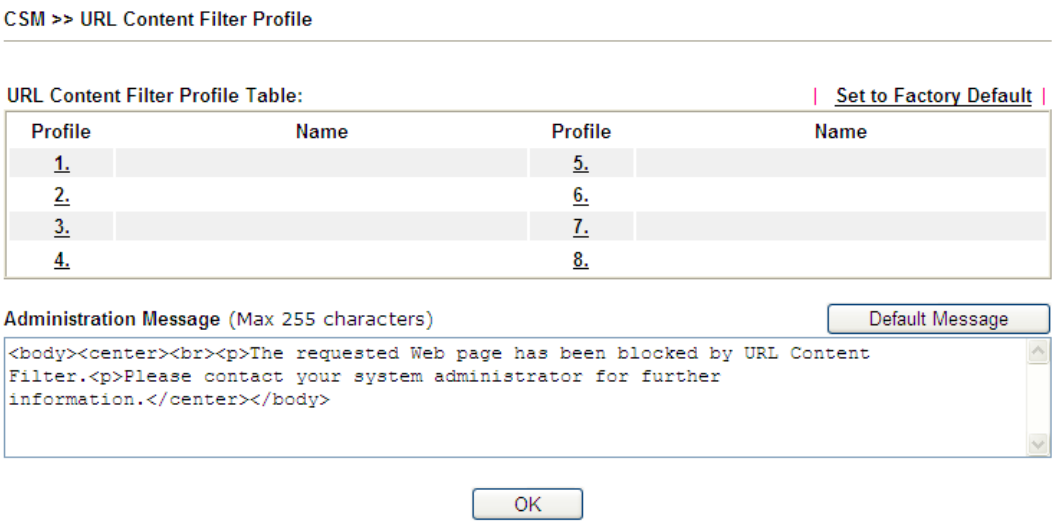
URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.

On the other hand, Vigor modem 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 modem 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".

3.6.1 URL Content Filter Profile

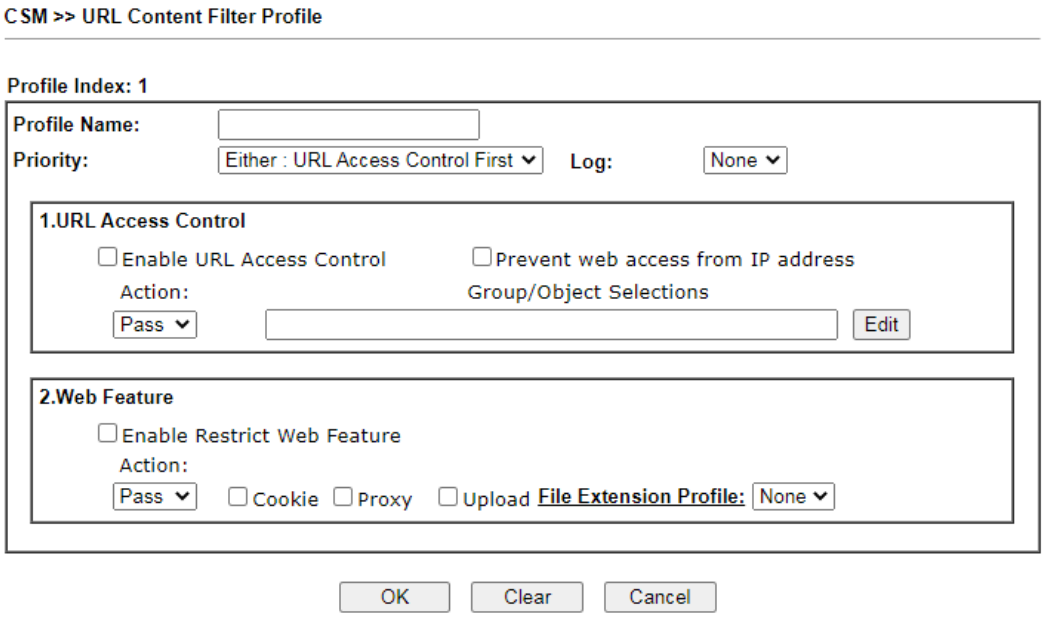
Click **CSM** and click **URL Content Filter Profile** to open the profile setting page.



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 -** Click this button to apply the default message offered by the modem.

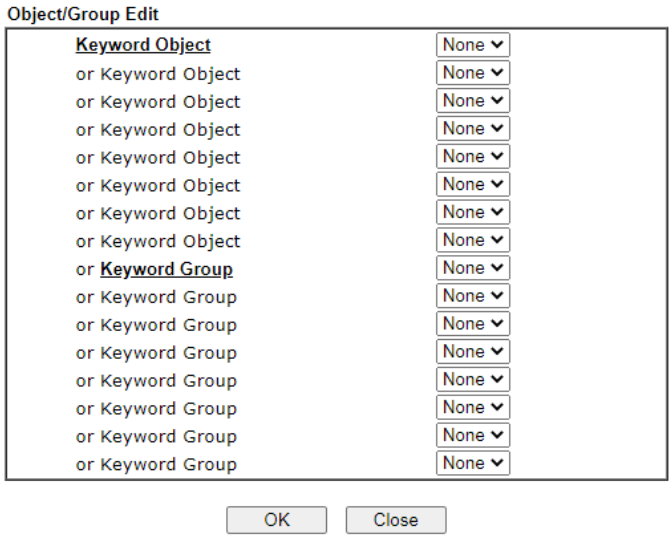
You can set eight profiles as URL content filter. Simply click the index number under Profile to open the following web page.



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	It determines the action that this modem will apply. **Both: Pass** – The modem 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. **Both:Block** –The modem 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. **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 modem will process the packages with the conditions set below for URL first, then Web feature second. **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 modem will process the packages with the conditions set below for web feature first, then URL second.
Log	**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.
URL Access Control	**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 modem will execute the action specified in this field and ignore the action specified under Restrict Web Feature. **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. **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 keyword set here, it will be processed with reverse action. **Group/Object Selections** – The Vigor modem 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 modem 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 modem performs.



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 Firs** is selected. **Pass** allows accessing into the corresponding webpage with the keywords listed on the box below.
***Pass* -** Allow accessing into the corresponding webpage with the keywords listed on the box below.

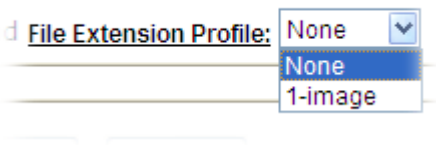
***Block* -** Restrict accessing into the corresponding webpage with the keywords listed on the box below.
If the web pages do not match with the specified feature set here, it will be processed with reverse action.

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

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

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

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



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

3.7 Applications

Below shows the menu items for Applications.

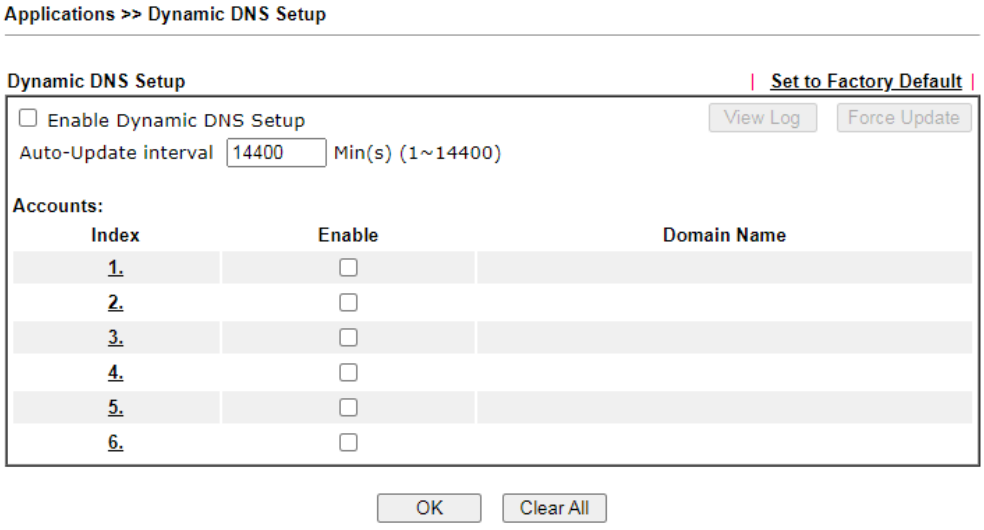
3.7.1 Dynamic DNS

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 modem 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 modem to update its online WAN IP address mappings on the specified Dynamic DNS server. Once the modem is online, you will be able to use the registered domain name to access the modem or internal virtual servers from the Internet. It is particularly helpful if you host a web server, FTP server, or other server behind the modem.

Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers. The modem provides up to three accounts from three different DDNS service providers. Basically, Vigor modems 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 modem.

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. In the DDNS setup menu, check **Enable Dynamic DNS Setup**.

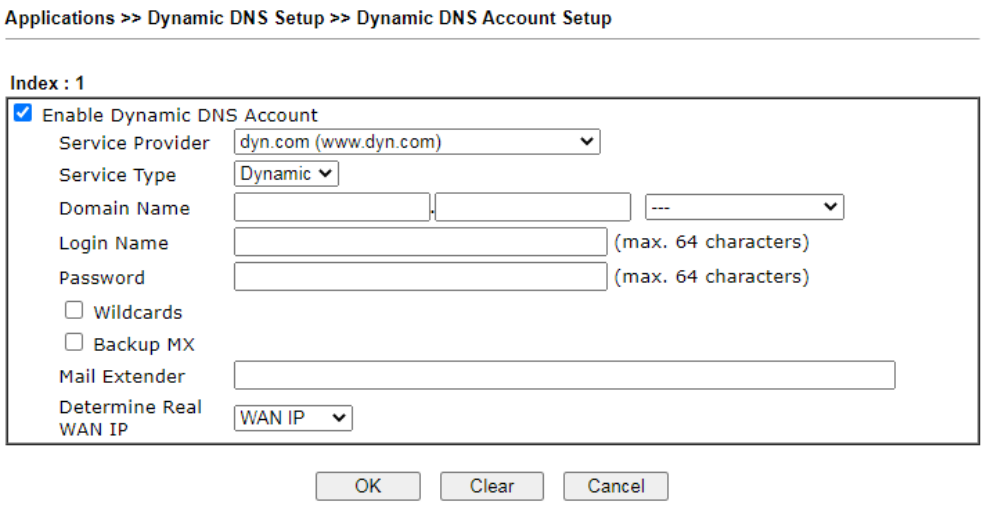


Available settings are explained as follows:

Item	Description
Enable Dynamic DNS Setup	Check this box to enable DDNS function.

Set to Factory Default	Clear all profiles and recover to factory settings.
View Log	Display DDNS log status.
Force Update	Force the modem updates its information to DDNS server.
Auto-Update interval	Set the time for the modem 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.

3. Select Index number 1 to add an account for the modem. 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*.



Available settings are explained as follows:

Item	Description
Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
Service Provider	Select the service provider for the DDNS account.
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.
Domain Name	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.
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.
Force WAN IP Update	When the IP address of the WAN interface in Vigor modem is private IP, the system will detect the Public IP used by the modem in front of Vigor modem and use that Public IP to update DDNS server forcefully.
Determine Real WAN IP	If a Vigor modem is installed behind any NAT modem, you can enable such function to locate the real WAN IP. When the WAN IP used by Vigor modem is private IP, this function can detect the public IP used by the NAT modem and use the detected IP address for DDNS update. There are two methods offered for you to choose: **WAN IP** - If it is selected and the WAN IP of Vigor modem is private, DDNS update will take place right away. **Internet IP** – If it is selected and the WAN IP of Vigor modem is private, it will be converted to public IP before DDNS update takes place.

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

The Wildcard and Backup MX features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.

Disable the Function and Clear all Dynamic DNS Accounts

In the DDNS setup menu, uncheck **Enable Dynamic DNS Setup**, and push **Clear All** button to disable the function and clear all accounts from the modem.

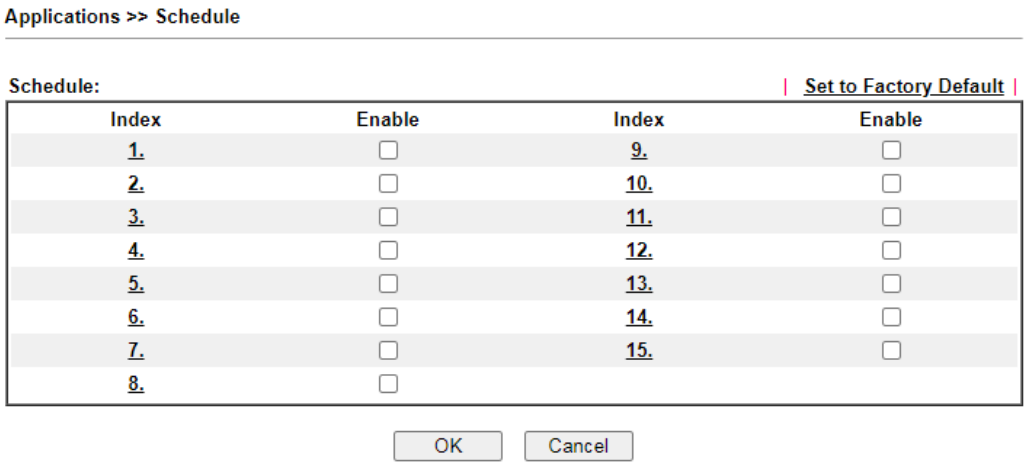
Delete a Dynamic DNS Account

In the DDNS setup menu, click the **Index** number you want to delete and then push **Clear All** button to delete the account.

3.7.2 Schedule

The Vigor modem has a built-in real time clock which can update itself manually or automatically by means of Network Time Protocols (NTP). As a result, you can not only schedule the modem 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 modem's clock to current time of your PC. The clock will reset once if you power down or reset the modem. There is another way to set up time. You can inquiry an NTP server (a time server) on the Internet to synchronize the modem's clock. This method can only be applied when the WAN connection has been built up.



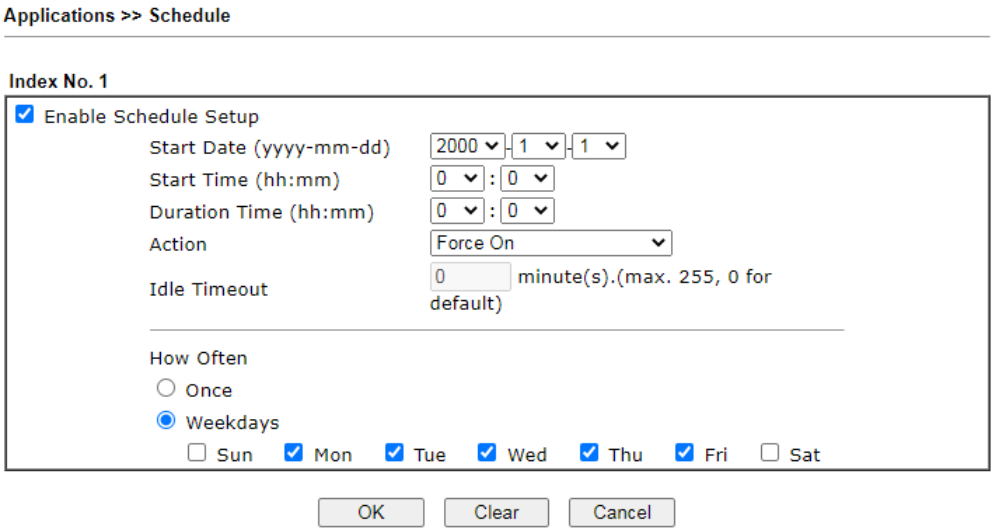
Available settings are explained as follows:

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** 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.



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.

3. Click **OK** button to save the settings.

Example

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

Office Hour:

(Force On)

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

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

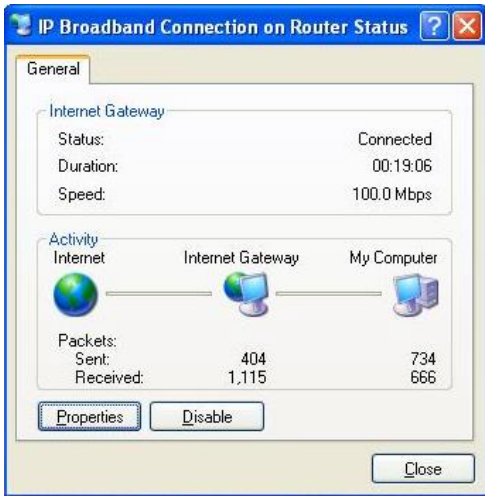
3.7.3 UPnP

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 modems, the major feature of UPnP on the modem is “NAT Traversal”. This enables applications inside the firewall to automatically open the ports that they need to pass through a modem. It is more reliable than requiring a modem to work out by itself which ports need to be opened. Further, the user does not have to manually set up port mappings or a DMZ. **UPnP is available on Windows XP** and the modem provide the associated support for MSN Messenger to allow full use of the voice, video and messaging features.

Available settings are explained as follows:

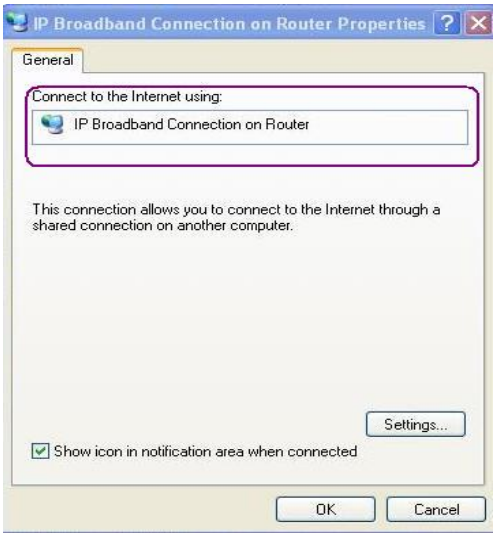
Item	Description
Enable UPNP Service	Accordingly, you can enable either the **Connection Control Service** or **Connection Status Service**.

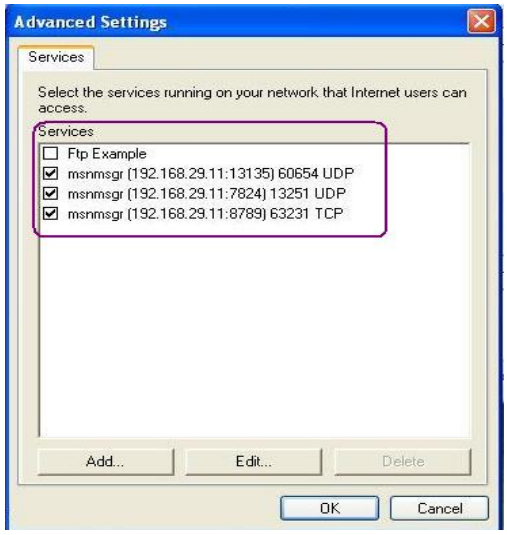
After setting **Enable UPNP Service** setting, an icon of **IP Broadband Connection on Modem** on Windows XP/Network Connections will appear. The connection status and control status will be able to be activated. The NAT Traversal of UPnP enables the multimedia features of your applications to operate. This has to manually set up port mappings or use other similar methods. The screenshots below show examples of this facility.



The UPnP facility on the modem enables UPnP aware applications such as MSN Messenger to discover what are behind a NAT modem. The application will also learn the external IP

address and configure port mappings on the modem. Subsequently, such a facility forwards packets from the external ports of the modem to the internal ports used by the application.





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 modem functions, including removing and adding port mappings.

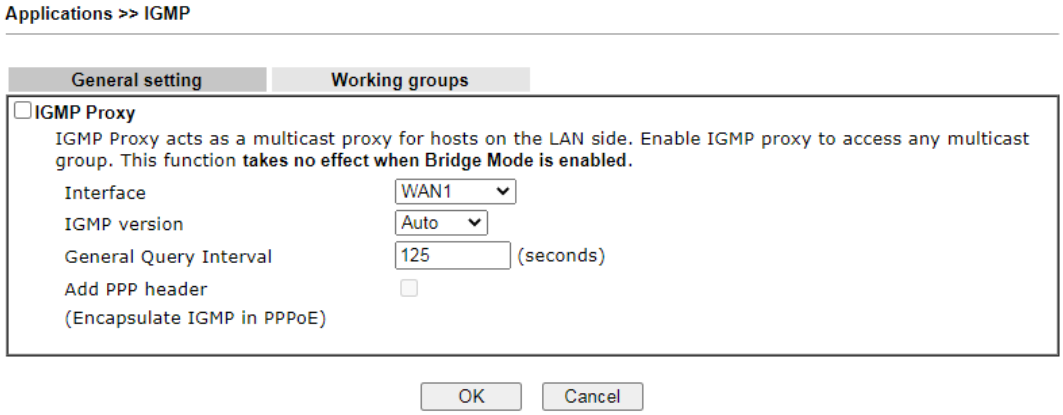
The UPnP function dynamically adds port mappings on behalf of some UPnP-aware applications. When the applications terminate abnormally, these mappings may not be removed.

3.7.4 IGMP

Internet Group Management Protocol (IGMP) is an IPv4 communication protocol for establishing multicast group memberships.

To configure IGMP settings, from the Main Menu select **Applications** >> **IGMP**.

3.7.4.1 General Setting



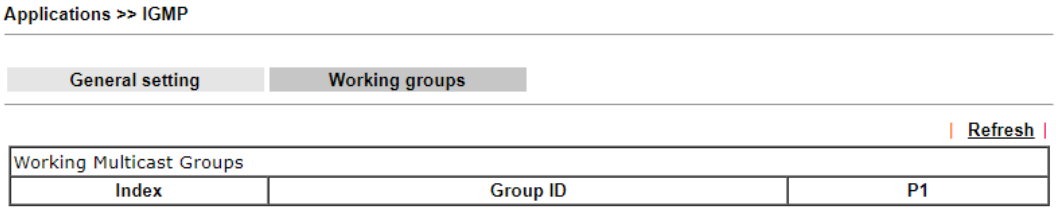
Available settings are explained as follows:

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

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

3.7.4.2 Working Status

Displays a list of active multicast groups.



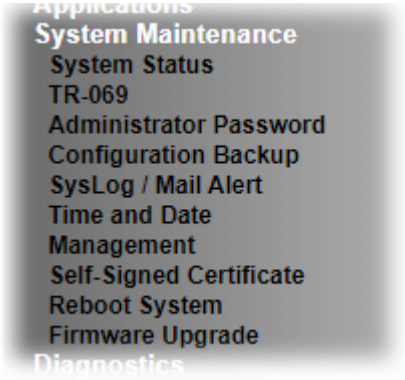
Available settings are explained as follows:

Item	Description
Refresh	Click to reload the Multicast Group Table with the latest information.
Index	Index number of the multicast group.
Group ID	ID port of the multicast group, which is within the IP range reserved for IGMP, 224.0.0.0 through 239.255.255.254.
P1 to P4	LAN ports that have IGMP hosts joined to this multicast group.

3.8 System Maintenance

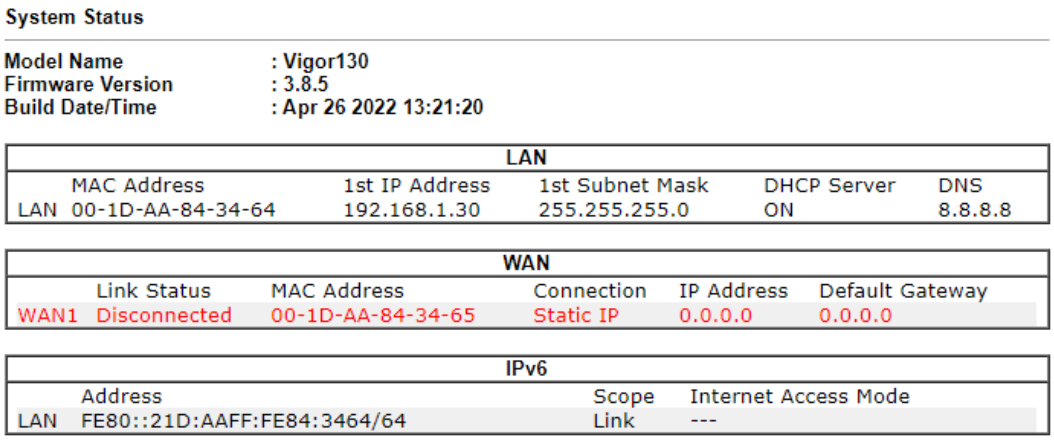
For the system setup, there are several items that you have to know the way of configuration: Status, Administrator Password, Configuration Backup, Syslog, Time setup, Reboot System, Firmware Upgrade.

Below shows the menu items for System Maintenance.



3.8.1 System Status

The **System Status** provides basic network settings of Vigor modem. It includes LAN and WAN interface information. Also, you could get the current running firmware version or firmware related information from this presentation.



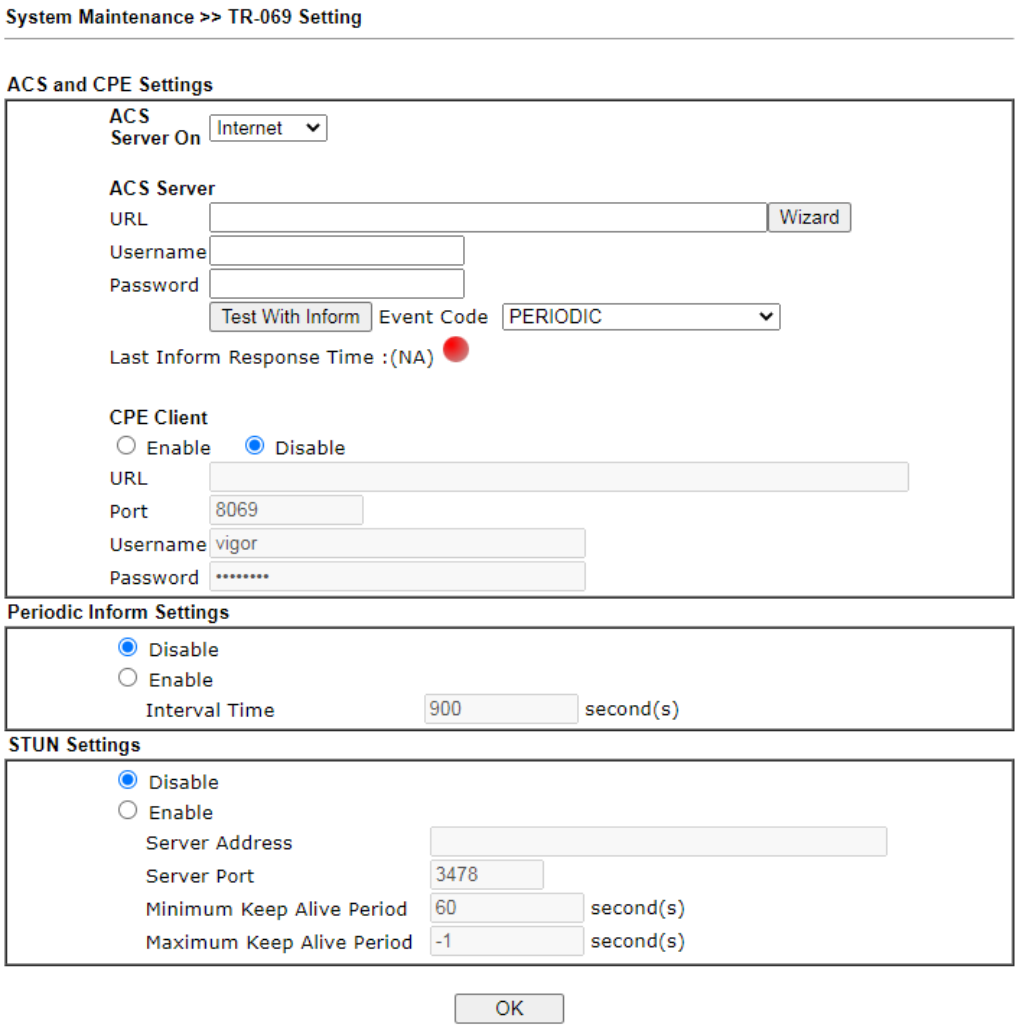
Available settings are explained as follows:

Item	Description
Model Name	Display the model name of the modem.
Firmware Version	Display the firmware version of the modem.
Build Date/Time	Display the date and time of the current firmware build.
LAN	**MAC Address** - Display the MAC address of the LAN Interface. **1st IP Address** - Display the IP address of the LAN interface. **1st Subnet Mask** - Display the subnet mask address of the LAN interface. **DHCP Server**

	- Display the current status of DHCP server of the LAN interface **DNS** - Display the assigned IP address of the primary DNS.
WAN	**Link Status** - Display current connection status. **MAC Address** - Display the MAC address of the WAN Interface. **Connection** - Display the connection type. **IP Address** - Display the IP address of the WAN interface. **Default Gateway** - Display the assigned IP address of the default gateway.
IPv6	**Address -** Display the IPv6 address for LAN. **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. **Internet Access Mode –** Display the connection mode chosen for accessing into Internet.

3.8.2 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.



Available settings are explained as follows:

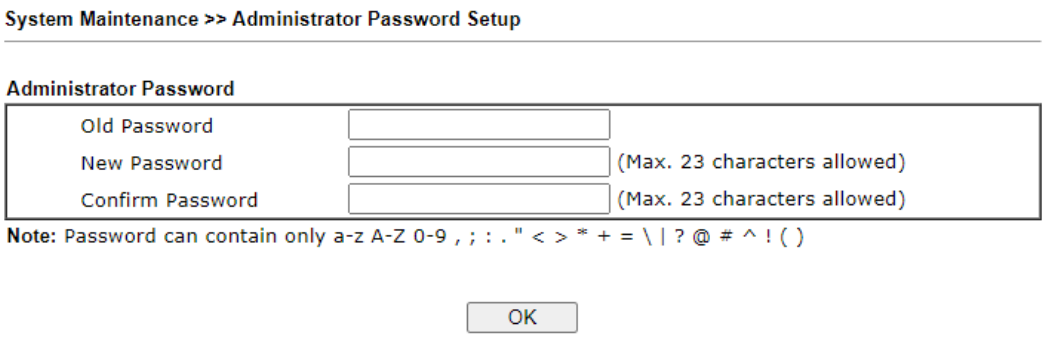
Item	Description
ACS Server On	Choose the interface for the modem connecting to ACS server.
ACS Server	**URL/Username/Password –** Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information. **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. **Event Code** – Use the drop down menu to specify an event to perform the test. **Last Inform Response Time** – Display the time that VigorACS server made a response while receiving Inform message from CPE last time.

CPE Client	Such information is useful for Auto Configuration Server. **Enable/Disable** – Allow/Deny the CPE Client to connect with Auto Configuration Server. **Port** – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE. **Username and Password** – Type the username and password that VigorACS can use to access into such CPE.
Periodic Inform Settings	The default setting is **Enable**. Please set interval time or schedule time for the modem to send notification to CPE. Or click **Disable** to close the mechanism of notification.
STUN Settings	The default is **Disable**. If you click **Enable**, please type the relational settings listed below: **Server IP –** Type the IP address of the STUN server. **Server Port –** Type the port number of the STUN server. **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". **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.

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

3.8.3 Administrator Password

This page allows you to set new password.



Available settings are explained as follows:

Item	Description
Old Password	Type in the old password. The factory default setting for password is **"admin"**.
New Password	Type in new password in this field.
Confirm Password	Type in the new password again.

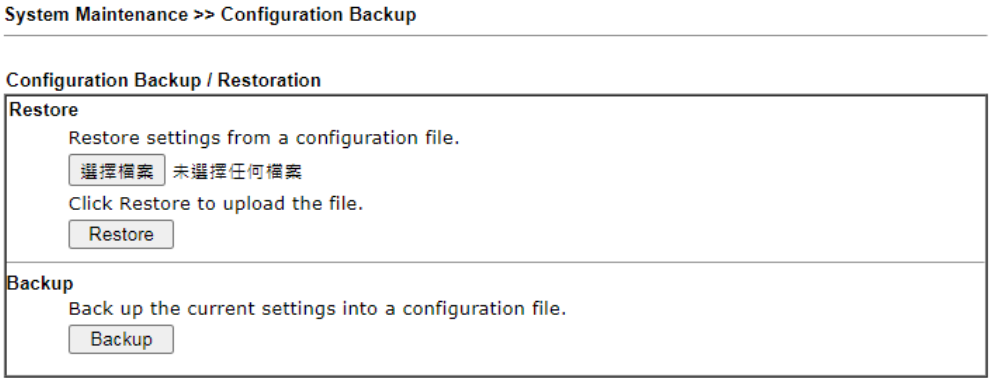
When you click **OK**, the login window will appear. Please use the new password to access into the Web User Interface again.

3.8.4 Configuration Backup

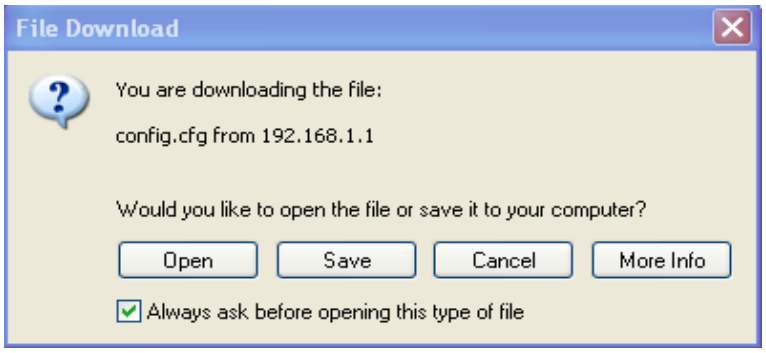
Backup the Configuration

Follow the steps below to backup your configuration.

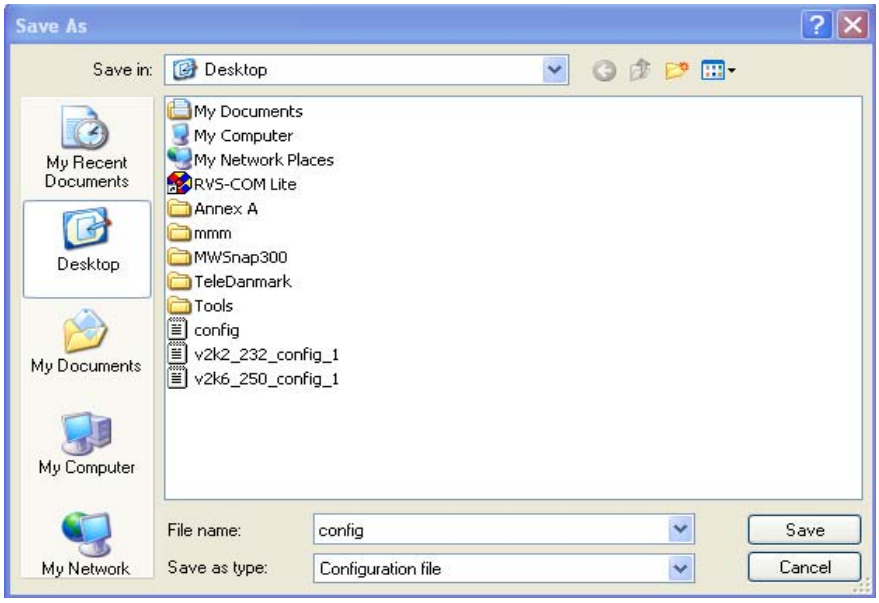
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.



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.



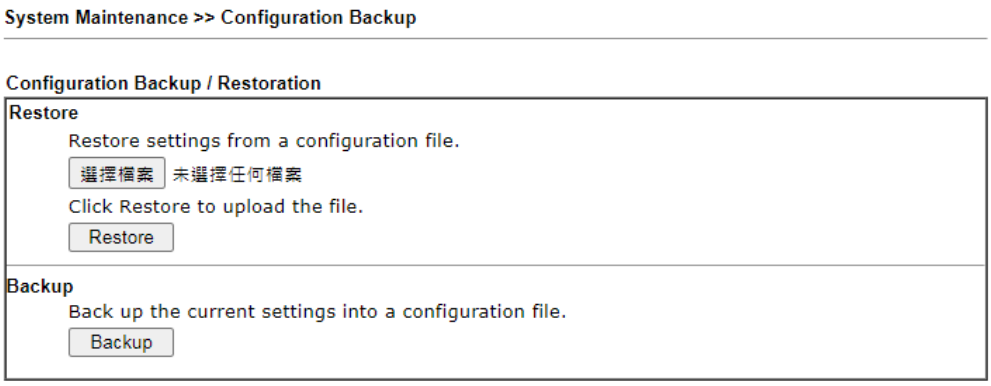
4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

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.

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

Restore Configuration

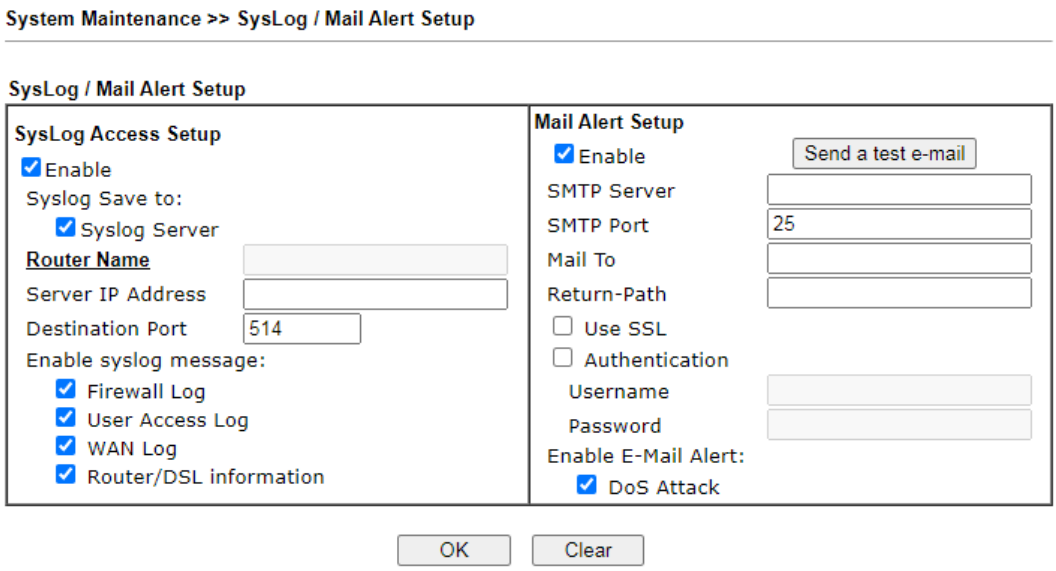
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.



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

3.8.5 Syslog/Mail Alert

SysLog function is provided for users to monitor modem. There is no bother to directly get into the Web User Interface of the modem or borrow debug equipments.



Available settings are explained as follows:

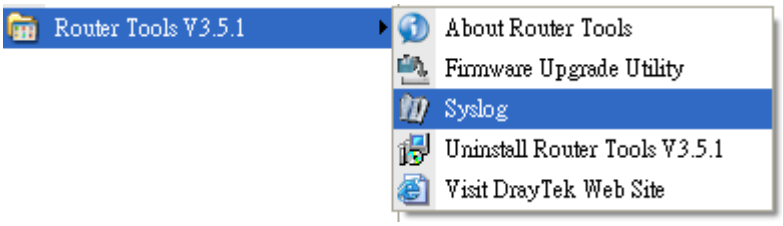
Item	Description
SysLog Access Setup	**Enable** - Check **Enable** to activate function of syslog. **Syslog Save to** – Check **Syslog Server** to save the log to Syslog server.
Router Name	Display the name for such modem configured in **System Maintenance>>Management.** If there is no name here, simply lick the link to access into **System Maintenance>>Management** to set the modem name. **Server IP Address** -The IP address of the Syslog server. **Destination Port** - Assign a port for the Syslog protocol. **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.
Mail Alert Setup	Check "**Enable**" to activate function of mail alert. **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. **SMTP Server** - The IP address of the SMTP server. **Mail To** - Assign a mail address for sending mails out. **Return-Path** - Assign a path for receiving the mail from outside.

	Use SSL - Check this box to use port 465 for SMTP server for some e-mail server uses https as the transmission method. **Authentication -** Check this box to activate this function while using e-mail application. **User Name -** Type the user name for authentication. **Password -** Type the password for authentication. **Enable E-mail Alert -** Check the box to send alert message to the e-mail box while the modem detects the item you specify here.

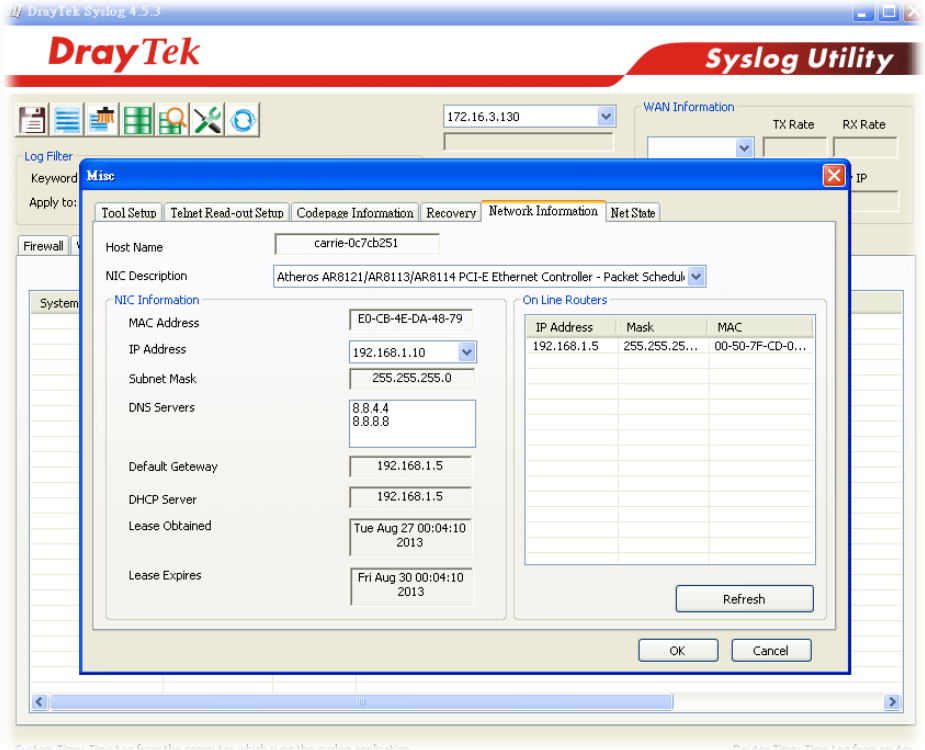
Click **OK** to save these settings.

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 Modem Tools in the **Utility** within provided CD. After installation, click on the **Modem Tools>>Syslog** from program menu.

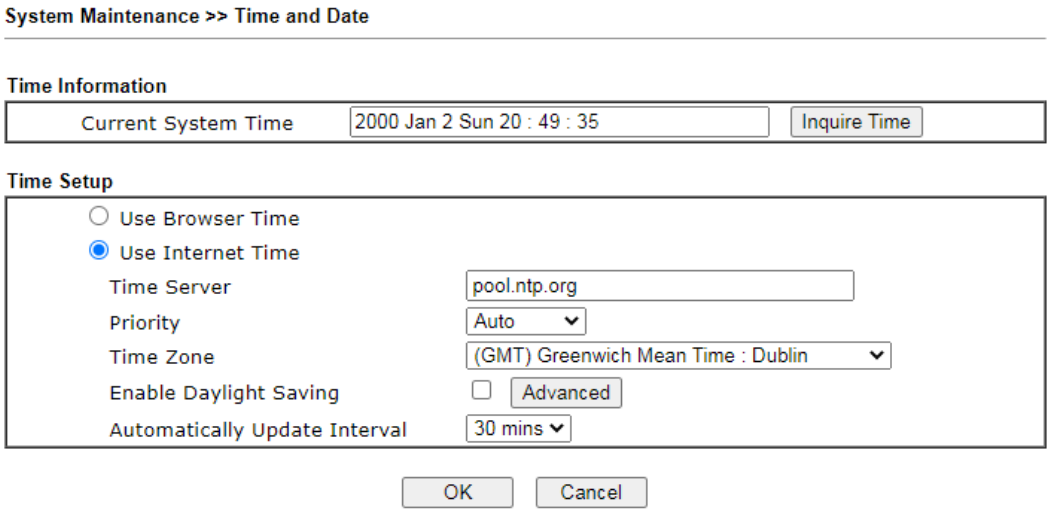


3. From the Syslog screen, select the modem you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the modem. Otherwise, you won't succeed in retrieving information from the modem.

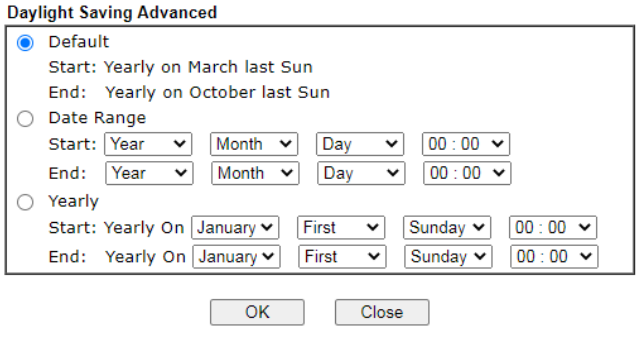


3.8.6 Time and Date

It allows you to specify where the time of the modem should be inquired from.



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 modem's system time.
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.
Time Protocol	Select a time protocol.
Server IP Address	Type the IP address of the time server.
Time Zone	Select the time zone where the modem 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.  Use the default time setting or set user defined time for your requirement.
Automatically Update Interval	Select a time interval for updating from the NTP server.

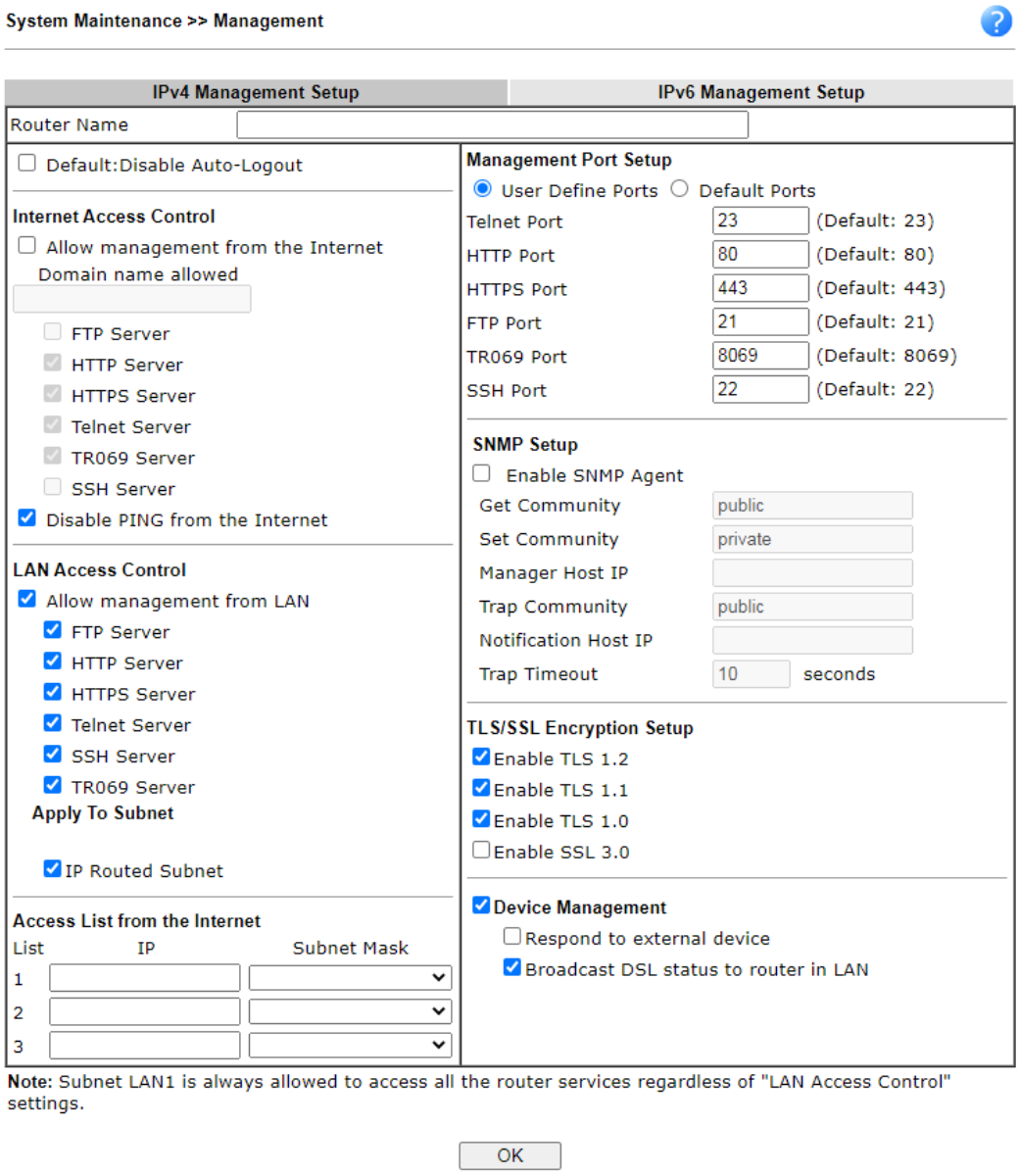
Click **OK** to save these settings.

3.8.7 Management

This page allows you to manage the settings for access control, access list, port setup, and SNMP setup.

The management pages for IPv4 and IPv6 protocols are different.

For IPv4



Available settings are explained as follows:

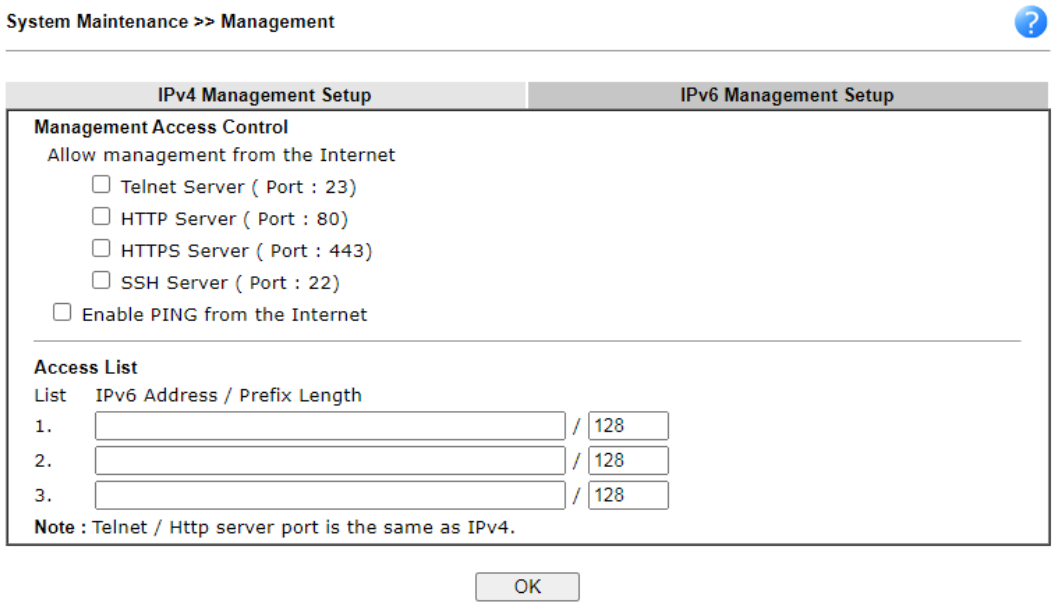
Item	Description
Router Name	Type in the modem name provided by ISP.
Default: Disable Auto-Logout	If it is enabled, the function of auto-logout for web user interface will be disabled.

	 The web user interface will be open until you click the Logout icon manually. 
Internet Access Control	**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 modem from Internet. Check the box(es) to specify. **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.
LAN Access Control	**Allow management from the LAN** - Enable the checkbox to allow system administrators to login from LAN interface. There are several servers provided by the system which allow you to manage the router from LAN interface. Check the box(es) to specify. **Apply To Subnet -** Check the LAN interface for the administrator to use for accessing into web user interface of Vigor router.
Access List from the Internet	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed. **List IP** - Indicate an IP address allowed to login to the modem. **Subnet Mask -** Represent a subnet mask allowed to login to the modem.
Management Port Setup	**User Define Ports -** Check to specify user-defined port numbers for the Telnet, HTTP, HTTPS, FTP, TR-069 and SSH servers. **Default Ports -** Check to use standard port numbers for the Telnet and HTTP servers.
SNMP Setup	**Enable SNMP Agent -** Check it to enable this function.. **Get Community -** Set the name for getting community by typing a proper character. The default setting is **public.** **Set Community -** Set community by typing a proper name. The default setting is **private.** **Manager Host IP -** Set one host as the manager to execute SNMP function. Please type in IPv4 address to specify certain host. **Trap Community -** Set trap community by typing a proper

	name. The default setting is **public.** **Notification Host IP -** Set the IPv4 address of the host that will receive the trap community. **Trap Timeout -** The default setting is 10 seconds.
TLS/SSL Encryption Setup	**Enable SSL 3.0/1.0/1.1/1.2 –** Check the box to enable SSL 3.0/1.0/1.1/1.2 encryption protocols. For improved security, the HTTPS and SSL VPN servers that are built into the router have been upgraded to TLS 1.x protocol. If you are using an old web browser (eg. IE 6.0) or an old version of the SmartVPN Client, you may need to enable SSL 3.0 to connect to the router. However, it is recommended that you instead upgrade your web browser or SmartVPN client to a version that supports TLS protocols that are far more secure than SSL.
Device Management	Check the box to enable the device management function for Vigor130. **Respond to external device –** If it is enabled, Vigor130 will be regarded as slave device. When the external device (master device) sends request packet to Vigor130**,** Vigor130 would send back information to respond the request coming from the external device which is able to manage Vigor130. **Broadcast DSL status to router in LAN** – Clients in LAN can get current DSL connection status if such function is enabled.

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

For IPv6



Available settings are explained as follows:

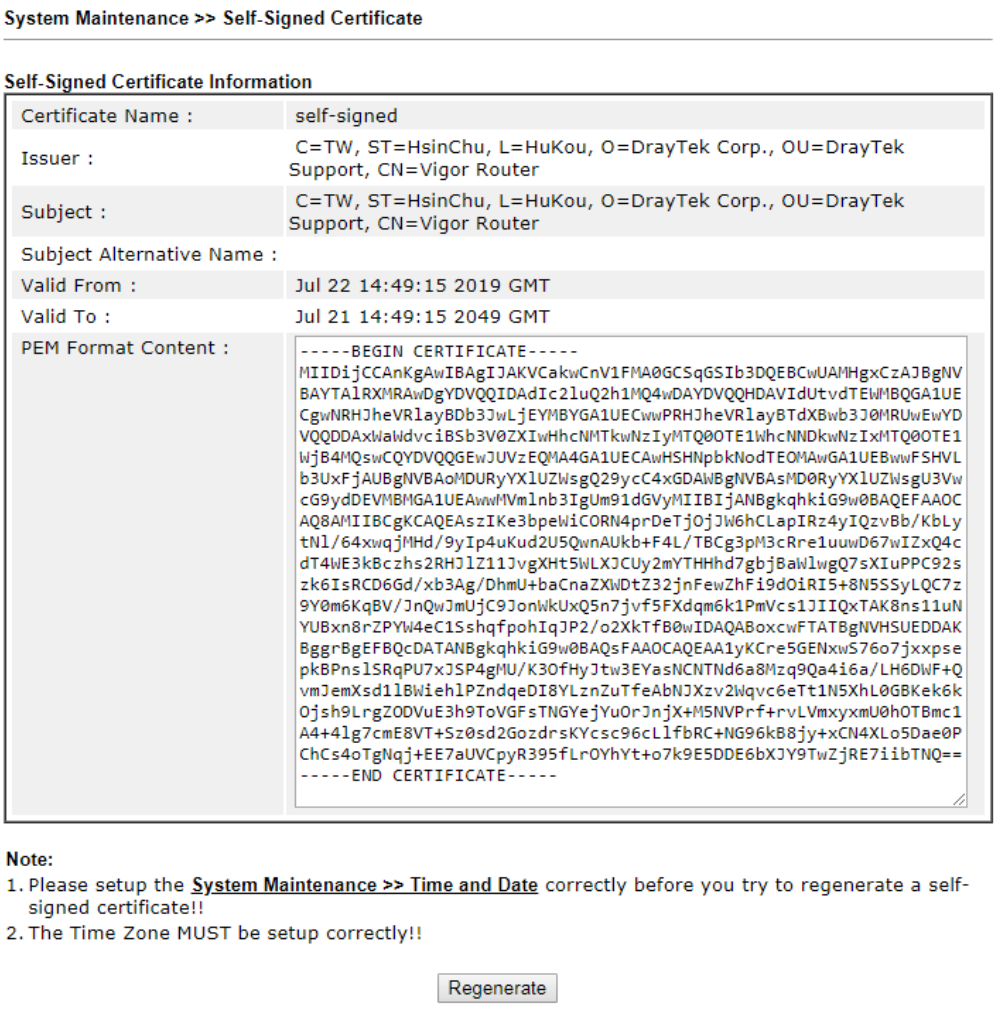
Item	Description
Management Access	**Allow management from the Internet** -Enable the

Control	checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the modem from Internet. Check the box(es) to specify. **Enable PING from the Internet** - Check the checkbox to enable all PING packets from the Internet. For security issue, this function is disabled by default.
Access List	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. **IPv6 Address /Prefix Length**- Indicate the IP address(es) allowed to login to the modem.

3.8.8 Self-Signed Certificate

A self-signed certificate is a *unique* identification for the device (e.g., Vigor router) which generates the certificate by itself to ensure the router security. Such self-signed certificate is signed with its own private key.

The self-signed certificate can be used for services such as SSL VPN and HTTPS. In addition, it can be created for free by using a wide variety of tools.



System Maintenance >> Self-Signed Certificate

Self-Signed Certificate Information

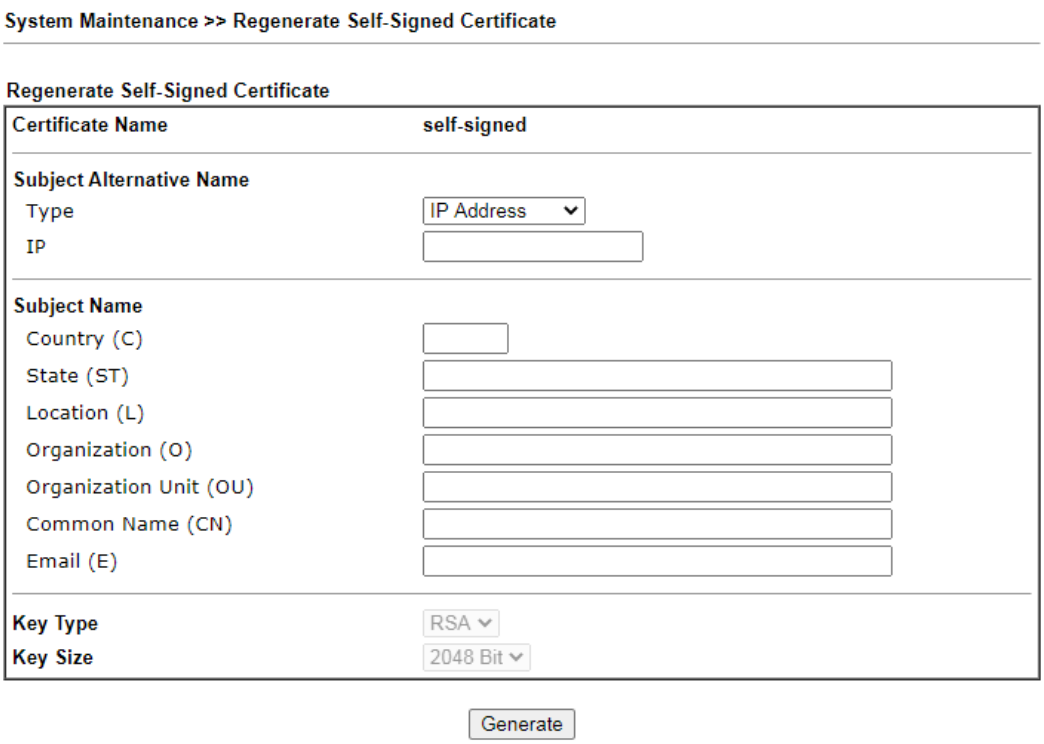
Certificate Name :	self-signed
Issuer :	C=TW, ST=HsinChu, L=HuKou, O=DrayTek Corp., OU=DrayTek Support, CN=Vigor Router
Subject :	C=TW, ST=HsinChu, L=HuKou, O=DrayTek Corp., OU=DrayTek Support, CN=Vigor Router
Subject Alternative Name :	
Valid From :	Jul 22 14:49:15 2019 GMT
Valid To :	Jul 21 14:49:15 2049 GMT
PEM Format Content :	-----BEGIN CERTIFICATE----- MIIDijCCAnKgAwIBAgIJAKVCakwCnV1FMA0GCSqGSIb3DQEBCwUAMHgxCzAJBgNV BAYTAlRXMRAwDgYDVQQIDAdIc2luQ2h1MQ4wDAYDVQQHDAVIdUtvdTEWMBQGA1UE CgwNRHJheVRlayBDb3JwLjEYMBYGA1UECwwPRHJheVRlayBTdXBwb3J0MRUwEwYD VQQDDAxWaWdvciBSb3V0ZXIwHhcNMTkwNzIyMTQ0OTE1WhcNNDkwNzIxMTQ0OTE1 WjB4MQswCQYDVQQGEwJUVzEQMA4GA1UECAwHSHNpbkNodTEOMAwGA1UEBwwFSHVL b3UxFjAUBgNVBAoMDURyYXlUZWsgQ29ycC4xGDAWBgNVBAsMD0RyYXlUZWsgU3Vw cG9ydDEVMBMGA1UEAwwMVmlnb3IgUm91dGVyMIIBIjANBgkqhkiG9w0BAQEFAAOC AQ8AMIIBCgKCAQEAszIKe3bpeWiCORN4prDeTjOjJW6hCLapIRz4yIQzvBb/KbLy tNl/64xwqjMHd/9yIp4uKud2U5QwnAUkb+F4L/TBCg3pM3cRre1uuwD67wIZxQ4c dT4WE3kBczhs2RHJlZ11JvgXHt5WLXJCUy2mYTHHhd7gbjBaWlwgQ7sXIuPPC92s zk6IsRCD6Gd/xb3Ag/DhmU+baCnaZXWDtZ32jnFewZhFi9dOiRI5+8N5SSyLQC7z 9Y0m6KqBV/JnQwJmUjC9JonWkUxQ5n7jvf5FXdqm6k1PmVcs1JIIQxTAK8ns11uN YUBxn8rZPYW4eC1SshqfpohIqJP2/o2XkTfB0wIDAQABoxcwFTATBgNVHSUEDDAK BggrBgEFBQcDATANBgkqhkiG9w0BAQsFAAOCAQEAA1yKCre5GENxwS76o7jxxpse pkBPnslSRqPU7xJSP4gMU/K3OfHyJtw3EYasNCNTNd6a8Mzq9Qa4i6a/LH6DWF+Q vmJemXsd1lBWiehlPZndqeDI8YLznZuTfeAbNJXzv2Wqvc6eTt1N5XhL0GBKek6k Ojsh9LrgZODVuE3h9ToVGFsTNGYejYuOrJnjX+M5NVPrf+rvLVmxyxmU0hOTBmc1 A4+4lg7cmE8VT+Sz0sd2GozdrsKYcsc96cLlfbRC+NG96kB8jy+xCN4XLo5Dae0P ChCs4oTgNqj+EE7aUVCpyR395fLrOYhYt+o7k9E5DDE6bXJY9TwZjRE7iibTNQ== -----END CERTIFICATE-----

Note:

1. Please setup the **System Maintenance >> Time and Date** correctly before you try to regenerate a self-signed certificate!!
2. The Time Zone MUST be setup correctly!!

Regenerate

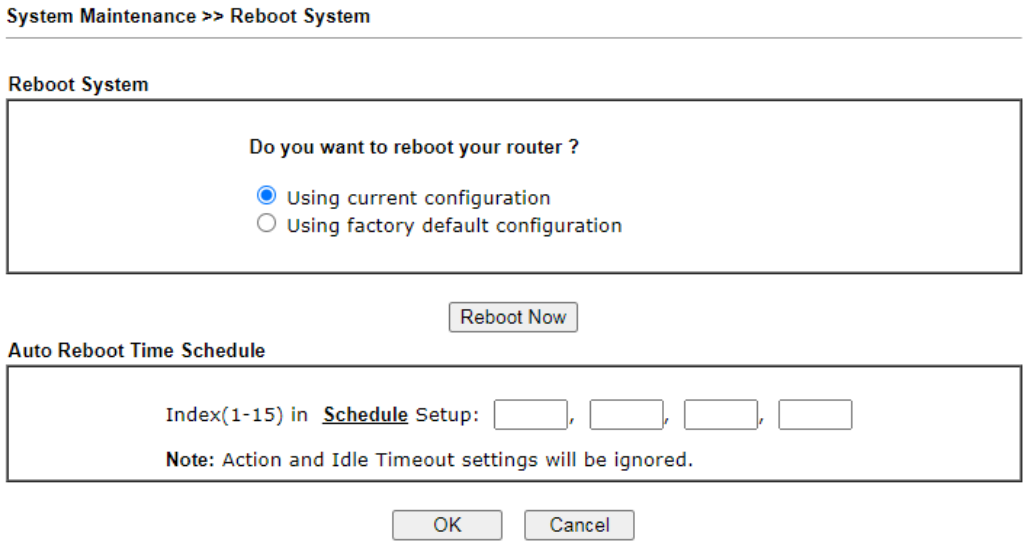
Click **Regeneration** to open **Regenerate Self-Signed Certificate** window.



Enter all requested information including certificate name (used to differentiate different certificates), subject alternative name type and relational settings for subject name. Then click **GENERATE**.

3.8.9 Reboot System

The Web User Interface may be used to restart your modem. Click **Reboot System** from **System Maintenance** to open the following page.



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

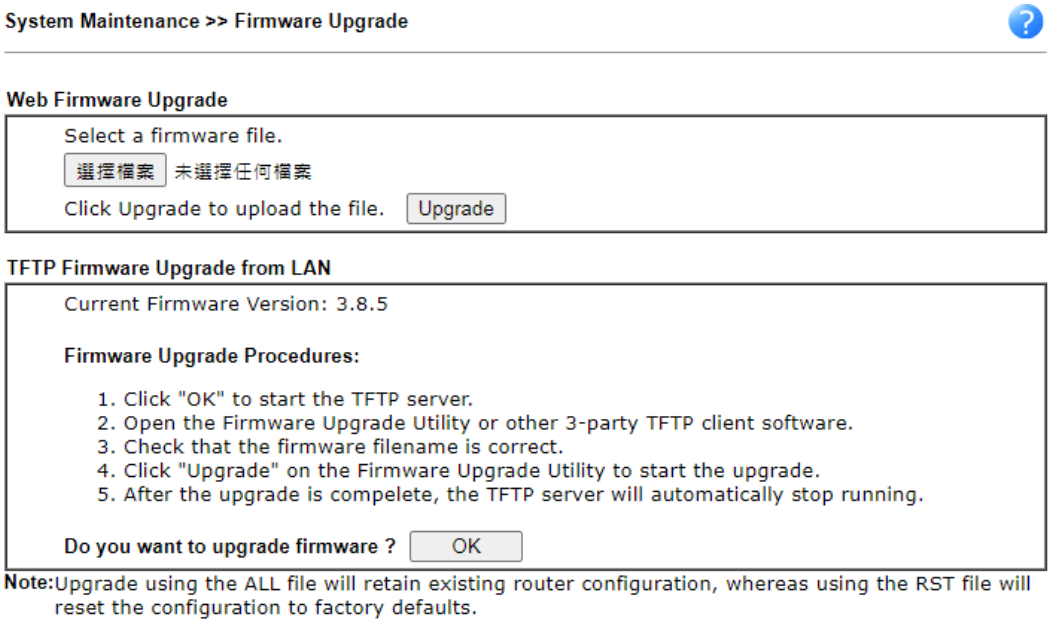
Note: When the system pops up Reboot System web page after you configure web settings, please click **OK** to reboot your modem for ensuring normal operation and preventing unexpected errors of the modem in the future.

3.8.10 Firmware Upgrade

Before upgrading your modem firmware, you need to install the Modem Tools. The **Firmware Upgrade Utility** is included in the tools. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).

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.

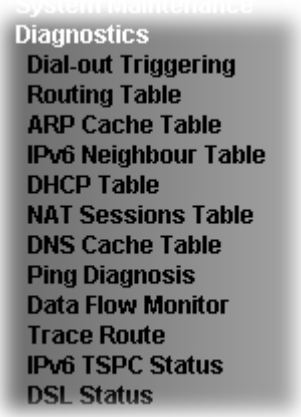


Click **OK**. The following screen will appear. Please execute the firmware upgrade utility first.

3.9 Diagnostics

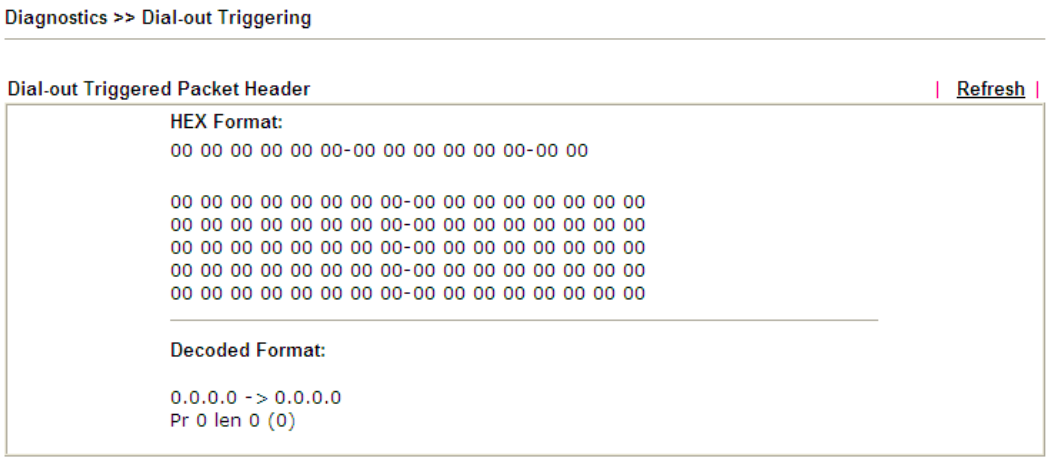
Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor modem.

Below shows the menu items for Diagnostics.



3.9.1 Dial-out Triggering

Click **Diagnostics** and click **Dial-out Trigger** to open the web page. The internet connection (e.g., PPPoE, PPPoA, etc) is triggered by a package sending from the source IP address.

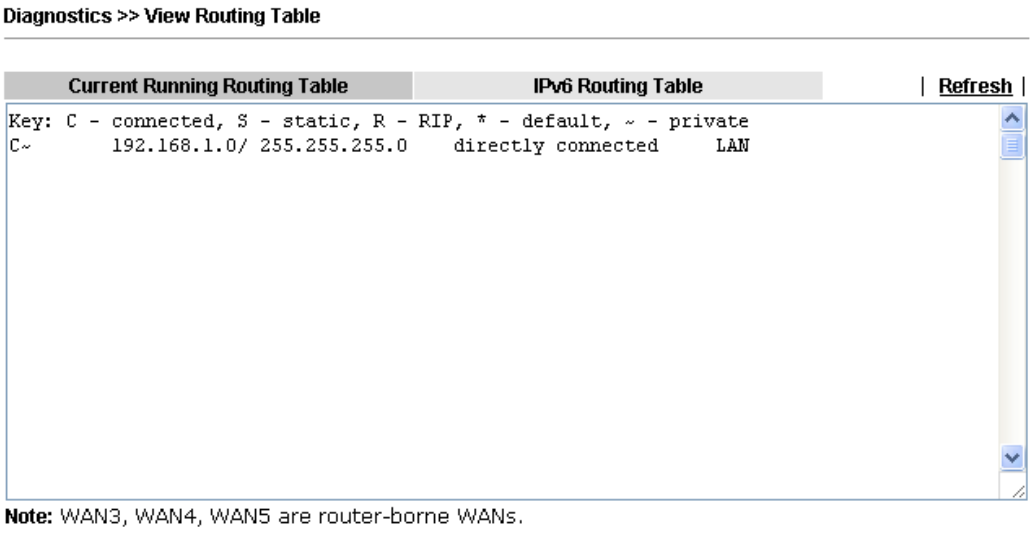


Available settings are explained as follows:

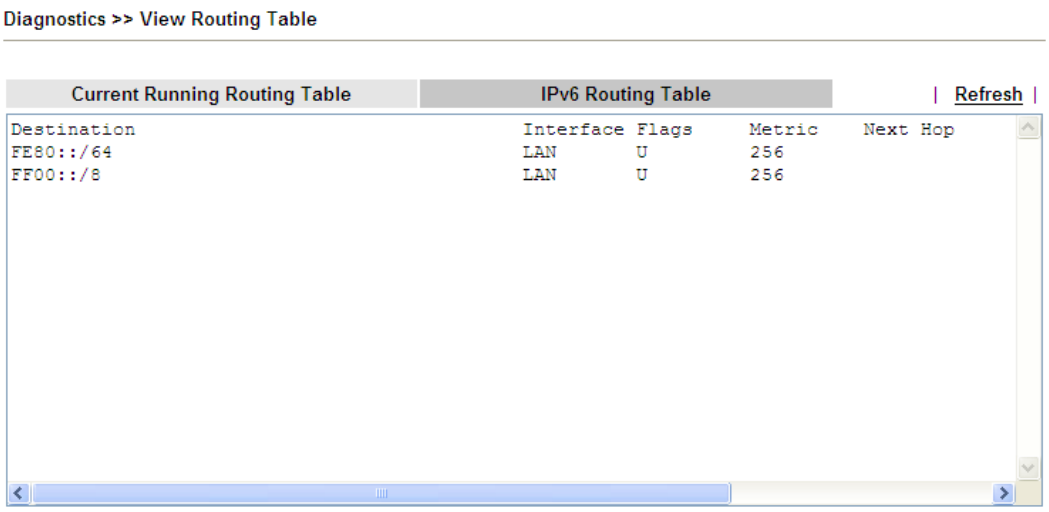
Item	Description
Decoded Format	It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.
Refresh	Click it to reload the page.

3.9.2 Routing Table

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



And,

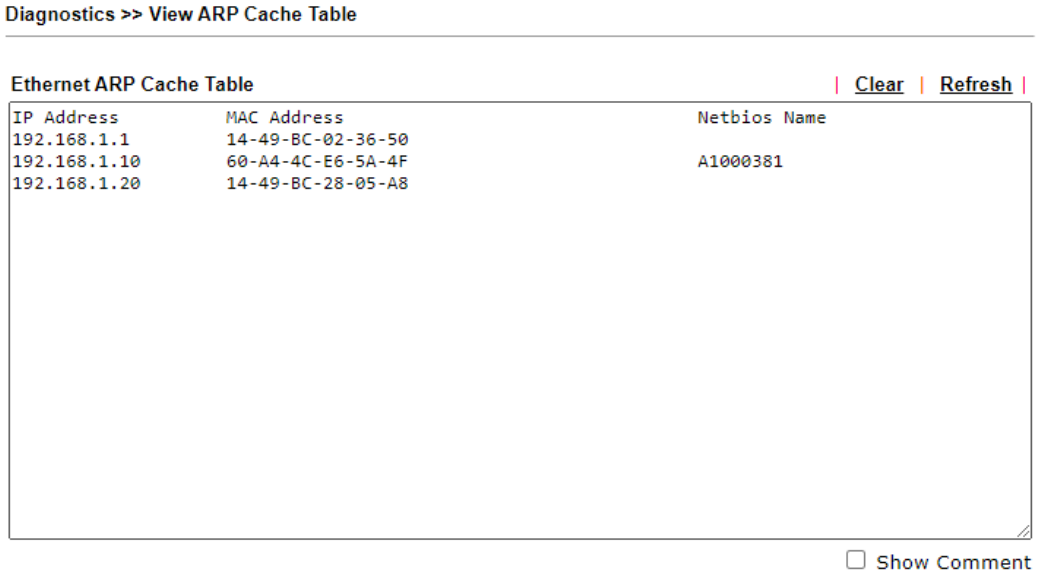


Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

3.9.3 ARP Cache Table

Click **Diagnostics** and click **ARP Cache Table** to view the content of the ARP (Address Resolution Protocol) cache held in the modem. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.



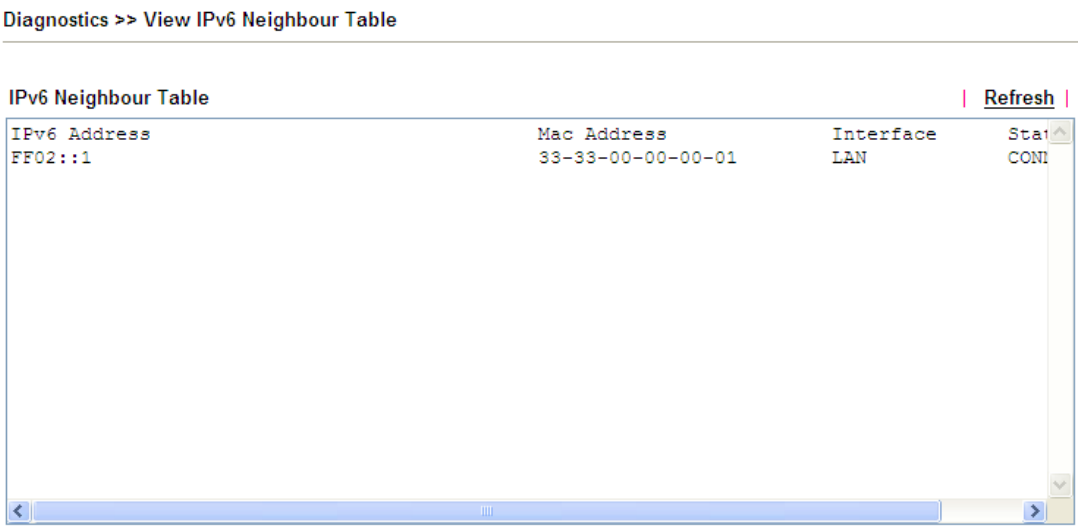
Available settings are explained as follows:

Item	Description
Clear	Click it to clear the whole table.
Refresh	Click it to reload the page.

3.9.4 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.



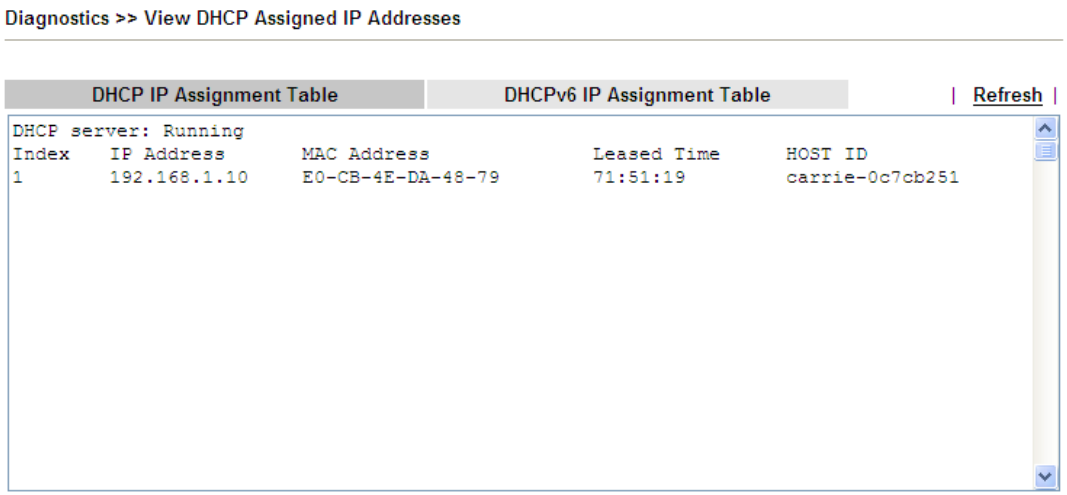
Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

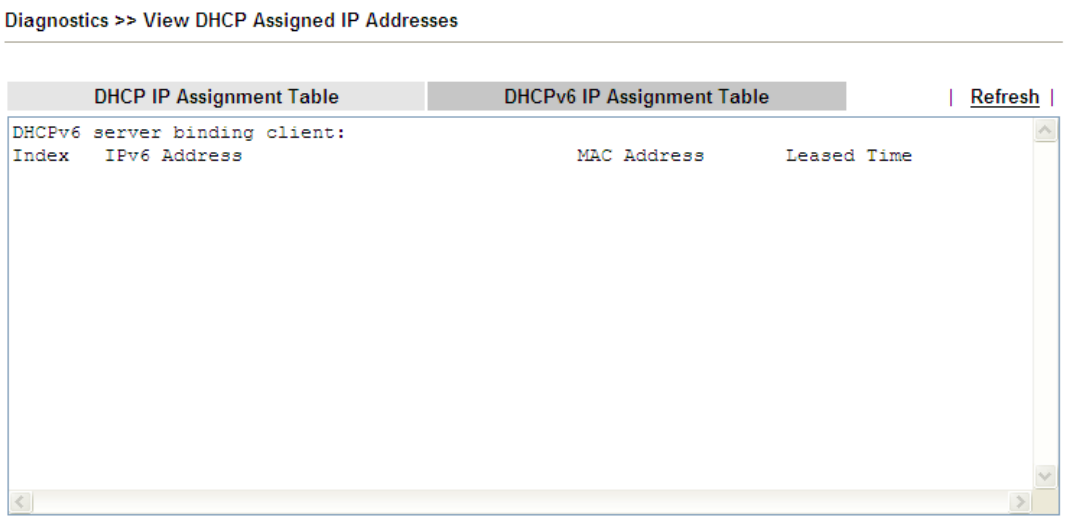
3.9.5 DHCP Table

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.



And,



Each item is explained as follows:

Item	Description
Index	It displays the connection item number.
IP Address	It displays the IP address assigned by this modem 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.

3.9.6 NAT Sessions Table

Click **Diagnostics** and click **NAT Sessions Table** to open the list page.

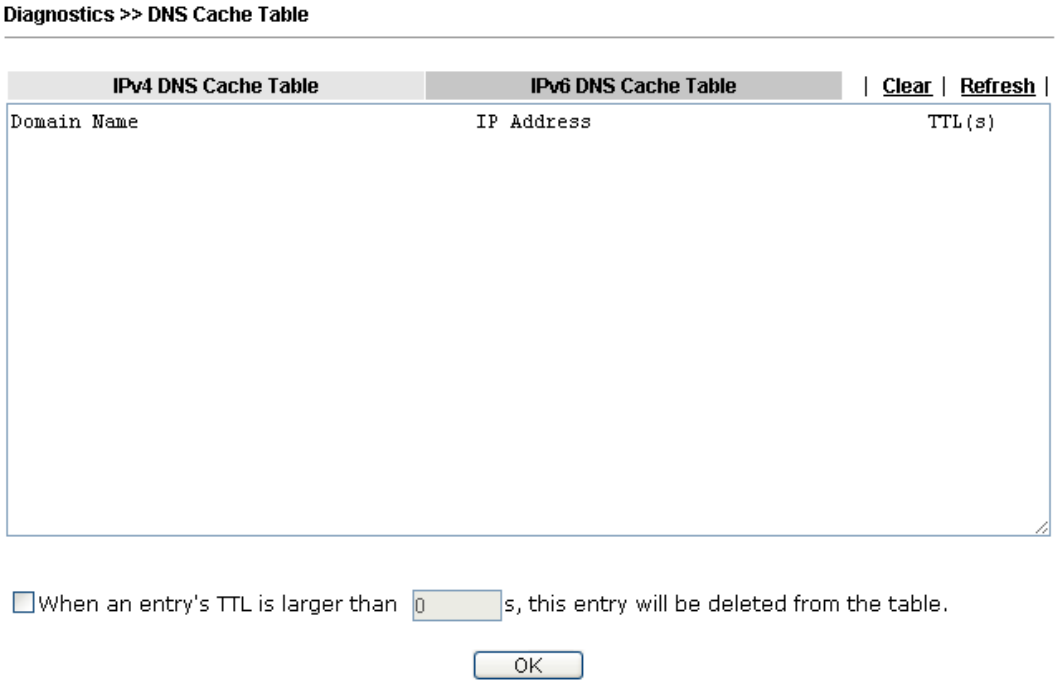
Available settings are explained as follows:

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 modem 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.

3.9.7 DNS Cache Table

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

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

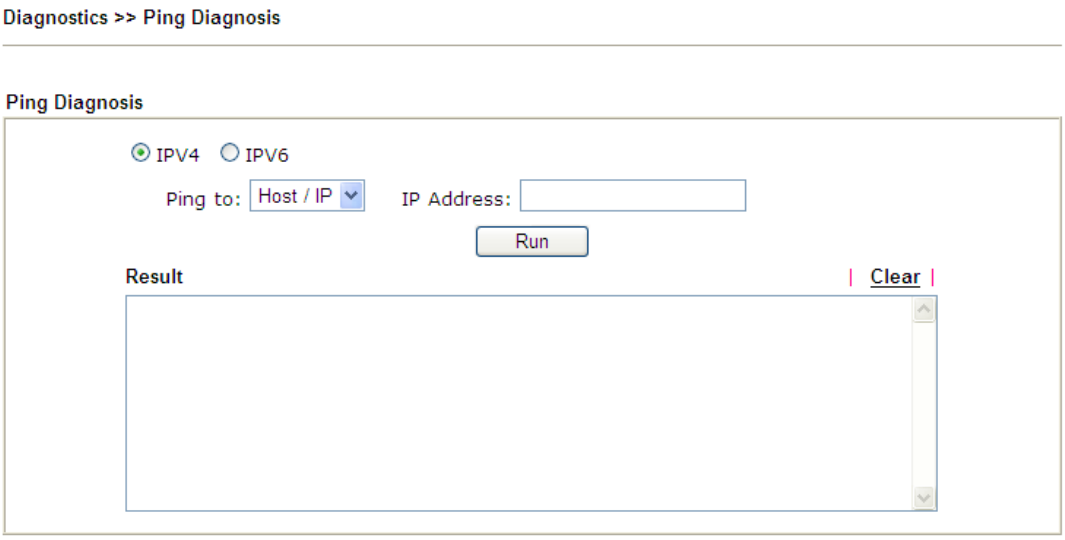


Available settings are explained as follows:

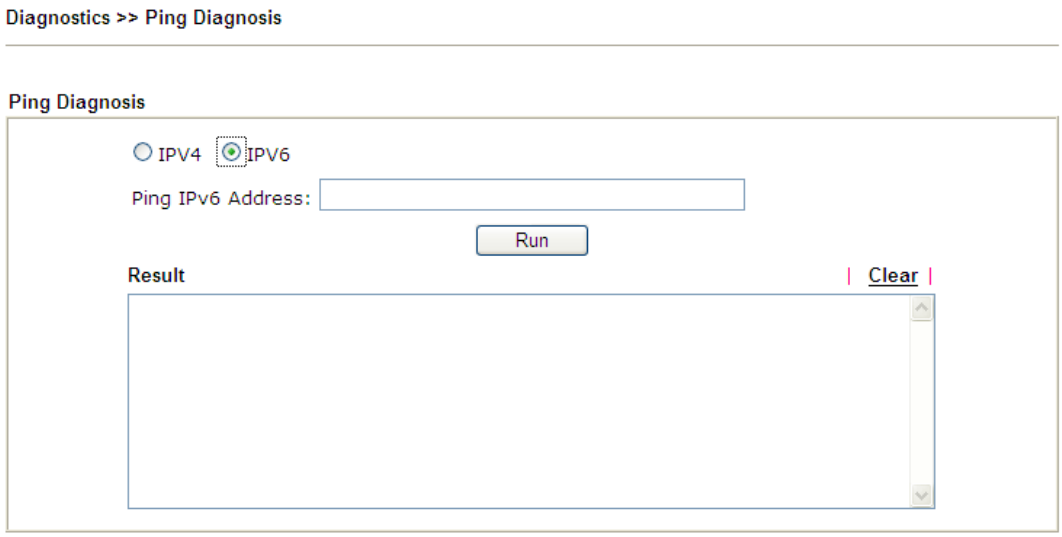
Item	Description
Clear	Click this link to remove the result on the window.
Refresh	Click it to reload the page.
When an entry's TTL is larger than….	Check the box the type the value of TTL (time to live) for each entry. Click **OK** to enable such function. It means when the TTL value of each DNS query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

3.9.8 Ping Diagnosis

Click **Diagnostics** and click **Ping Diagnosis** to pen the web page.



And,



Available settings are explained as follows:

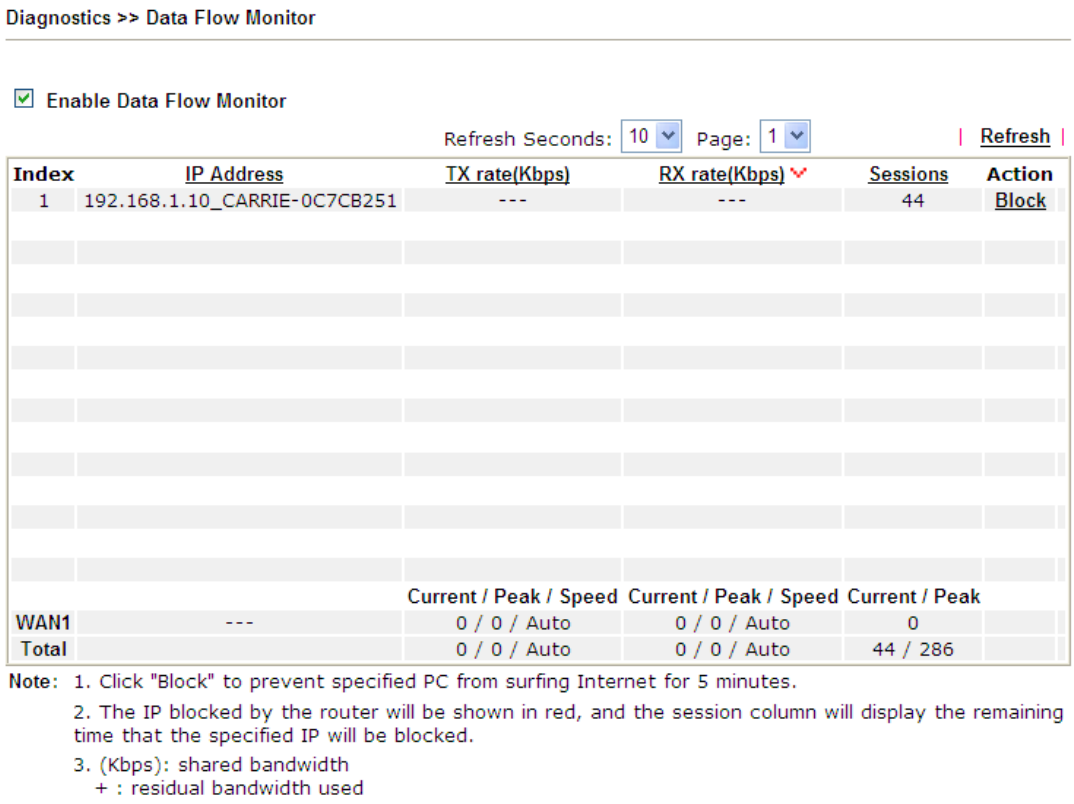
Item	Description
IPV4 /IPV6	Choose the interface for such function.
Ping through	Use the drop down list to choose the WAN interface that you want to ping through or choose **Unspecified** to be determined by the modem automatically.
Ping to	Use the drop down list to choose the destination that you want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

	displayed on the screen.
Clear	Click this link to remove the result on the window.

3.9.9 Data Flow Monitor

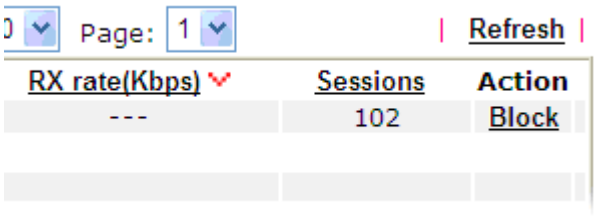
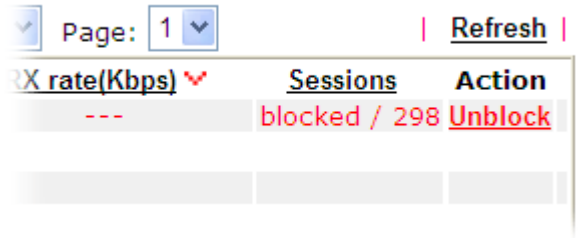
This page displays the running procedure for the IP address monitored and refreshes the data in an interval of several seconds.

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



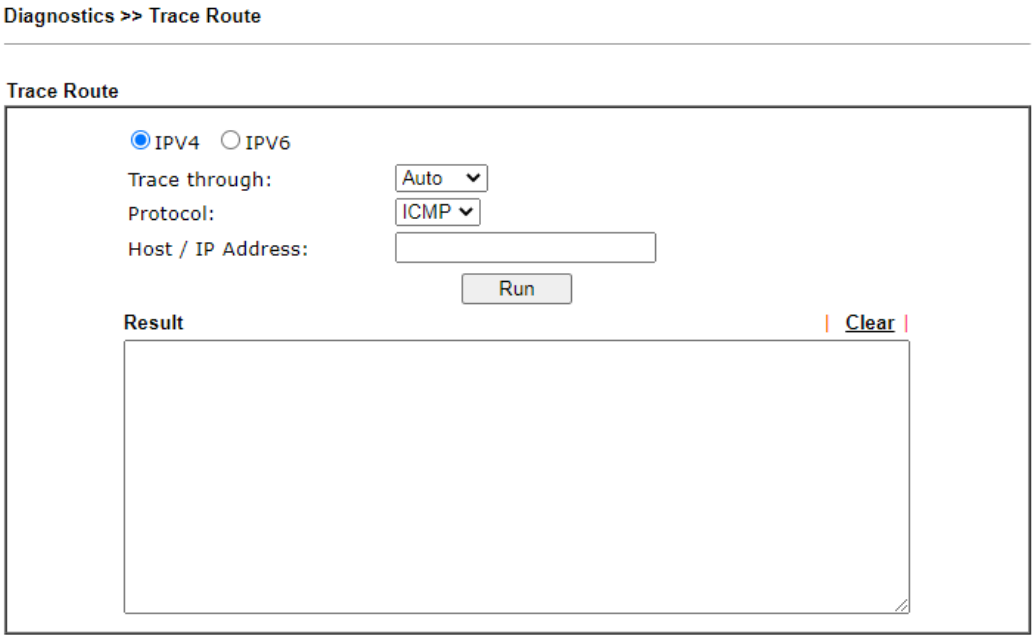
Available settings are explained as follows:

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

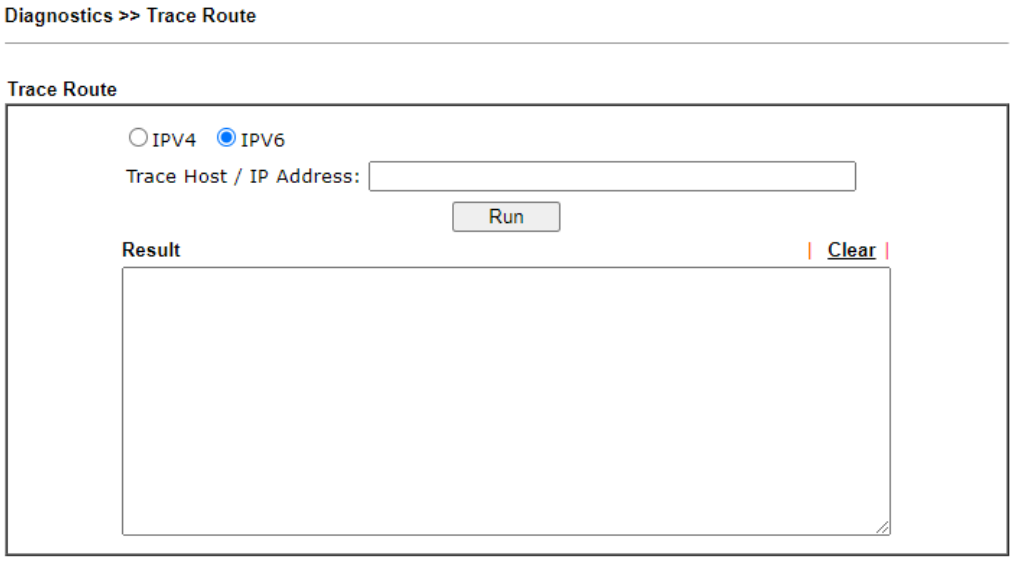
Action	**Block** - can prevent specified PC accessing into Internet within 5 minutes.  **Unblock** – the device with the IP address will be blocked in five minutes. The remaining time will be shown on the session column. 
Current /Peak/Speed	**Current** means current transmission rate and receiving rate for WAN interface. **Peak** means the highest peak value detected by the modem in data transmission. **Speed** means line speed specified in **WAN>>General Setup**. If you do not specify any rate at that page, here will display **Auto** for instead.

3.9.10 Trace Route

Click **Diagnostics** and click **Trace Route** to open the web page. This page allows you to trace the routes from modem 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.



or



Available settings are explained as follows:

Item	Description
IPv4 / IPv6	Click one of them to display corresponding information for it.
Protocol	Use the drop down list to choose the protocol that you want to ping through.
Host/IP Address	It indicates the IP address of the host.

Trace Host/IP Address	It indicates the IPv6 address of the host.
Run	Click this button to start route tracing work.
Clear	Click this link to remove the result on the window.

3.9.11 IPv6 TSPC Status

IPv6 TSPC status web page could help you to diagnose the connection status of TSPC.

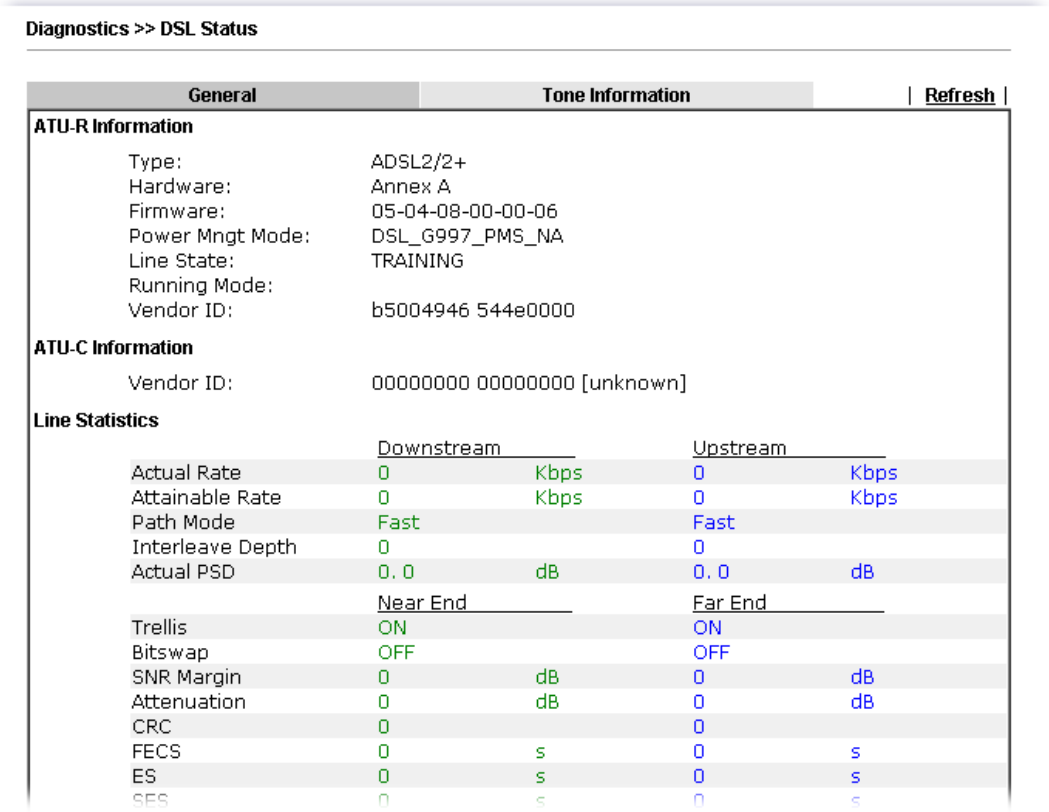
If TSPC has configured properly, the modem will display the following page when the user connects to tunnel broker successfully.

Available settings are explained as follows:

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

3.9.12 DSL Status

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



Diagnostics >> DSL Status

General | Tone Information | Refresh |

ATU-R Information

Type:	ADSL2/2+
Hardware:	Annex A
Firmware:	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

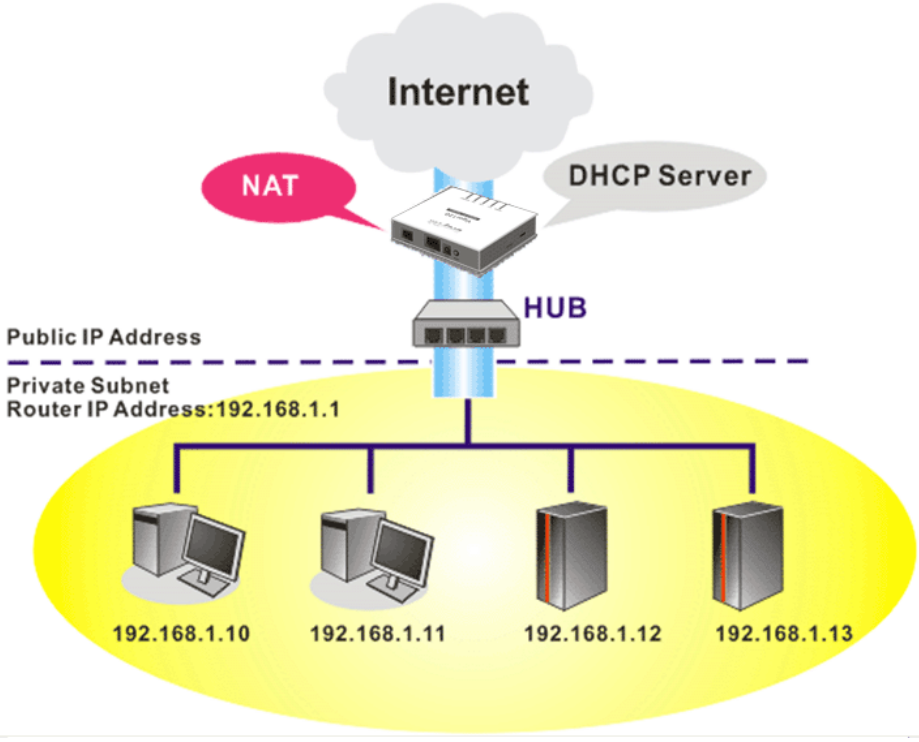
	Downstream		Upstream	
Actual Rate	0	Kbps	0	Kbps
Attainable Rate	0	Kbps	0	Kbps
Path Mode	Fast		Fast	
Interleave Depth	0		0	
Actual PSD	0.0	dB	0.0	dB
	Near End		Far End	
Trellis	ON		ON	
Bitswap	OFF		OFF	
SNR Margin	0	dB	0	dB
Attenuation	0	dB	0	dB
CRC	0		0	
FECS	0	s	0	s
ES	0	s	0	s
SES	0	s	0	s

This page is left blank.

4 Application and Examples

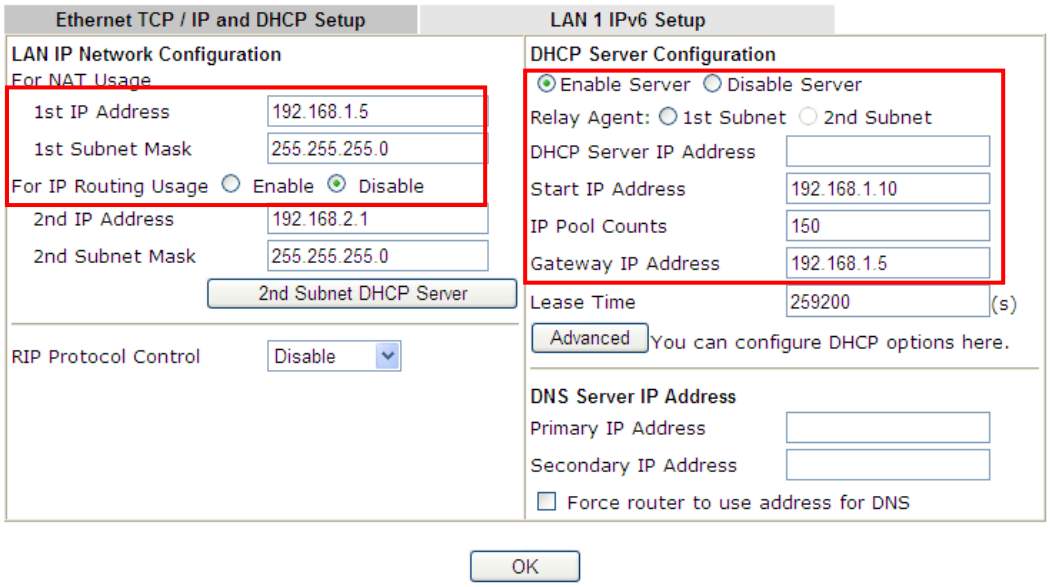
4.1 LAN – Created by Using NAT

An example of default setting and the corresponding deployment are shown below. The default Vigor modem private IP address/Subnet Mask is 192.168.1.1/255.255.255.0. The built-in DHCP server is enabled so it assigns every local NATed host an IP address of 192.168.1.x starting from 192.168.1.10.

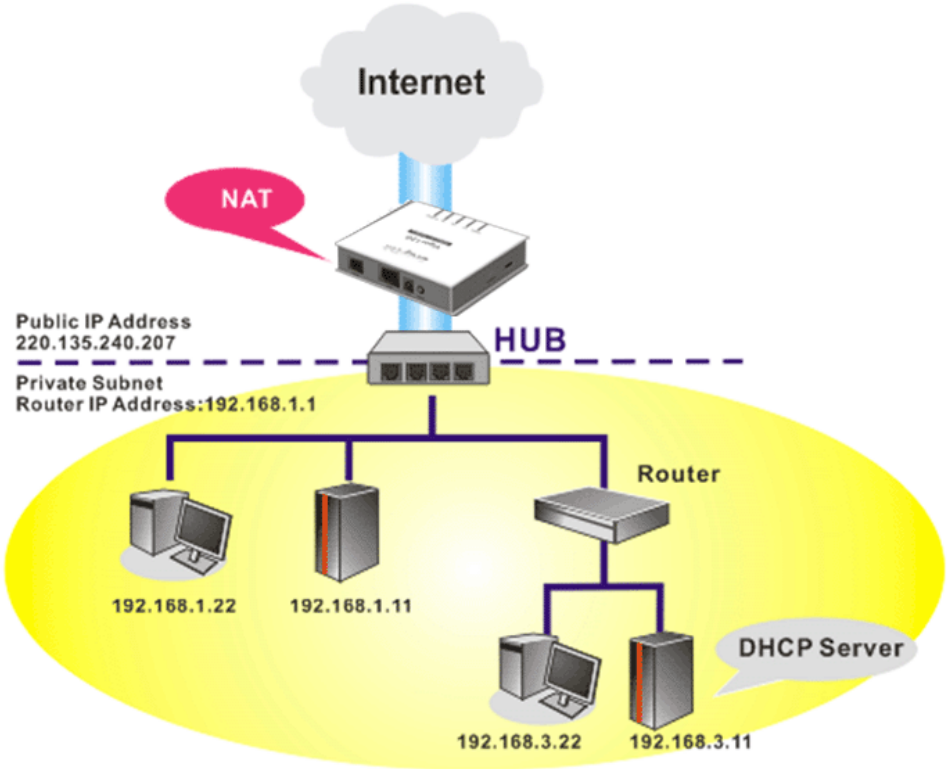


You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.

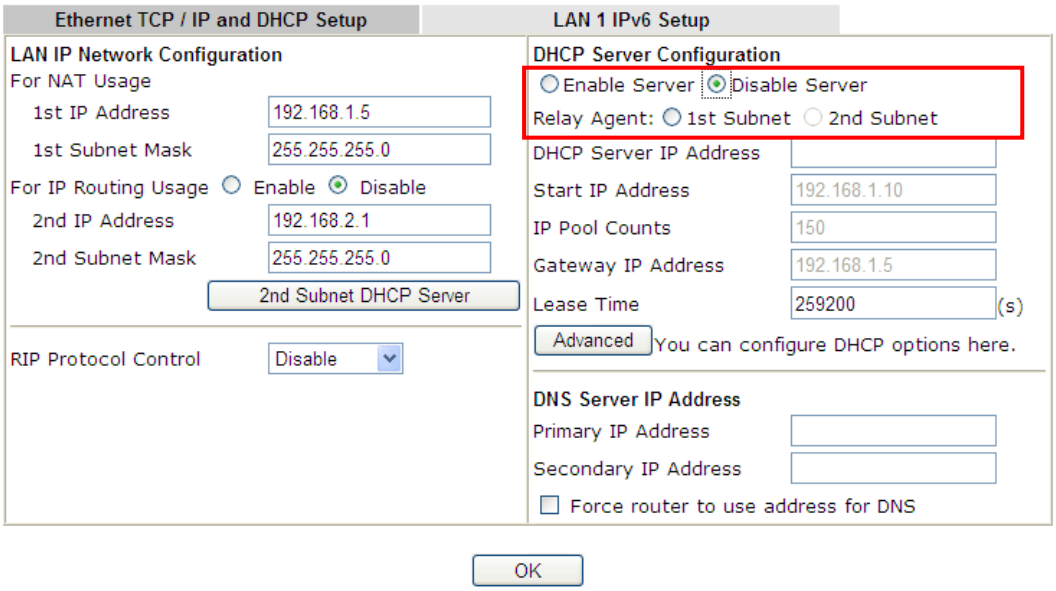
LAN >> General Setup



To use another DHCP server in the network rather than the built-in one of Vigor Modem, you have to change the settings as show below.



LAN >> General Setup



This page is left blank.

5 Trouble Shooting

This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the modem 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 modem 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 modem still cannot run normally, it is the time for you to contact your dealer for advanced help.

5.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

1. Check the power line and DSL/LAN cable connections.
   Refer to "**1.3 Hardware Installation"** for details.
2. Power on the modem. Make sure the **ACT** LED and **LAN** LED are bright.
3. If not, it means that there is something wrong with the hardware status. Simply back to **"1.3 Hardware Installation"** to execute the hardware installation again. And then, try again.

5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not

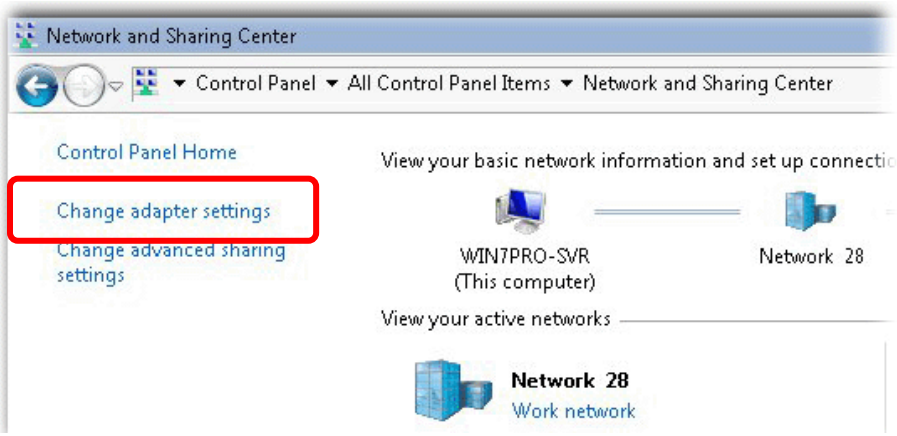
Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows

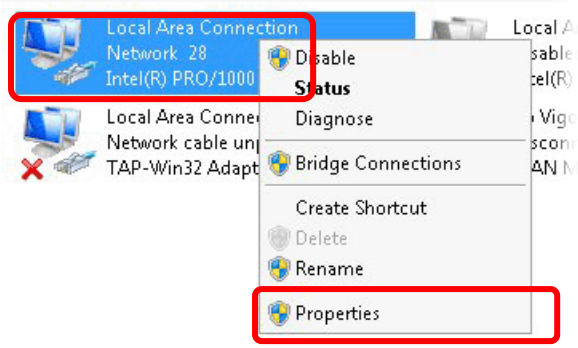
> The example is based on Windows 7. As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.DrayTek.com**.

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

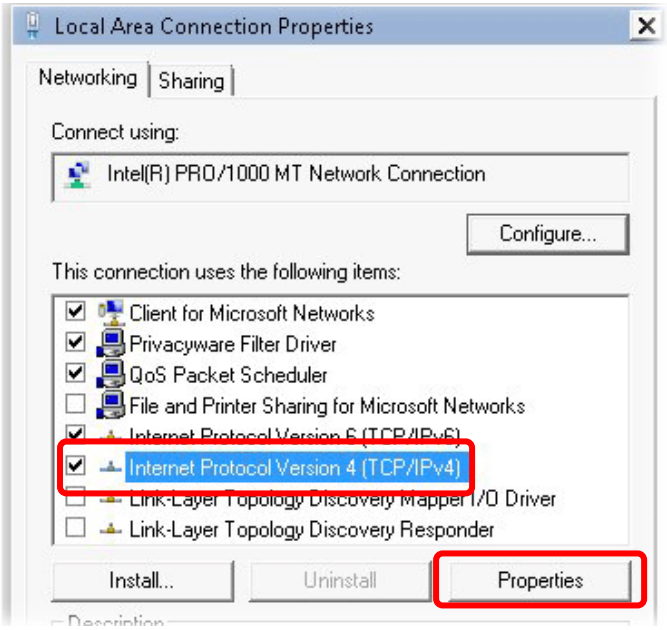
2. In the following window, click **Change adapter settings**.



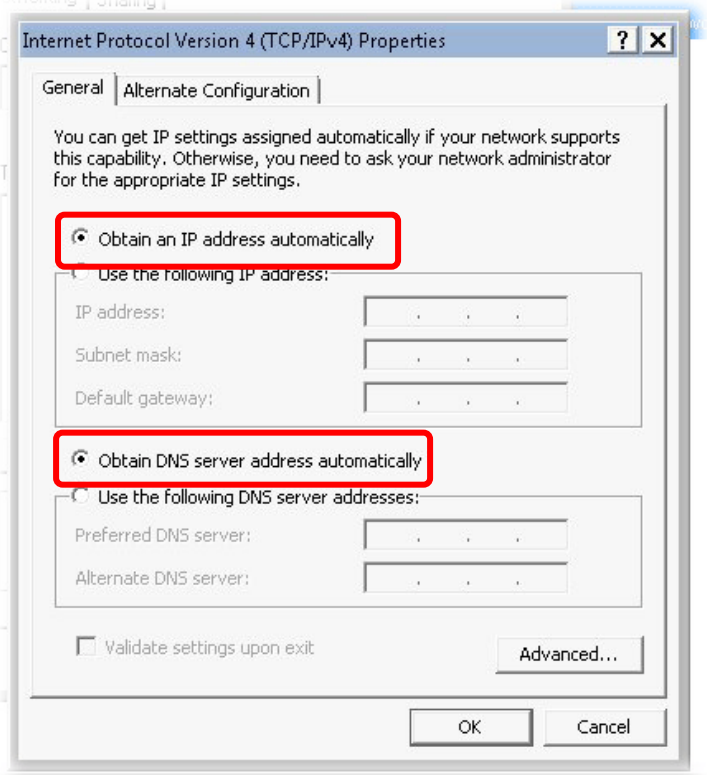
3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



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

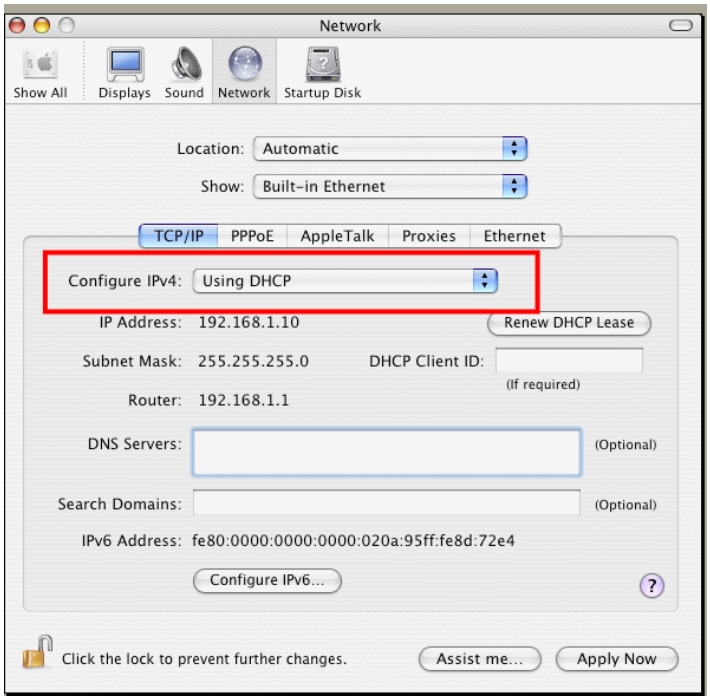


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



For MacOs

1. Double click on the current used MacOs 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.



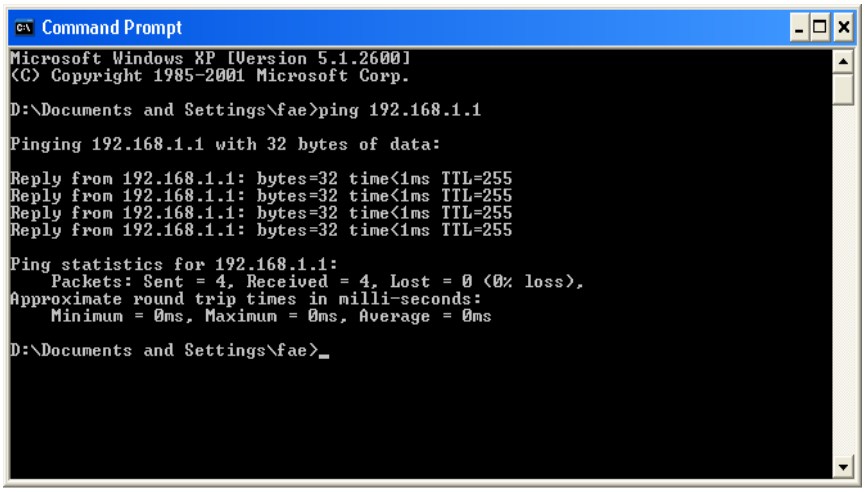
5.3 Pinging the Modem from Your Computer

The default gateway IP address of the modem is 192.168.1.1. For some reason, you might need to use "ping" command to check the link status of the modem. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section 5.2)

Please follow the steps below to ping the modem correctly.

For Windows

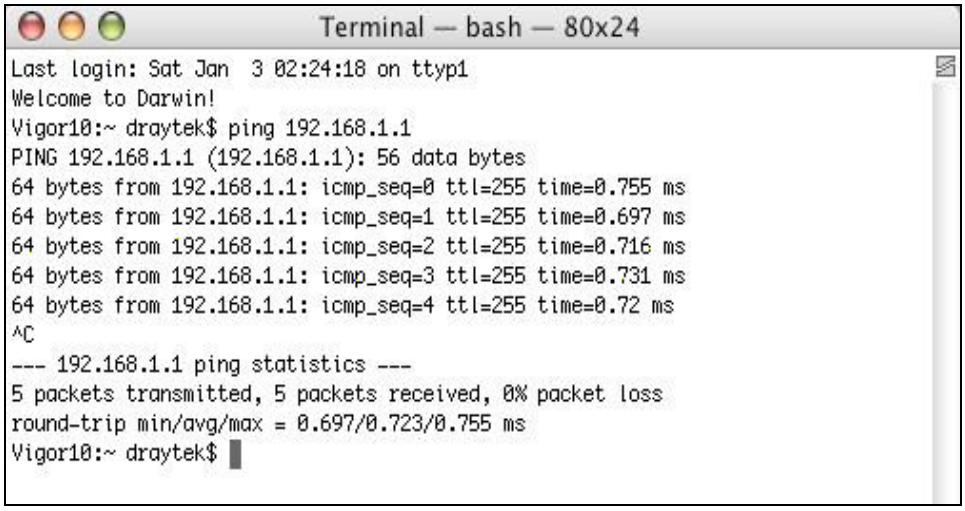
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista). The DOS command dialog will appear.



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.

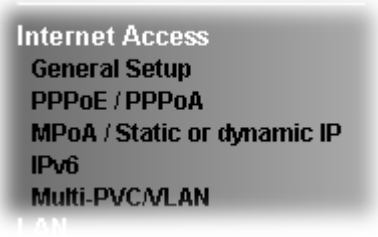
For MacOs (Terminal)

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.



5.4 Checking If the ISP Settings are OK or Not

Click **Internet Access** group and then check whether the ISP settings are set correctly.



5.5 Backing to Factory Default Setting If Necessary

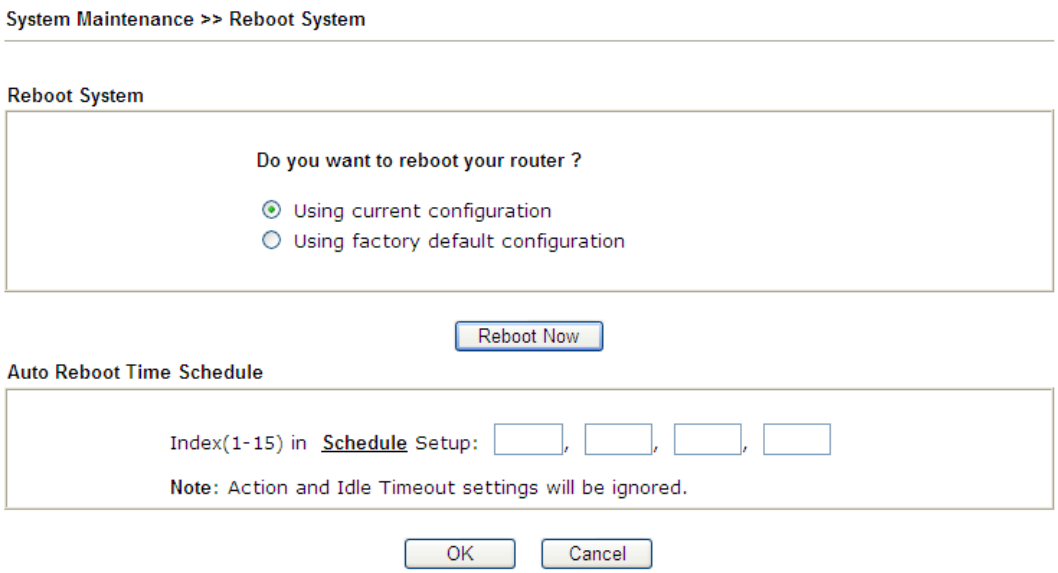
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the modem by software or hardware.

Warning: After pressing **factory default setting**, you will loose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null.

Software Reset

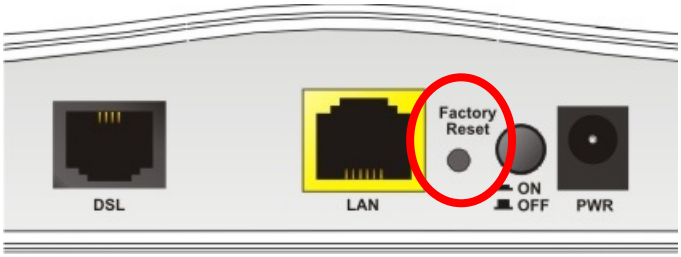
You can reset the modem to factory default via Web page.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **OK**. After few seconds, the modem will return all the settings to the factory settings.



Hardware Reset

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



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

5.6 Contacting DrayTek

If the modem still cannot work correctly after trying many efforts, please feel free to send e-mail to support@draytek.com.

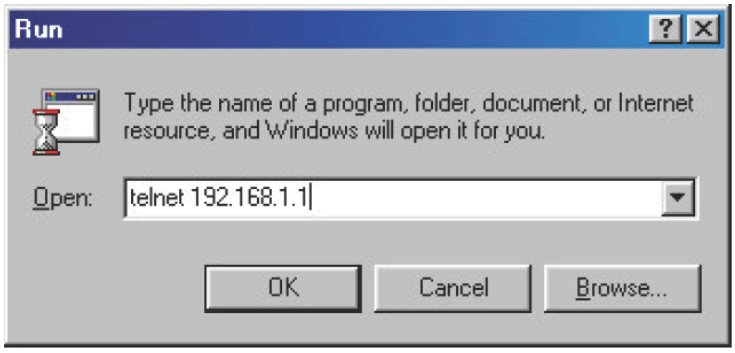
This page is left blank.

Telnet Command Reference

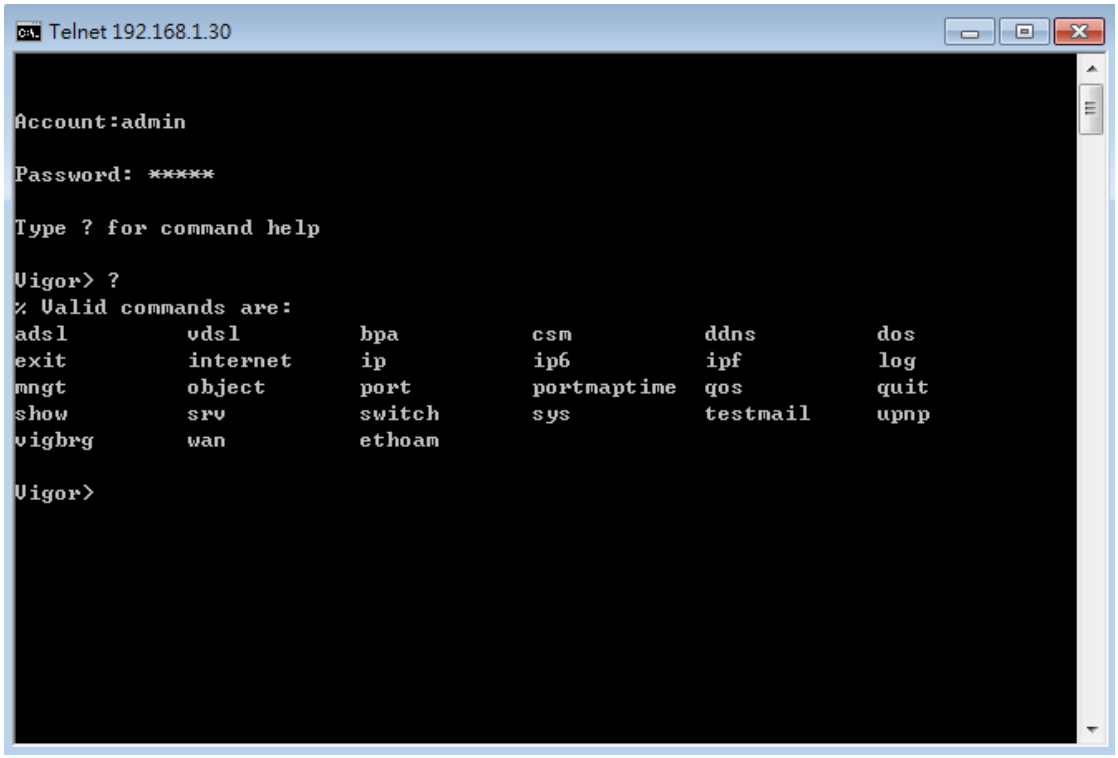
Accessing Telnet of Vigor130

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

Click **Start** > **Run** and type **Telnet 192.168.1.1** in the Open box as below. 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.



Click **OK**. The Telnet terminal will be open. Please type admin/admin for Account/Password. Then, type **?**. You will see a list of valid/common commands depending on the router that your use.



Telnet Command: adsl txpct /adsl rxpct

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

Syntax

adsl txpct [auto:percent]

adsl rxpct [auto:percent]

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

Example

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

Telnet Command: adsl status

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

Syntax

adsl status

Example

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

Telnet Command: adsl ppp

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

Syntax

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

Syntax Description

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

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

Example

```
> adsl ppp o 35 8 1 1 4 1 -1 draytek draytek
pvc no.=0
vci=35
```

```
vpi=8
encap=LLC(1)
proto=PPPoE(1)
modu=MULTI(4)
AcquireIP: Dhcp_client(1)
Idle timeout:-1
Username=draytek
Password=draytek
```

Telnet Command: adsl bridge

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

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

Syntax Description

Parameter	Description
pvc_no	It means *pvc* number and must be between 0(Channel 1) to 7(Channel 8).
status	It means to shown the whole bridge status.
save	It means to save the configuration to flash.
enable	It means to enable the Multi-VLAN function.
disable	It means to 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 and clear all the PVC settings.
tag tag_no	No tag: -1 Available number for tag: 0-4095
pri pri_no	The number 0 to 7 can be set to indicate the priority. “7” is the highest.
service type	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.
px…	It means the number of LAN port (x=2~4). Port 1 is locked for NAT.

Example

```
> adsl bridge 4 on p2 p3
 PVC  Bridge   p1   p2   p3   p4   Service Type   Tag    Pri
```

```
-------------------------------------------------------------
  4    ON      0    0    1    0     Normal    -1(OFF)   0
PVC 0 & 1 can't set for bridge mode.
Please use 'save' to save config.
```

Telnet Command: adsl idle

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

Example

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

Telnet Command: adsl drivemode

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

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

Telnet Command: adsl reboot

This command can wake up the idle router.

Example

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

Telnet Command: adsl oamlb

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

adsl oamlb *[n][type]*

adsl oamlb chklink *[on/off]*

adsl oamlb *[log_on/log_off]*

Syntax Description

Parameter	Description
n	It means the total number of transmitted packets.
type	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)
chklink	Check the DSL connection.
Log_on/log_off	Enable or disable the OAM log for debug.

Example

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

Telnet Command: adsl vcilimit

This command can cancel the limit for vci value.

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

adsl vcilimit *[n]*

Syntax Description

Parameter	Description
n	The number shall be between 1 ~ 254.

Example

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

Telnet Command: adsl annex

This command can display the annex interface of this router.

Example

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

Telnet Command: adsl automode

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

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

Syntax Description

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

Example

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

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

Telnet Command: adsl showbins

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

adsl showbins *[startbin endbin |up]*

Syntax Description

Parameter	Description
startbin	The number is between 0 ~ 517.
endbin	The number is between 4 ~ 511.

Example

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

Telnet Command: adsl optn

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

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

Syntax Description

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

Example

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

Telnet Command: adsl femec

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

adsl fdmec *[mode]*

Syntax Description

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

Example

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

Telnet Command: adsl savecfg

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

Example

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

Telnet Command: adsl vendorid

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

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

Syntax Description

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

Example

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

```
% User define CPE Vendor ID is ON
```

Telnet Command: adsl atm

This command can set QoS parameter for ATM.

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

adsl atm *scr [pvc_no][SCR]*

adsl atm *mbs [pvc_no][MBS]*

adsl atm *status*

Syntax Description

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

Example

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

> adsl atm pcr status
  pvc   channel       PCR
 ---------------------------
   0      1          0
   1      2          200
   2      3          0
   3      4          0
   4      5          0
   5      6          0
   6      7          0
   7      8          0
> adsl atm mbs 2 300 max
% MBS is 300 for pvc 2.
```

Telnet Command: adsl pvcbinding

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

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

Syntax Description

Parameter	Description

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

Example

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

The above example means PVC3 has been bound to PVC5.

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

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

Telnet Command: vdsl status

This command is used for display VDSL status.

Example

```
> vdsl status
  ---------------------- ATU-R Info (hw: annex A, f/w: annex A/B/C) -----------
   Running Mode          :              State               : TRAINING
   DS Actual Rate        :       0 bps   US Actual Rate      :       0 bps
   DS Attainable Rate    :       0 bps   US Attainable Rate  :       0 bps
   DS Path Mode          :       Fast    US Path Mode        :       Fast
   DS Interleave Depth   :       0       US Interleave Depth :       0
   NE Current Attenuation :       0 dB    Cur SNR Margin      :       0  dB
   DS actual PSD         :    0. 0 dB    US actual PSD       :    0. 0  dB
   NE CRC Count          :       0       FE CRC Count        :       0
   NE ES Count           :       0       FE  ES Count        :       0
   Xdsl Reset Times      :       0       Xdsl Link  Times    :       0
   ITU Version[0]        : b5004946      ITU Version[1]      : 544e0000
   VDSL Firmware Version   : 05-04-08-00-00-06
   Power Management Mode   : DSL_G997_PMS_NA
   Test Mode             : DISABLE
  -------------- ATU-C Info ---------------------------------
   Far Current Attenuation :       0 dB    Far SNR Margin      :       0  dB
   CO ITU Version[0]      : 00000000      CO ITU Version[1]    : 00000000
   DSLAM CHIPSET VENDOR    : < unknown >
```

Telnet Command: vdsl idle

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

adsl idle *[on | tcpmessage | tcpmessage_off]*

Syntax Description

Parameter	Description
on	
tcpmessage	
Tcpmessage_off	

Example

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

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

Telnet Command: vdsl drivermode

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

Example

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

Telnet Command: vdsl reboot

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

Example

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

Telnet Command: vdsl annex

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

Example

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

Telnet Command: vdsl showbins

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

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

adsl showbins *[startbin endbin | up]*

Syntax Description

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

Example

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

Telnet Command: vdsl optn

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

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

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

Syntax Description

Parameter	Description
FUNC	**Available settings:** trellis', 'bitswap', 'sra', 'retx', 'aelem', 'status', 'g.vector' ‘default'.
us/ds/bi	us – upstream ds – downstream bi – birection.

value	bitswap=0~2, sra=0~4
on/off	On – Enable the function. Off – Disable the function.

Example

```
>
```

Telnet Command: vdsl savecfg

This command is used to save the confugration.

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

Example

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

Telnet Command: vdsl vendorid

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

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

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

Syntax Description

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

Example

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

Telnet Command: vdsl snr

This command is used to .

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

adsl srn *[delta]*

Syntax Description

Parameter	Description

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

Example

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

Telnet Command: bpa

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

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

Syntax Description

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

Example

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

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

>
```

Telnet Command: csm appe prof

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

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

csm appe prof -i *INDEX [-v | -n NAME]*

Syntax Description

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

Example

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

Telnet Command: csm appe im

It is used to configure IM settings for APP Enforcement Profile.

csm appe im *-i INDEX [-v | -e AP | -d AP| -a AP [ACTION]]*

Syntax Description

Parameter	Description
INDEX	It means to specify the index number of CSM profile, from 1 to 32.
- v	It means to view the IM configuration of the CSM profile.
-e	It means to enable the blocking for specific application.
-d	It means to disable the blocking for specific application.
-a	Set the action of specific application
AP	Specify one of the following applications for such profile. MSN : MSN YIM : YahooIM AIM : AIM ICQ : ICQ QQTM : QQ/TM iChat : iChat Jabber : Jabber/GoogleTalk GC : GoogleChat AliWW : AliWW Skype : Skype Kubao : Kubao Gizmo : Gizmo SIP : SIP/RTP

	TelTel : TelTel TeamSpk: TeamSpeak WIM : WebIMs RaidCall : RaidCall
ACTION	Specify the action of the application, 0 or 1. 0: Block. All of the applications meet the CSM rule will be blocked. 1: Pass. All of the applications meet the CSM rule will be passed.

Example

```
> csm appe im -i 1 -e ICQ Login -a ICQ 0
Profile 1 - : ICQ is enabled.
```

Telnet Command: csm appe p2p

It is used to configure P2P settings for APP Enforcement Profile.

csm appe p2p *-i INDEX [-v | -e AP | -d AP | -a AP [ACTION]]*

Syntax Description

Parameter	Description
INDEX	It means to specify the index number of CSM profile, from 1 to 32.
- v	It means to view the P2P configuration of the CSM profile.
-e	It means to enable the blocking for specific application.
-d	It means to disable the blocking for specific application.
-a	Set the action of specific application, 0 or 1. 0: Block. All of the applications meet the CSM rule will be blocked. 1: Pass. All of the applications meet the CSM rule will be passed.
AP	Specify one of the following applications for such profile. SoulSeek: SoulSeek Protocol eDonkey: eDonkey Protocol FastTrack : FastTrack Protocol OpenFT: OpenFT Protocol Gnutella: Gnutella Protocol OpenNap: OpenNap Protocol BitTorrent: BitTorrent Protocol
ACTION	Specify the action of the application, 0 or 1. 0: Block. All of the applications meet the CSM rule will be blocked. 1: Pass. All of the applications meet the CSM rule will be passed.

Example

```
> csm appe p2p -i 1 -e BitTorrent -a BitTorrent 0
```

```
Profile 1 - : BitTorrent is enabled.
```

Telnet Command: csm appe misc

It is used to configure miscellaneous settings for APP Enforcement Profile.

csm appe misc *-i INDEX [-v | -e AP | -d AP | -a AP [ACTION]]*

Syntax Description

Parameter	Description
INDEX	It means to specify the index number of CSM profile, from 1 to 32.
- v	It means to view the protocol configuration of the CSM profile.
-e	It means to enable the blocking for specific application.
-d	It means to disable the blocking for specific application.
-a	Set the action of specific application, 0 or 1. 0: Block. All of the applications meet the CSM rule will be blocked. 1: Pass. All of the applications meet the CSM rule will be passed.
AP	Specify one of the following applications for such profile. **Streaming:** MMS: MMS RTSP: RTSP TVAnts: TVAnts PPStream: PPStream PPlive: PPlive FeiDian: FeiDian UUSee: UUSee NSPlayer: NSPlayer PCAST: PCAST TVKoo: TVKoo SopCast: SopCast UDLiveX: UDLiveX TVUPlayer: TVUPlayer MySee: MySee Joost: Joost FlashVideo: FlashVideo SilverLight: MS SilverLight Slingbox: Slingbox QVOD: QVOD QQLive: QQLive
ACTION:	Specify the action of the application, 0 or 1. 0: Block. All of the applications meet the CSM rule will be blocked. 1: Pass. All of the applications meet the CSM rule will be passed.

Example

```
> csm appe misc -i 1 -e TVUPlayer -a 0
Profile 1 - : TVUPlayer is enabled.
```

Telnet Command: csm ucf

It is used to configure settings for URL control filter profile.

csm ucf show

csm ucf setdefault

csm ucf msg *MSG*

csm ucf obj *INDEX [-n PROFILE_NAME | -l [P|B|A|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
show	It means to display all of the profiles.
setdefault	It means to return to default settings for all of the profile.
msg MSG	It means de set the administration message. MSG means the content (less than 255 characters) of the message itself.
obj	It means to specify the object for the profile.
INDEX	It means to specify the index number of CSM profile, from 1 to 8.
-n	It means to set the profile name.
PROFILE_NAME	It means to specify the name of the profile (less than 16 characters)
-p	It means to set the priority for the profile.
VALUE	Available numbers you can define are listed below: 0: It means Bundle: Pass. 1: It means Bundle: Block. 2: It means Either: URL Access Control First. 3: It means Either: Web Feature First.
-l	It means the log type of the profile. They are: P: Pass, B: Block, A: All, N: None
MSG	It means to specify the Administration Message, less then 255 characters
uac	It means to set URL Access Control part.
wf	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).

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

ex	
-g	Set the keyword group.
KEY_WORD_Group_Index	Specify the index number of the group profile.

Example

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

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

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

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

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

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

Telnet Command: csm ucf obj INDEX wf

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

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
INDEX	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 restriction of web feature.
-d	It means to disable the restriction of web feature.
-a	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.
-s	It means to enable the the Web Feature configuration. Features available for configuration are: c: Cookie p: Proxy u: Upload
-u	It means to cancel the web feature configuration.
-f	It means to set the file extension object index number.
File_Extension_Object_index	Type the index number (1 to 8) for the file extension object.

Example

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

[ ]Enable URL Access Control
 Action:[block]
 [v] Prevent web access from IP address.
```

```
 No  Obj NO.    Object Name
--- -------- --------------------------------

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

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

Telnet Command: csm wcf

It means to configure the settings regarding to web control filter (wcf).

csm wcf show
csm wcf look
csm wcf cache
csm wcf server WCF_SERVER
csm wcf msg MSG
csm wcf setdefault
csm wcf obj *INDEX -v*
csm wcf obj *INDEX -a P|B*
csm wcf obj *INDEX -n PROFILE_NAME*
csm wcf obj *INDEX -l N|P|B|A*
csm wcf obj *INDEX -o KEY_WORD Object Index*
csm wcf obj *INDEX -g KEY_WORD Group Index*
csm wcf obj *INDEX -w E|D|P|B*
csm wcf obj *INDEX -s CATEGORY|WEB_GROUP*
csm wcf obj *INDEX -u CATEGORY|WEB_GROUP*

Syntax Description

Parameter	Description
show	It means to display the web content filter profiles.
Look	It means to display the license information of WCF.
Cache	It means to set the cache level for the profile.
Server WCF_SERVER	It means to set web content filter server.
Msg MSG	It means de set the administration message. MSG means the content (less than 255 characters) of the message itself.
setdefault	It means to return to default settings for all of the profile.
obj	It means to specify the object profile.
INDEX	It means to specify the index number of web content filter profile, from 1 to 8.
- v	It means to view the web content filter profile.
-a	Set the action of web content filter profile, P or B. B: Block. The web access meets the web feature will be blocked. P: Pass. The web access meets the web feature will be

	passed.
-n	It means to set the profile name.
PROFILE_NAME	It means to specify the name of the profile (less than 16 characters)
-l	It means the log type of the profile. They are: P: Pass, B: Block, A: All, N: None
-o	Set the keyword object.
KEY_WORD_Object_Index	Specify the index number of the object profile.
-g	Set the keyword group.
KEY_WORD_Group_Index	Specify the index number of the group profile.
-w	It means to set the action for the black and white list. E:Enable, D:Disable, P:Pass, B:Block
-s	It means to choose the items under CATEGORY or WEB_GROUP.
-u	It means to discard items under CATEGORY or WEB_GROUP.
WEB_GROUP	Child_Protection, Leisure, Business, Chating, Computer Internet, Other
CATEGORY	Includes: Alcohol & Tobacco, Criminal Activity, Gambling, Hate & Intoleranc, Illegal Drug, Nudity, Pornography/Sexually Explicit, Weapons, Violence, School Cheating,Sex Education, Tasteless, Child Abuse Imges, Entertainment, Games, Sports, Travel, Leisure & Recreation, Fashin & Beauty, Business, Job Search, Web-based Emai, Chat, Instant Messaging, Anonymizers, Forums & Newsgroups, Computers & Technology, Download Sites, Streaming Media & Downloads, Phishing & Fraud, Search Engines & Portals, Social Networking, Spam Sites,Malware, Botnets, Hacking, Illegal Software, Information Security,Peer-to-eer, Advertisements & Pop-Ups, Arts, Transportation, Compromised, Dating & Personals, , Education, Finance, Government,Health & Medcine, News, Non-profits & NGOs, Personal Sites,Politics, Real Estate, Rligion, Restaurants & Dining,Shopping, Translators, General, Cults,Greetig cards, Image Sharing, Network Errors, Parked Domains, Private IP Addresses)

Example

```
> csm wcf obj 1 -n test_wcf
Profile Index: 1
Profile Name:[test_wcf]
[]White/Black list
Action:[block]
  No  Obj NO.    Object Name
 --- -------- --------------------------------
  No  Grp NO.    Group Name
 --- -------- --------------------------------
Action:[block]
Log:[block]
-----------------------------------------------------------------
-------------
child Protection Group:
  [v]Alcohol & Tobacco    [v]Criminal & Activity   [v]Gambling
  [v]Hate & Intolerance    [v]Illegal Drug         [v]Nudity
  [v]Pornography & Sexually explicit  [v]Violence
[v]Weapons

  [v]School Cheating      [v]Sex Education        [v]Tasteless
  [v]Child Abuse Images
-----------------------------------------------------------------
-------------
leisure Group:
  [ ]Entertainment        [ ]Games               [ ]Sports
  [ ]Travel             [ ]Leisure & Recreation  [ ]Fashion & Beauty
.
.
>
```

Telnet Command: ddns log

Displays the DDNS log.

Example

```
>ddns log
>
```

Telnet Command: ddns time

Sets and displays the DDNS time.

ddns time <*update in minutes*>

Syntax Description

Parameter	Description
Update in minutes	Type the value as DDNS time. The range is from 1 to 1440.

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.

dos *[-V | D | A]*

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

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

Syntax Description

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

Example

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

Telnet Command: exit

Type this command will leave telnet window.

Telnet Command: Internet

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

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

Syntax Description

Parameter	Description
-M n	M means to set Internet Access Mode (Mandatory) and n means different modes (represented by 0 – 3) n=0: Offline n=1: PPPoE n=2: Dynamic IP n=3: Static IP
<command><parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-S <isp name>	It means to set ISP Name (max. 23 characters).
-P <on/off>	It means to enable PPPoE Service.
-u <username>	It means to set username (max. 49 characters) for Internet accessing.
-p <password>	It means to set password (max. 49 characters) for Internet accessing.
-a n	It means to set PPP Authentication Type and n means different types (represented by 0-1). n=0: PAP/CHAP (this is default setting) n=1: PAP Only
-t n	It means to set connection duration and n means different conditions. n=-1: Always-on n=1 ~ 999: Idle time for offline (default 180 seconds)
-i <ip address>	It means that *PPPoE server* will assign an IP address specified here for CPE (PPPoE client). If you type 0.0.0.0 as the <ip address>, ISP will assign suitable IP address for you. However, if you type an IP address here, the router will use that one as a fixed IP.
-w <ip address>	It means to assign WAN IP address for such connection. Please type an IP address here for WAN port.
-n <netmask>	It means to assign netmask for WAN connection. You have to type 255.255.255.xxx (x is changeable) as the netmask for WAN port.
-g <gateway>	It means to assign gateway IP for such WAN connection.

-V	It means to view Internet Access profile.

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.

ip 2ndsubnet *<Enable/Disable>*

Syntax Description

Parameter	Description
Enable	Enable the function.
Disable	Disable the function.

Example

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

Telnet Command: ip 2ndaddr

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

ip 2ndaddr *?*

ip 2ndaddr *<2nd subnet IP address>*

Syntax Description

Parameter	Description
?	Display an IP address which allows users set as the public 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 subnet mask for second subnet mask of your router.

ip 2ndmask *?*

ip 2ndmask *<public subnet mask>*

Syntax Description

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

Example

```
> ip 2ndmask ?
% ip 2ndmask <2nd subnet mask>
% Now: 255.255.255.0

> ip 2ndmask 255.255.0.0
% Set 2nd subnet mask done !!!
```

Telnet Command: ip aux

This command is used for configuring WAN IP Alias.

ip aux add *[IP] [Join to NAT Pool]*

ip aux remove *[index]*

Syntax Description

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

Example

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

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

%%    Where IP = Auxiliary WAN IP Address.
%%         Join to NAT Pool = 0 or 1.
%%         Index = The Index number of table.

Now auxiliary WAN1 IP Address table:
Index no.      Status  IP address     NAT IP pool
-----------------------------------------------------
  1          Disable 0.0.0.0 Yes
  2          Enable  192.168.1.65    Yes
```

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

```
Index no.   Status  IP address      IP pool
-------------------------------------------
    1       Enable  172.16.3.229    Yes
    2       Enable  172.16.3.56     No
    3       Enable  172.16.3.113    No
```

Telnet Command: ip addr

This command allows users to set/add a specified LAN IP your router.

ip addr *[IP address]*

Syntax Description

Parameter	Description
IP address	It means the LAN IP address.

Example

```
>ip addr 192.168.50.1
% Set IP address OK !!!
```

Note: 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.

ip nmask *[IP netmask]*

Syntax Description

Parameter	Description
IP netmask	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.

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
IP address	It means the LAN IP address.
MAC address	It means the MAC address of your router.
LAN or WAN	It indicates the direction for the arp function.
0/1/2/3/4/5	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.
Time	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.

ip dhcpc *option*

ip dhcpc *option -h|l*

ip dhcpc *option -d [idx]*

ip dhcpc *option -e [1 or 0] -w [wan unmber] -c [option number] -v [option value]*

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

ip dhcpc *option -u [idx unmber]*

ip dhcpc *release*

ip dhcpc *renew*

ip dhcpc *status*

Syntax Description

Parameter	Description
option	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
release	It means to release current WAN IP address.
renew	It means to renew the WAN IP address and obtain another new one.
status	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.

ip ping *[IP address] [WAN1 /PVC3/PVC4/PVC5]*

Syntax Description

Parameter	Description
IP address	It means the WAN IP address.
WAN1/PVC3/PVC4/PVC5	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.

ip tracert *[Host/IP address] [WAN1/WAN2] [Udp/Icmp]*

Syntax Description

Parameter	Description
IP address	It means the target IP address.
WAN1/WAN2	It means the WAN port that the above IP address passes through.
Udp/Icmp	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.

ip telnet *[IP address][Port]*

Syntax Description

Parameter	Description
IP address	Type the WAN or LAN IP address of the remote device.
Port	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.

ip rip *[0/1/2]*

Syntax Description

Parameter	Description
0/1/2	0 means disable; 1 means first subnet and 2 means second subnet.

Example

```
> ip rip 1
%% Set RIP 1st subnet.
```

Telnet Command: ip wanrip

This command allows users to set the RIP (routing information protocol) of WAN IP.

ip wanrip *[ifno] -e [0/1]*

Syntax Description

Parameter	Description
ifno	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.

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
add	It means to add an IP address as static route.
del	It means to delete specified IP address.
status	It means current status of static route.
dst	It means the IP address of the destination.
netmask	It means the netmask of the specified IP address.
gateway	It means the gateway of the connected router.
ifno	It means the connection interface. 3=WAN1 5=WAN3,6=WAN4,7=WAN5 However, WAN3, WAN4, WAN5 are router-borne WANs
rtype	It means the type of the route. default : default route; static: static route.
cnc	It means current IP range for CNC Network.
default	Set WAN1/WAN2/off as current default route.
clean	Clean all of the route settings. 1: Enable the function. 0: Disable the function.

Example

```
> ip route add 172.16.2.0 255.255.255.0 172.16.2.4 3 static
> ip route status

Codes: C - connected, S - static, R - RIP, * - default, ~ - private
C~       192.168.1.0/   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.

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
set	It means to enable proxy server.
reset	It means to disable proxy server.
wan	It means to specify WAN interface for IGMP service.
t_home	It means to specify t_home proxy server for using.
On/off/show/help	It means to turn on/off/display or get more information of the T_home service.
query	It means to set IGMP general query interval. The default value is 125000 ms.
ppp	0 – No need to set IGMP with PPP header. 1 – Set IGMP with PPP header.
status	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 wanaddr

This command is used to configure WAN IP address.

ip wanaddr *[IP address]]<IP netmask] [gateway ip]*

Syntax Description

Parameter	Description
IP address	Type the IP address for WAN.
IP netmask	Type the net mask for the IP address.
gateway ip	Type the IP address of the gateway.

Example

```
> ip wanaddr 172.16.3.221 255.255.0.0 172.16.3.2
% Set WAN IP address OK !!!
```

Telnet Command: ip wanttr

This command is used to setup the time to return WAN1 from backup WAN.

ip wanttr *[time in seconds]*

Syntax Description

Parameter	Description
time in seconds	The available range is 0 ~600 (seconds).

Example

```
> ip ip wanttr 500
>
```

Telnet Command: ip dmz

Specify MAC address of certain device as the DMZ host.

ip dmz *[mac]*

Syntax Description

Parameter	Description
mac	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.

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
on	It means to turn on session limit for each IP.
off	It means to turn off session limit for each IP.
default [num]	It means to set the default number of session num limit.
Defautlp2p [num]	It means to set the default number of session num limit for p2p.
status	It means to display the current settings.
show	It means to display all session limit settings in the IP range.
timer [num]	It means to set when the IP session block works. The unit is second.
[block/unblock][IP]	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.
add	It means to add the session limits in an IP range.
del	It means to delete the session limits in an IP range.
IP1-IP2	It means the range of IP address specified for this command.
num	It means the number of the session limits, e.g., 100.
p2pnum	It means the number of the session limits, e.g., 50 for P2P.

Example

```
>ip session default 100
> ip session add 192.168.1.5-192.168.1.100 100 50
> ip session on
> ip session status
```

```
  IP range:
    192.168.1.5 - 192.168.1.100 : 100

  Current ip session limit is turn on

  Current default session number is 100
```

Telnet Command: ip bandwidth

This command allows users to set maximum bandwidth limit number for the specified IP.

ip bandwidth *on*

ip bandwidth *off*

ip bandwidth *default [tx_rate][rx_rate]*

ip bandwidth *status*

ip bandwidth *show*

ip bandwidth *[add/del] [IP1-IP2][tx][rx][shared]*

Syntax Description

Parameter	Description
on	It means to turn on the IP bandwidth limit.
off	It means to turn off the IP bandwidth limit.
default [tx_rate][rx_rate]	It means to set default tx and rx rate of bandwidth limit. The range is from 0 – 65535 Kpbs.
status	It means to display the current settings.
show	It means to display all the bandwidth limits settings within the IP range.
add	It means to add the bandwidth within the IP range.
del	It means to delete the bandwidth within the IP range.
IP1-IP2	It means the range of IP address specified for this command.
tx	It means to set transmission rate for bandwidth limit.
rx	It means to set receiving rate for bandwidth limit.
shared	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.

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
on	It means to turn on IP bandmac policy. Even the IP is not in the policy table, it can still access into network.
off	It means to turn off all the bindmac policy.
strict_on	It means that only those IP address in IP bindmac policy table can access into network.
show	It means to display the IP address and MAC address of the pair of binded one.
add	It means to add one ip bindmac.
del	It means to delete one ip bindmac.
IP	It means to type the IP address for binding with specified MAC address.
MAC	It means to type the MAC address for binding with the IP address specified.
Comment	It means to type words as a brief description.
All	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.

ip maxnatuser *user no*

Syntax Description

Parameter	Description
User no	A number specified here means the total NAT users that Vigor router supports. 0 – It means no limitation.

Example

```
> ip maxnatuser 100
% Max NAT user = 100
```

Telnet Command: ip6 addr

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

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
-s	It means to add a static ipv6 address.
-d	It means to delete an ipv6 address.
-a	It means to show current address(es) status.
-u	It means to show only unicast addresses.
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.
LAN|WAN1|WAN2|iface#	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.

ip6 dhcp *req_opt* [*LAN|WAN1|WAN2|iface#] [-<command> <parameter>| ...]*

Syntax Description

Parameter	Description
req_opt	It means option-request.
LAN|WAN1|WAN2|iface#	It means to specify LAN or WAN interface for such address.
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-a	It means to show current DHCPv6 status.
-s	It means to ask the SIP.
-S	It means to ask the SIP name.
-d	It means to ask the DNS setting.
-D	It means to ask the DNS name.
-n	It means to ask NTP.
-i	It means to ask NIS.
-I	It means to ask NIS name.
-p	It means to ask NISP.
-P	It means to ask NISP name.
-b	It means to ask BCMCS.
-B	It means to ask BCMCS name.
-r	It means to ask refresh time.
Parameter	1: the parameter related to the request will be displayed. 0: the parameter related to the request will not be displayed.

Example

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

Telnet Command: ip6 dhcp client

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

ip6 dhcp *client [WAN1|WAN2|iface#] [-<command> <parameter>| ...]*

Syntax Description

Parameter	Description
client	It means the dhcp client settings.
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-a	It means to show current DHCPv6 status.
-p [IAID]	It means to request identity association ID for Prefix Delegation.
-n [IAID]	It means to request identity association ID for Non-temporary Address.
-c [parameter]	It means to send rapid commit to server.
-i [parameter]	It means to send information request to server.
-e[parameter]	It means to enable or disable the DHCPv6 client. 1: Enable 0: Disable

Example

```
> ip6 dhcp client WAN2 –p 2008::1
> ip6 dhcp client WAN2 –a
  Interface WAN2 has following DHCPv6 client settings:
       DHCPv6 client enabled
       request IA_PD whose IAID equals to 2008
> ip6 dhcp client WAN2 –n 1023456
> ip6 dhcp client WAN2 –a
  Interface WAN2 has following DHCPv6 client settings:
       DHCPv6 client enabled
       request IA_NA whose IAID equals to 2008
> system reboot
```

Telnet Command: ip6 dhcp server

This command allows you to configure DHCPv6 server.

ip6 dhcp *server [-<command> <parameter>| ...]*

Syntax Description

Parameter	Description
server	It means the dhcp server settings.
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-a	It means to show current DHCPv6 status.
-<pool_min_addr>	It means to set the start IPv6 address of the address pool.
-x<pool_max_addr>	It means to set the end IPv6 address of the address pool.

-d<addr>	It means to set the first DNS IPv6 address.
-D<addr>	It means to set the second DNS IPv6 address.
-c<parameter>	It means to send rapid commit to server. 1: Enable 0: Disable
-e<parameter>	It means to enable or disable the DHCPv6 server. 1: Enable 0: Disable

Example

```
> ip6 dhcp server -d FF02::1
> ip6 dhcp server -i ff02::1
> ip6 dhcp server -x ff02::3
> ip6 dhcp server -a
% Interface LAN has following DHCPv6 server settings:
%    DHCPv6 server disabled
%    maximum address of the pool: FF02::3
%    minimum address of the pool: FF02::1
%   1st DNS IPv6 Addr: FF02::1
```

Telnet Command: ip6 internet

This command allows you to configure settings for accessing Internet.

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.

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 pneigh

This command allows you to add a proxy neighbour.

ip6 pneigh *-s inet6_addr [LAN|WAN1|WAN2]*

ip6 pneigh *-d inet6_addr [LAN|WAN1|WAN2]*

ip6 pneigh *-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	Spcify 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

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                                  LAN      0   UNICAST     U
                          0    ::
 FE80::250:7FFF:FE00:0/128                   LAN      0   UNICAST     U
                          0    ::
 FE80::/64                                   LAN    256   UNICAST     U
                          0
 FE80::/16                                   LAN   1024   UNICAST     UGA
                          0    FE80::250:7FFF:FE12:100
 FF02::1/128                                 LAN      0   UNICAST     UC
                          0    FF02::1
 FF00::/8                                   LAN    256   UNICAST     U
                          0
 ::/0                                        LAN     -1   UNREACHABLE !
                          0
```

Telnet Command: ip6 ping

This command allows you to pin an IPv6 address or a host.

ip6 ping *[IPV6 address/Host] [LAN/WAN1/WAN2]*

Syntax Description

Parameter	Description
IPV6 address/Host	It means to specify the IPv6 address or host for ping.
LAN/WAN1/WAN2	It means to specify LAN or WAN interface for such address.

Example

```
> ip6 ping 2001:4860:4860::8888 WAN2

Pinging 2001:4860:4860::8888 with 64 bytes of Data:

Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms

Packets: Sent = 5, Received = 5, Lost = 0 <% loss>
>
```

Telnet Command: ip6 tracert

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

ip6 tracert *[IPV6 address/Host]*

Syntax Description

Parameter	Description
IPV6 address/Host	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 tspc

This command allows you to diplay TSPC status.

ip6 tspc *[ifno]*

Syntax Description

Parameter	Description
ifno	It means the connection interface. Ifno=1 (means WAN1) Info=2 (means WAN2)

Example

```
> ip6 tspc 2
Local Endpoint v4 Address : 111.243.177.223
Local Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b9
Router DNS name : 8886666.broker.freenet6.net
Remote Endpoint v4 Address :81.171.72.11
Remote Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b8
Tspc Prefixlen : 56
Tunnel Broker: Amsterdam.freenet.net

Status: Connected
```

```
>
```

Telnet Command: ip6 radvd

This command allows you to enable or disable RADVD server.

Ip6 radvd *–s [1|0] [lifetime]*

ip6 radvd *–V*

Syntax Description

Parameter	Description
-s	It means to enable or disable the default lifetime of the RADVD server. 1: Enable the RADVD server. 0: Disable the RADVD server.
Lifetime	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.
-V	It means to show the RADVD configuration.
-r	It means RA default test.
-r [num]	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.

ip6 mngt list

ip6 mngt list *[add<index> <prefix> <prefix-length>|remove <index>|flush]*

ip6 mngt status

ip6 mngt *[http|telnet|ping] [on|off]*

Syntax Description

Parameter	Description
list	It means to show the setting information of the access list.
status	It means to show the status of IPv6 management.

add	It means to add an IPv6 address which can be used to execute management through Internet.
index	It means the number (1, 2 and 3) allowed to be configured for IPv6 management.
prefix	It means to type the IPv6 address which will be used for accessing Internet.
prefix-length	It means to type a fixed value as the length of the prefix.
remove	It means to remove (delete) the specified index number with IPv6 settings.
flush	It means to clear the IPv6 access table.
http|telnet|ping	These protocols are used for accessing Internet.
on|off	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.

ip6 *online [ifno]*

Syntax Description

Parameter	Description
ifno	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.

ip6 aiccu *[ifno]*

ip6 aiccu subnet *[add <ifno> <prefix> <prefix-length>|remove <ifno>|show <info>]*

Syntax Description

Parameter	Description
ifno	It means the connection interface. 1=WAN1 2=WAN2
add	It means to add an IPv6 address which can be used to execute management through Internet.
prefix	It means to type the IPv6 address which will be used for accessing Internet.
prefix-length	It means to type a fixed value as the length of the prefix.
remove	It means to remove (delete) the specified index number with IPv6 settings.
show	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.

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.

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 filter rule for firewall.

ipf set *[Options]*

ipf set *[SET_NO]* ***rule*** *[RULE_NO] [Options]*

Syntax Description

Parameter	Description
SET_NO	It means to specify the index number (from 1 to 12) of filter set.
RULE_NO	It means to specify the index number (from 1 to 7) of filter rule set.
Options	There are several options provided here, such as *-v, -c [SET_NO], -d [SET_NO], and etc.*
-v	Type “-v” to view the configuration of general set.
-c [SET_NO]	It means to setup Call Filter, e.g., **-c 2**. The range for the index number you can type is “0” to “12” (0 means “disable).
-d [SET_NO]	It means to setup Data Filter, e.g., ***-d 3***. The range for the index number you can type is “0” to “12” (0 means “disable).
-l [VALUE]	It means to setup Log Flag, e.g., ***-l 2*** Type “0” to disable the log flag. Type “1” to display the log of passed packet. Type “2” to display the log of blocked packet. Type “3” to display the log of non-matching packet.
- p [VALUE]	It means to setup actions for packet not matching any rule, e.g., ***-p 1*** Type “0” to let all the packets pass; Type “1” to block all the packets.
-M [P2P_NO]	It means to configure IM/P2P for the packets not matching with any rule, e.g., ***-M 1*** Type “0” to let all the packets pass; Type “1” to block all the packets.
-U [URL_NO]	It means to configure URL content filter for the packets not matching with any rule, e.g., ***-U 1*** Type “0” to let all the packets pass; Type “1” to block all the packets.
-a [AD_SET]	It means to configure the advanced settings.
-f [VALUE]	It means to accept large incoming fragmented UDP or ICMP packets.
-E [VALUE]	It means to set the maximum count for session limitation.

-F [VALUE]	It means to configure the load-balance policy.
-Q [VALUE]	It means to set the QoS class.

Example

```
> ipf set 2 rule 1 -p 0
Setting saved.
> ipf set 2 rule 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       : Any
Destination IP  : Any
Service Type    : TCP/UDP, Port: from 137~139 to 53
Fragments       : Don't Care

Pass or Block               : Pass Immediately
Branch to Other Filter Set  : None
Max Sessions Limit          : 12000
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.

ipf flowtrack set *[-re]*

ipf flowtrack view *[-f]*

ipf flowtrack *[-i][-p][-t]*

Syntax Description

Parameter	Description
-r	It means to refresh the flowtrack.
-e	It means to enable or disable the flowtrack. 0: Disable 1: Enable
-f	It means to show the sessions state of flowtrack. If you do not specify any IP address, then all the session state of flowtrack will be displayed.
-b	It means to show all of IP sessions state.
- i [IP address]	It means to specify IP address (e.g,, -i 192.168.2.55).
-p[value]	It means to type a port number (e.g., -p 1024). Available settings are 0 ~ 65535.
-t [value]	It means to specify a protocol (e.g., -t tcp). Available settings include: *tcp* *udp* *icmp*

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.

log *[-cfhiptwx?] [-F a| c | f | w]*

Syntax Description

Parameter	Description

-c	It means to show the latest call log.
-f	It means to show the IP filter log.
-F	It means to show the flush log buffer. a: flush all logs c: flush the call log f: flush the IP filter log w: flush the WAN log
-h	It means to show this usage help.
-p	It means to show PPP/MP log.
-t	It means to show all logs saved in the log buffer.
-w	It means to show WAN log.
-x	It means to show packet body hex dump.

Example

```
> log -w
25:36:25.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
       Client IP     = 0.0.0.0
       Your IP       = 0.0.0.0
       Next server IP = 0.0.0.0
       Relay agent IP = 0.0.0.0
25:36:33.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
       Client IP     = 0.0.0.0
       Your IP       = 0.0.0.0
       Next server IP = 0.0.0.0
       Relay agent IP = 0.0.0.0
25:36:41.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
       Client IP     = 0.0.0.0
       Your IP       = 0.0.0.0
       Next server IP = 0.0.0.0
       Relay agent IP = 0.0.0.0
25:36:49.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
       Client IP     = 0.0.0.0
       Your IP       = 0.0.0.0
       Next server IP = 0.0.0.0
       Relay agent IP = 0.0.0.0
25:36:57.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
       Client IP     = 0.0.0.0
       Your IP       = 0.0.0.0
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
```

Telnet Command: mngt ftpport

This command allows users to set FTP port for management.

mngt ftpport *[FTP port]*

Syntax Description

Parameter	Description
FTP port	It means to type the number for FTP port. The default setting is 21.

Example

```
> mngt ftpport 21
% Set FTP server port to 21 done.
```

Telnet Command: mngt httpport

This command allows users to set HTTP port for management.

mngt httpport *[Http port]*

Syntax Description

Parameter	Description
Http port	It means to enter the number for HTTP port. The default setting is 80.

Example

```
> mngt httpport 80
% Set web server port to 80 done.
```

Telnet Command: mngt httpsport

This command allows users to set HTTPS port for management.

mngt httpsport *[Https port]*

Syntax Description

Parameter	Description
Https port	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.

mngt telnetport *[Telnet port]*

Syntax Description

Parameter	Description
Telnet port	It means to type the number for telnet port. The default setting is 23.

Example

```
> mngt telnetport 23
% Set Telnet server port to 23 done.
```

Telnet Command: mngt sshport

This command allows users to set SSH port for management.

mngt sshport *[ssh port]*

Syntax Description

Parameter	Description
ssh port	It means to type the number for SSH port. The default setting is 22.

Example

```
> mngt sshport 23
% Set ssh port to 23 done.
```

Telnet Command: mngt ftpserver

This command can enable/disable FTP server.

mngt ftpserver *[enable]*

mngt ftpserver *[disable]*

Syntax Description

Parameter	Description
enable	It means to activate FTP server function.
disable	It means to inactivate FTP server function.

Example

```
> mngt ftpserver enable
%% FTP server has been enabled.

> mngt ftpserver disable
%% FTP server has been disabled.
```

Telnet Command: mngt noping

This command is used to pass or block Ping from LAN PC to the internet.

mngt noping *[on]*

mngt noping *[off]*

mngt noping *[viewlog]*

mngt noping *[clearlog]*

Syntax Description

Parameter	Description
on	All PING packets will be forwarded from LAN PC to Internet.
off	All PING packets will be blocked from LAN PC to Internet.
viewlog	It means to display a log of ping action, including source MAC and source IP.
clearlog	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.

mngt defenseworm *[on]*

mngt defenseworm *[off]*

mngt defenseworm *[add port]*

mngt defenseworm *[del port]*

mngt defenseworm *[viewlog]*

mngt defenseworm *[clearlog]*

Syntax Description

Parameter	Description
on	It means to activate the function of defense worm packet out.
off	It means to inactivate the function of defense worm packet out.
add port	It means to add a new TCP port for block.
del port	It means to delete a TCP port for block.
viewlog	It means to display a log of defense worm packet, including source MAC and source IP.
clearlog	It means to remove the log of defense worm packet.

Example

```
> mngt defenseworm add 21
Add TCP port 21
Block TCP port list: 135, 137, 138, 139, 445, 21
> mngt defenseworm del 21
Delete TCP port 21
Block TCP port list: 135, 137, 138, 139, 445
```

Telnet Command: mngt rmtcfg

This command can allow the system administrators to login from the Internet. By default, it is not allowed.

mngt rmtcfg *[status]*

mngt rmtcfg *[enable]*

mngt rmtcfg *[disable]*

mngt rmtcfg *[http/https/ftp/telnet/ssh/tr069] [on/off]*

Syntax Description

Parameter	Description
status	It means to display current setting for your reference.
enable	It means to allow the system administrators to login from the Internet.

disable	It means to deny the system administrators to login from the Internet.
http/https/ftp/telnet/ssh/tr069	It means to specify one of the servers/protocols for enabling or disabling.
On/off	on – enable the function. off – disable the function.

Example

```
> mngt rmtcfg enable
%% Remote configure function has been enabled.
```

Telnet Command: mngt echoicmp

This command is used to reject or accept PING packets from the Internet.

mngt echoicmp *[enable]*

mngt echoicmp *[disable]*

Syntax Description

Parameter	Description
enable	It means to accept the echo ICMP packet.
disable	It means to drop the echo ICMP packet.

Example

```
> mngt echoicmp enable
%% Echo ICMP packet enabled.
```

Telnet Command: mngt accesslist

This command allows you to specify that the system administrator can login from a specific host or network. A maximum of three IPs/subnet masks is allowed.

mngt accesslist *list*

mngt accesslist *add [index][ip addr][mask]*

mngt accesslist *remove [index]*

mngt accesslist *flush*

Syntax Description

Parameter	Description
list	It can display current setting for your reference.
add	It means adding a new entry.
index	It means to specify the number of the entry.
ip addr	It means to specify an IP address.
mask	It means to specify the subnet mask for the IP address.

remove	It means to delete the selected item.
flush	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.

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 comman is used to create an IP object profile.

object ip obj setdefault

object ip obj *INDEX -v*

object ip obj *INDEX -n NAME*

object ip obj *INDEX -i INTERFACE*

object ip obj *INDEX -s INVERT*

object ip obj I*NDEX -a TYPE [START_IP] [END/MASK_IP]*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX	It means the index number of the specified object profile.
-v	It means to view the information of the specified object profile. Example: `object ip obj 1 -v`
-n NAME	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: `object ip obj 9 -n bruce`
-i INTERFACE	It means to define an interface for the IP object. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=3, means WAN Example: `object ip obj 8 -i 0`
-s INVERT	It means to set invert seletion for the object profile. INVERT=0, means disableing the function. INVERT=1, means enabling the function. Example: `object ip obj 3 -s 1`
-a TYPE	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: `object ip obj 3 -a 2`
[START_IP]	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.

[END/MASK_IP]	Type an IP address (different with START_IP) as the end IP address.

Example

```
> object ip obj 1 -n marketing
> object ip obj 1 -a 1 192.168.1.45
> object ip obj 1 -v
 IP Object Profile 1
 Name   :[marketing]
 Interface:[Any]
 Address type:[single]
 Start ip address:[192.168.1.45]
 End/Mask ip address:[0.0.0.0]
 Invert Selection:[0]
```

Telnet Command: object ip grp

This command is used to integrate several IP objects under an IP group profile.

object ip grp setdefault

object ip grp *INDEX -v*

object ip grp *INDEX -n NAME*

object ip grp *INDEX -i INTERFACE*

object ip grp *INDEX -a IP_OBJ_INDEX*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX	It means the index number of the specified group profile.
-v	It means to view the information of the specified group profile. Example: `object ip grp 1 -v`
-n NAME	It means to define a name for the IP group. NAME: Type a name with less than 15 characters. Example: `object ip grp 8 -n bruce`
-i INTERFACE	It means to define an interface for the IP group. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=2, means WAN Example: `object ip grp 3 -i 0`
-a IP_OBJ_INDEX	It means to specify IP object profiles for the group profile. Example: `:object ip grp 3 -a 1 2 3 4 5` 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.

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
setdefault	It means to return to default settings for all profiles.
INDEX	It means the index number of the specified service object profile.
-v	It means to view the information of the specified service

	object profile. Example: *object service obj 1 -v*
-n NAME	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: *object service obj 9 -n bruce*
-i PROTOCOL	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: *object service obj 8 -i 0*
CHK	It means the check action for the port setting. 0=equal**(=)**, when the starting port and ending port values are the same, it indicates one port; when the starting port and ending port values are different, it indicates a range for the port and available for this service type. 1=not equal**(!=)**, when the starting port and ending port values are the same, it indicates all the ports except the port defined here; when the starting port and ending port values are different, it indicates that all the ports except the range defined here are available for this service type. 2=larger**(>)**, the port number greater than this value is available.. 3=less**(<)**, the port number less than this value is available for this profile.
-s CHK [START_P] [END_P]	It means to set souce port check and configure port range (1~65565) for TCP/UDP. END_P, type a port number to indicate source port. Example: *object service obj 3 -s 0 100 200*
-d CHK [START_P] [END_P]	It means to set destination port check and configure port range (1~65565) for TCP/UDP. END_P, type a port number to indicate destination port. Example: *object service obj 3 -d 1 100 200*

Example

```
> object service obj 1 -n limit
> object service obj 1 -p 255
> object service obj 1 -s 1 120 240
> object service obj 1 -d 1 200 220
> object service obj 1 -v
 Service Object Profile 1
 Name   :[limit]
```

```
Protocol:[255]
Source port check action:[!=]
Source port range:[120~240]
Destination port check action:[!=]
Destination port range:[200~220]
```

Telnet Command: object service grp

This command is used to integrate several service objects under a service group profile.

object service grp setdefault

object service grp *INDEX -v*

object service grp *INDEX -n NAME*

object service grp *INDEX -a SER_OBJ_INDEX*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX	It means the index number of the specified group profile.
-v	It means to view the information of the specified group profile. Example: *`object service grp 1 -v`*
-n NAME	It means to define a name for the service group. NAME: Type a name with less than 15 characters. Example: *`object service grp 8 -n bruce`*
-a SER_OBJ_INDEX	It means to specify service object profiles for the group profile. Example: *`:object service grp 3 -a 1 2 3 4 5`* The service object profiles with index number 1,2,3,4 and 5 will be group under such profile.

Example

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

> object service grp 1 -a 1 2
 Service Group Profile 1
```

```
 Name   :[Grope_1]
 Included service object index:
 [0:][1]
 [1:][2]
 [2:][0]
 [3:][0]
 [4:][0]
 [5:][0]
 [6:][0]
 [7:][0]
```

Telnet Command: object kw

This command is used to create keyword profile.

object kw obj setdefault

object kw obj show PAGE

object kw obj *INDEX -v*

object kw obj *INDEX -n NAME*

object kw obj *INDEX -a CONTENTS*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
show PAGE	It means to show the contents of the specified profile. PAGE: type the page number.
show	It means to show the contents for all of the profiles.
INDEX	It means the index number of the specified keyword profile.
-v	It means to view the information of the specified keyword profile.
-n NAME	It means to define a name for the keyword profile. NAME: Type a name with less than 15 characters.
-a CONTENTS	It means to set the contents for the keyword profile. Example: *object kw obj 40 -a test*

Example

```
> object kw obj 1 -n children
 Profile 1
 Name   :[children]
 Content:[]
> object kw obj 1 -a gambling
 Profile 1
 Name   :[children]
 Content:[gambling]

> object kw obj 1 -v
```

```
Profile 1
Name   :[children]
Content:[gambling]
```

Telnet Command: object fe

This command is used to create File Extension Object profile.

object fe show

object fe setdefault

object fe obj *INDEX -v*

object fe obj *INDEX -n NAME*

object fe obj *INDEX -e CATEGORY|FILE_EXTENSION*

object fe obj *INDEX -d CATEGORY|FILE_EXTENSION*

Syntax Description

Parameter	Description
show	It means to show the contents for all of the profiles.
setdefault	It means to return to default settings for all profiles.
INDEX	It means the index number (from 1 to 8) of the specified file extension object profile.
-v	It means to view the information of the specified file extension object profile.
-n NAME	It means to define a name for the file extension object profile. NAME: Type a name with less than 15 characters.
-e	It means to enable the specific CATEGORY or FILE_EXTENSION.
-d	It means to disable the specific CATEGORY or FILE_EXTENSION
CATEGORY|FILE_EXTENSION	CATEGORY: Image, Video, Audio, Java, ActiveX, Compression, Executation Example: *`object fe obj 1 -e Image`* 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: *object fe obj 1 -e .bmp*

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
------------------------------------------------------------------------
------
Executation 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.

port *[1,2,all] [AN, 100F, 100H, 10F, 10H, status]*

port status

port wanfc

Syntax Description

Parameter	Description
1,2,all	It means the number of LAN port.
AN… 10H	It means the physical type for the specific port. AN: auto-negotiate. 100F: 100M Full Duplex. 100H: 100M Half Duplex. 10F: 10M Full Duplex. 10H: 10M Half Duplex.
status	It means to view the Ethernet port status.
wanfc	It means to set WAN flow control.

Example

```
> port 1 100F
%Set Port 1 Force speed 100 Full duplex OK !!!
```

Telnet Command: portmaptime

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

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

Syntax Description

Parameter	Description
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-t <sec>	It means “TCP” protocol. <sec>: Type a number to set the TCP session timeout.
-u <sec>	It means “UDP” protocol. <sec>: Type a number to set the UDP session timeout.
-i <sec>	It means “IGMP” protocol. <sec>: Type a number to set the IGMP session timeout.
-w <sec>	It means “TCP WWW” protocol. <sec>: Type a number to set the TCP WWW session

	timeout.
-s <sec>	It means “TCP SYN” protocol. <sec>: Type a number to set the TCP SYN session timeout.
-f	It means to flush all portmaps (useful for diagnostics).
-l <List>	List all settings.

Example

```
> portmaptime -t 86400 -u 300  -i 10
> portmaptime -l
------ Current setting ------
TCP Timeout   : 86400 sec.
UDP Timeout   : 300 sec.
IGMP Timeout  : 10 sec.
TCP WWW Timeout: 60 sec.
TCP SYN Timeout: 60 sec.
```

Telnet Command: qos setup

This command allows user to set general settings for QoS.

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

Syntax Description

Parameter	Description
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-h	Type it to display the usage of this command.
-m <mode>	It means to define which traffic the QoS control settings will apply to and eable QoS control. 0: disable. 1: in, apply to incoming traffic only. 2: out, apply to outgoing traffic only. 3: both, apply to both incoming and outgoing traffic. Default is enable (for outgoing traffic).
-i <bandwidth>	It means to set inbound bandwidth in kbps (Ethernet WAN only) The available setting is from 1 to 100000.
-o <bandwidth>	It means to set outbound bandwidth in kbps (Ethernet WAN only). The available setting is from 1 to 100000.
-r <index:ratio>	It means to set ratio for class index, in %.
-u <mode>	It means to enable bandwidth control for UDP. 0: disable 1: enable Default is disable.

-p <ratio>	It means to enable bandwidth limit ratio for UDP.
-t <mode>	It means to enable/disable Outbound TCP ACK Prioritize. 0: disable 1: enable
-V	Show all the settings.
-D	Set all to factory default (for all WANs).
[…]	It means that you can type in several commands in one line.

Example

```
> qos setup -m 3 -i 9500 -o 8500 -r 3:20 -u 1 -p 50 -t 1

 WAN1 QOS mode is both
 Wan 1 is XDSL model ,don,t need to set up
 Wan 1 is XDSL model ,don,t need to set up
 WAN1 class 3 ratio set to 20
 WAN1 udp bandwidth control set to enable
 WAN1 udp bandwidth limit ratio set to 50
 WAN1 Outbound TCP ACK Prioritizel set to enable
QoS WAN1 set complete; restart QoS
>
```

Telnet Command: qos class

This command allows user to set QoS class.

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. *Addr1* – It means Single address. Please specify the IP address directly, for example, "*-l 172.16.3.9*". *addr1:addr2* – It means Range address. Please specify the IP addresses, for example, "*-l 172.16.3.9: 172.16.3.50*." *addr1:subnet* – It means the subnet address with start IP address. Please type the subnet and the IP address, for example, "*-l 172.16.3.9:255.255.0.0".0* *any* – It means Any address. Simple type "*-l*" to specify any address for this command.
-r <addr>	Set the remote address. *addr1* – It means Single address. Please specify the IP address directly, for example, "*-l 172.16.3.9*". *addr1:addr2* – It means Range address. Please specify the IP addresses, for example, "*-l 172.16.3.9: 172.16.3.50*." *addr1:subnet* – It means the subnet address with start IP address. Please type the subnet and the IP address, for example, "*-l 172.16.3.9:255.255.0.0".0* *any* – It means Any address. Simple type "*-l*" to specify any address for this command.
-p <DSCP id>	Specify the ID.

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

Example

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

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

Telnet Command: qos type

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

qos type *[-a <service name> | -e <no> | -d <no>]*.

Syntax Description

Parameter	Description
-a <name>	It means to add rule.
-e <no>	It means to edit user defined service type. “no” means the index number. Available numbers are 1~40.
-d <no>	It means to delete user defined service type. “no” means the index number. Available numbers are 1~40.
-n <name>	It means the name of the service.
-t <type>	It means protocol type. 6: tcp(default) 17: udp 0: tcp/udp <1~254>: other
-p <port>	It means service port. The typing format must be [start:end] (ex., 510:330).
-l	List user defined types. “no” means the index number. Available numbers are 1~40.

Example

```
> qos type -a draytek -t 6 -p 510:1330

 service name set to draytek
 service type set to 6:TCP
 Port type set to Range
 Service Port set to 510 ~ 1330
>
```

Telnet Command: quit

This command can exit the telnet command screen.

Telnet Command: show lan1

This command displays current status of LAN1 IP address settings.

Example

```
> show lan1
%% 1st subnet settings:
%%     IP address: 192.168.1.1
%%     Subnet mask: 255.255.255.0
%%     RIP : [1st Subnet]
```

Telnet Command: show lan2

This command displays current status of LAN2 IP address settings.

Example

```
> show lan2
%% 2nd subnet settings:
%%     Status: [Active]
%%     IP address: 192.168.2.5
%%     Subnet mask: 255.255.0.0
%%     RIP : [1st Subnet]
```

Telnet Command: show dhcp

This command displays current status of DHCP server.

Example

```
> 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 172.16.3.221
   2    Disable 192.168.1.65
```

Telnet Command: show dns

This command displays current status of DNS setting

Example

```
> show dns
%%     Domain name server settings:
%            Primary DNS: [Not set]
%            Secondary DNS: [Not set]
```

Telnet Command: show openport

This command displays current status of open port setting.

Example

```
> show openport
%%     Openport settings:
Index   Status  Comment        Local IP Address
*******************************************************
                 No data entry.
```

Telnet Command: show nat

This command displays current status of NAT.

Example

```
> show nat
 Port Redirection Running Table:

Index  Protocol  Public Port   Private IP       Private Port
 1          0          0   0.0.0.0                  0
 2          0          0   0.0.0.0                  0
 3          0          0   0.0.0.0                  0
 4          0          0   0.0.0.0                  0
 5          0          0   0.0.0.0                  0
 6          0          0   0.0.0.0                  0
 7          0          0   0.0.0.0                  0
 8          0          0   0.0.0.0                  0
 9          0          0   0.0.0.0                  0
10          0          0   0.0.0.0                  0
11          0          0   0.0.0.0                  0
12          0          0   0.0.0.0                  0
13          0          0   0.0.0.0                  0
14          0          0   0.0.0.0                  0
15          0          0   0.0.0.0                  0
```

```
16          0          0   0.0.0.0                   0
17          0          0   0.0.0.0                   0
18          0          0   0.0.0.0                   0
19          0          0   0.0.0.0                   0
20          0          0   0.0.0.0                   0
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
```

Telnet Command: show portmap

This command displays the table of NAT Active Sessions.

Example

```
> show portmap
-------------------------------------------------------------------------
  Private_IP:Port Pseudo_IP:Port Peer_IP:Port [Timeout/Protocol/Flag]
-------------------------------------------------------------------------
```

Telnet Command: show pmtime

This command displays the reuse time of NAT session.

Level0: It is the default setting.

Level1: It will be applied when the NAT sessions are smaller than 25% of the default setting.

Level2: It will be applied when the NAT sessions are smaller than the eighth of the default setting.

Example

```
> show pmtime
  Level0 TCP=86400001 UDP=300001 ICMP=10001
  Level1 TCP=600000 UDP=90000 ICMP=7000
  Level2 TCP=60000 UDP=30000 ICMP=5000
```

Telnet Command: show session

This command displays current status of current session.

Example

```
> show session
% Maximum Session Number: 10000
% Maximum Session Usage: 49
% Current Session Usage: 0
% Current Session Used(include waiting for free): 0
% WAN1 Current Session Usage: 0
```

Telnet Command: show status

This command displays current status of LAN and WAN connections.

Example

```
> show status
System Uptime:20:36:35
LAN Status
Primary DNS:8.8.8.8          Secondary DNS:8.8.4.4
IP Address:192.168.1.1       Tx Rate:12923    Rx Rate:8152

WAN 1 Status: Disconnected
Enable:Yes      Line:xDSL       Name:tcom
```

```
Mode:Static IP   Up Time:0:00:00     IP:172.16.3.221   GW
IP:172.16.3.2
TX Packets:0         TX Rate:0   RX Packets:0         RX Rate:0

ADSL Information:      ADSL Firmware Version:05-04-04-04-00-01
Mode:                 State:TRAINING   TX Block:0     RX Block:0
Corrected Blocks:0     Uncorrected Blocks:0
UP Speed:0         Down Speed:0         SNR Margin:0   Loop Att.:0
```

Telnet Command: show adsl

This command displays current status of ADSL.

Example

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

Telnet Command: show statistic

This command displays statistics for WAN interface.

show statistic

show statistic reset *[interface]*

Syntax Description

Parameter	Description
reset	It means to reset the transmitted/received bytes to Zero.
interface	It means to specify WAN1 ~WAN5 (including multi-PVC) interface for displaying related statistics.

Example

```
> show statistic
 WAN1 total TX: 0 Bytes ,RX: 0 Bytes
 WAN2 total TX: 0 Bytes ,RX: 0 Bytes
 WAN3 total TX: 0 Bytes ,RX: 0 Bytes
 WAN4 total TX: 0 Bytes ,RX: 0 Bytes
 WAN5 total TX: 0 Bytes ,RX: 0 Bytes
 >
```

Telnet Command: srv dhcp badip

This command is reserved for future using.

srv dhcp badip

Example

```
> srv dhcp badip
>
```

Telnet Command: srv dhcp public

This command allows users to configure DHCP server for second subnet.

srv dhcp public *start [IP address]*

srv dhcp public *cnt [IP counts]*

srv dhcp public *status*

srv dhcp public *add [MAC Addr XX-XX-XX-XX-XX-XX]*

srv dhcp public *del [MAC Addr XX-XX-XX-XX-XX-XX/all/ALL]*

Syntax Description

Parameter	Description
start <IP address>	It means the starting point of the IP address pool for the DHCP server. *<IP address>:* Specify an IP address as the starting point in the IP address pool.
cnt <IP counts>	It means the IP count number. *<IP counts>:* Specify the number of IP addresses in the pool. The maximum is 10.
status	It means the execution result of this command.
add <MAC Addr XX-XX-XX-XX-XX-XX>	It means creating a list of hosts to be assigned. <MAC Addr XX-XX-XX-XX-XX-XX>: Specify MAC Address of the host.
del <MAC Addr XX-XX-XX-XX-XX-XX/all/ALL>	It means removing the selected MAC address. <MAC Addr XX-XX-XX-XX-XX-XX>: Specify MAC Address of the host. all/ALL: It means all of the MAC addresses.

Example

```
Vigor> srv dhcp public start 192.168.1.100
%% You must enable IP routing !!!
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.

srv dhcp dns1 *[?]*

srv dhcp dns1 *[DNS IP address]*

Syntax Description

Parameter	Description
?	It means to display current IP address of DNS 1 for the DHCP server.
DNS IP address	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.

srv dhcp dns2 *[?]*

srv dhcp dns2 *[DNS IP address]*

Syntax Description

Parameter	Description
?	It means to display current IP address of DNS 2 for the DHCP server.
DNS IP address	It means the IP address that you want to use as DNS2. **Note:** The IP Routed Subnet DNS must be the same as NAT Subnet DNS).

Example

```
> srv dhcp dns2 10.1.1.1
% srv dhcp dns2 <DNS IP address>
% Now: 10.1.1.1
(IP Routed Subnet dns same as NAT Subnet dns)
```

Telnet Command: srv dhcp frcdnsmanl

This command can force the router to invoke DNS Server IP address.

srv dhcp frcdnsmanl *[on]*

srv dhcp frcdnsmanl *[off]*

Syntax Description

Parameter	Description
?	It means to display the current status.
on	It means to use manual setting for DNS setting.
Off	It means to use auto settings acquired from ISP.

Example

```
> srv dhcp frcdnsmanl on
% Domain name server now is using manual settings!
> srv dhcp frcdnsmanl off
% Domain name server now is using auto settings!
```

Telnet Command: srv dhcp gateway

This command allows users to specify gateway address for DHCP server.

srv dhcp gateway *[?]*

srv dhcp gateway *[Gateway IP]*

Syntax Description

Parameter	Description
?	It means to display current gateway that you can use.
Gateway IP	It means to specify a gateway address used for DHCP server.

Example

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

Telnet Command: srv dhcp ipcnt

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

srv dhcp ipcnt *[?]*

srv dhcp ipcnt *[IP counts]*

Syntax Description

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

Example

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

Telnet Command: srv dhcp off

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

Telnet Command: srv dhcp on

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

Telnet Command: srv dhcp relay

This command allows users to set DHCP relay setting.

srv dhcp relay servip *[server ip]*

srv dhcp relay subnet *[index]*

Syntax Description

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

Example

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

Telnet Command: srv dhcp startip

srv dhcp startip *[?]*

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.

srv dhcp leasetime *[?]*

srv dhcp leasetime *[Lease Time (sec)]*

Syntax Description

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

Example

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

Telnet Command: srv dhcp nodetype

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

srv dhcp nodetype <*count*>

Syntax Description

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

Example

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

Telnet Command: srv dhcp primWINS

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

srv dhcp primWINS *[WINS IP address]*

srv dhcp primWINS clear

Syntax Description

Parameter	Description
WINS IP address	It means the IP address of primary WINS server.
clear	It means to remove the IP address settings of primary WINS server.

Example

```
> srv dhcp primWINS 192.168.1.88
> srv dhcp primWINS ?
%% srv dhcp primWINS <WINS IP address>
%% srv dhcp primWINS clear
% Now: 192.168.1.88
```

Telnet Command: srv dhcp secWINS

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

srv dhcp secWINS *[WINS IP address]*

srv dhcp secWINS clear

Syntax Description

Parameter	Description
WINS IP address	It means the IP address of secondary WINS server.
clear	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.

srv dhcp expRecycleIP *<sec time>*

Syntax Description

Parameter	Description
sec time	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.

srv dhcp tftp *<TFTP server name>*

Syntax Description

Parameter	Description
TFTP server name	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.

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 unmber]*

Syntax Description

Parameter	Description
-h	It means to display usage of this command.
-l	It means to display all the user defined DHCP options.
-d[idx]	It means to delete the option number by specifying its index number.
-e [1 or 0]	It means to enable/disable custom option feature. 1:enable 0:disable
-c	It means to set option number. Available number ranges from 0 to 255.
-v	It means to set option number by typing string.
-a	It means to set the option value by specifying the IP address.
-x	It means to set option number with the format of Hexadecimal characters.
-u	It means to update the option value of the sepecified index.
idx number	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.

Srv nat dmz n m *[-<command> <parameter> | …]*

Syntax Description

Parameter	Description
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can Enter several commands in one line.
n	It means to map selected WAN IP to certain host. 1: wan1 2: wan2
m	It means the index number (1 to 8) 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.
-e	It means to enable/disable such feature. 1:enable 0:disable
-i	It means to specify the private IP address of the DMZ host.
-r	It means to remove DMZ host setting.
-v	It means to display current status.

Example

```
> srv nat dmz mapping 1 1 -i 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.

Srv nat ipsecpass *[options]*

Syntax Description

Parameter	Description
[options]	The available commands with parameters are listed below.
on	It means to enable IPSec ESP tunnel passthrough and IKE source port (500) preservation.
off	It means to disable IPSec ESP tunnel passthrough and IKE source port (500) preservation.
status	It means to display current status for checking.

Example

```
> srv nat ipsecpass status
%% Status: IPsec ESP pass-thru and IKE src_port:500 preservation is
OFF.
```

Telnet Command: srv nat openport

This command allows users to set open port settings for NAT server.

srv nat openport n m *[-<command> <parameter> | …]*

Syntax Description

Parameter	Description
n	It means the index number for the profiles. The range is from 1 to 20.
m	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.

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
Add[idx]	It means to add a new port redirection table with an index number. Available index number is from 1 to 10.
serv name	It means to type one name as service name.
proto	It means to specify TCP or UDP as the protocol.
pub port	It means to specify which port can be redirected to the specified Private IP and Port of the internal host.
pri ip	It means to specify the private IP address of the internal host providing the service.
pri port	It means to specify the private port number of the service offered by the internal host.
wan1/wan2	It means to specify WAN interface for the port redirection.
del [idx]	It means to remove the selected port redirection setting.
disable [idx]	It means to inactivate the selected port redirection setting.

enable [idx]	It means to activate the selected port redirection setting.
flush	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 ifno
 1    game             6         80   192.168.1.11        100     -1
 2                    0          0                    0     -2
 3                    0          0                    0     -2
 4                    0          0                    0     -2
 5                    0          0                    0     -2
 6                    0          0                    0     -2
 7                    0          0                    0     -2
 8                    0          0                    0     -2
 9                    0          0                    0     -2
10                    0          0                    0     -2
11                    0          0                    0     -2
12                    0          0                    0     -2
13                    0          0                    0     -2
14                    0          0                    0     -2
15                    0          0                    0     -2
16                    0          0                    0     -2
17                    0          0                    0     -2
18                    0          0                    0     -2

19                    0          0                    0     -2

20                    0          0                    0     -2


Protocol: 0 = Disable, 6 = TCP, 17 = UDP
```

Telnet Command: srv nat status

This command allows users to view NAT Port Redirection Running Table.

Example

```
> srv nat status
NAT Port Redirection Running Table:

Index  Protocol  Public Port   Private IP       Private Port
 1          6          80   192.168.1.11            100
 2          0           0   0.0.0.0                   0
 3          0           0   0.0.0.0                   0
 4          0           0   0.0.0.0                   0
 5          0           0   0.0.0.0                   0
 6          0           0   0.0.0.0                   0
 7          0           0   0.0.0.0                   0
 8          0           0   0.0.0.0                   0
 9          0           0   0.0.0.0                   0
10          0           0   0.0.0.0                   0
```

```
11          0          0   0.0.0.0                    0
12          0          0   0.0.0.0                    0
13          0          0   0.0.0.0                    0
14          0          0   0.0.0.0                    0
15          0          0   0.0.0.0                    0
16          0          0   0.0.0.0                    0
17          0          0   0.0.0.0                    0
18          0          0   0.0.0.0                    0
19          0          0   0.0.0.0                    0

20          0          0   0.0.0.0                    0

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

Telnet Command: srv nat 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: sys cfg

This command reset the router with factory default settings. When a user types this command, all the configuration will be reset to default setting.

sys cfg default

sys cfg status

Syntax Description

Parameter	Description
default	It means to reset current settings with default values.
status	It means to display current profile version and status.

Example

```
> sys cfg status
Profile version: 3.0.0   Status: 1 (0x491e5e6c)
> sys cfg default
>
```

Telnet Command: sys cmdlog

This command displays the history of the commands that you have typed.

Example

```
> sys cmdlog
% Commands Log: (The lowest index is the newest !!!)
    [1] sys cmdlog
    [2] sys cmdlog ?
    [3] sys ?
    [4] sys cfg status
    [5] sys cfg ?
```

Telnet Command: sys ftpd

This command displays current status of FTP server.

sys ftpd *on*

sys ftpd *off*

Syntax Description

Parameter	Description
on	It means to turn on the FTP server of the system.
off	It means to turn off the FTP server of the system.

Example

```
> sys ftpd on
% sys ftpd turn on !!!
```

Telnet Command: sys domainname

This command can set and remove the domain name of the system when DHCP mode is selected for WAN.

sys domainname *[wan1/wan2] [Domain Name Suffix]*

sys domainname *[wan1/wan2]*

Syntax Description

Parameter	Description
wan1/wan2	It means to specify WAN interface for assigning a name for it.
Domain Name Suffix	It means the name for the domain of the system. The maximum number of characters that you can set is 40.
clear	It means to remove the domain name of the system.

Example

```
> sys domainname wan1 clever
> sys domainname wan2 intellegent
> sys domainname ?
```

```
% sys domainname <wan1/wan2> <Domain Name Suffix (max. 40 characters)>
% sys domainname <wan1/wan2> clear
% Now: wan1 == clever, wan2 ==intelligent
>
```

Telnet Command: sys iface

This command displays the current interface connection status (UP or Down) with IP address, MAC address and Netmask for the router.

Example

```
> sys iface
Interface 0 Ethernet:
Status: UP
IP Address: 192.168.1.1      Netmask: 0xFFFFFF00 (Private)
IP Address: 0.0.0.0          Netmask: 0xFFFFFFFF
MAC: 00-50-7F-00-00-00
Interface 4 Ethernet:
Status: DOWN
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-02
Interface 5 Ethernet:
Status: DOWN
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-03
Interface 6 Ethernet:
Status: DOWN
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-04
Interface 7 Ethernet:
Status: DOWN
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-05
Interface 8 Ethernet:
Status: DOWN
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-06

Interface 9 Ethernet:
Status: DOWN
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-07
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
>
```

Telnet Command: sys name

This command can set and remove the name for the router when DHCP mode is selected for WAN.

sys name *[wan1] [ASCII string]*

sys name *[wan1]* **clear**

Syntax Description

Parameter	Description
wan1	It means to specify WAN interface for assigning a name for it.
ASCII string	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
ASCII string	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.

sys autoreboot *[on/off/hour(s)]*

Syntax Description

Parameter	Description
on/off	On – It means to enable the function of auto-reboot. Off – It means to disable the function of auto-reboot.
hours	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 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: Vigor130    Version: 3.7.1.3 English
Profile version: 3.0.0    Status: 1 (0x495b9fec)
Router IP: 192.168.1.1    Netmask: 255.255.255.0
Firmware Build Date/Time: Oct 15 2013 13:46:37
Router Name:
Revision: 37612 130_3712
ADSL Firmware Version: 05-04-04-04-00-01 Annex A
```

Telnet Command: sys qrybuf

This command can display the system memory status and leakage list.

Example

```
> sys qrybuf
System Memory Status and Leakage List

Buf sk_buff    ( 200B), used#: 1647, cached#:     30
Buf KMC4088    (4088B), used#:       0, cached#:      8
Buf KMC2552    (2552B), used#: 1641, cached#:     42
Buf KMC1016    (1016B), used#:       7, cached#:      1
Buf KMC504     ( 504B), used#:       8, cached#:      8
Buf KMC248     ( 248B), used#:     26, cached#:     22
Buf KMC120     ( 120B), used#:     67, cached#:     61
Buf KMC56      (  56B), used#:     20, cached#:     44
Buf KMC24      (  24B), used#:     58, cached#:     70
Dynamic memory: 13107200B; 4573168B used; 190480B/0B in level 1/2 cache.

FLOWTRACK Memory Status
# of free = 12000
# of maximum = 0
# of flowstate = 12000
# of lost by siganture = 0
# of lost by list = 0
```

Telnet Command: sys pollbuf

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

sys pollbuf *[on]*

sys pollbuf *[off]*

Syntax Description

Parameter	Description
on	It means to turn on pulling buffer.
off	It means to turn off pulling buffer.

Example

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

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

Telnet Command: sys britask

This command can improve triple play quality.

sys britask *[on]*

sys britask *[off]*

Syntax Description

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

Example

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

Telnet Command: sys tr069

This command can set CPE settings for applying in VigorACS.

sys tr069 get *[parm] [option]*

sys tr069 set *[parm] [value]*

sys tr069 getnoti *[parm]*

sys tr069 setnoti *[parm] [value]*

sys tr069 log

sys tr069 debug *[on/off]*

sys tr069 save

sys tr069 inform *[event code]*

sys tr069 port *[port num]*

sys tr069 cert_auth *[on/off]*

Syntax Description

Parameter	Description
get [parm] [option]	It means to get parameters for tr-069. option=<nextlevel>: only gets nextlevel for GetParameterNames.
set [parm] [value]	It means to set parameters for tr-069.
getnoti [parm]	It means to get parameter notification value.
setnoti [parm] [value]	It means to set parameter notification value.
log	It means to display the TR-069 log.
debug [on/off]	on: turn on the function of sending debug message to syslog. off: turn off the function of sending debug message to syslog.

save	It means to save the parameters to the flash memory of the router.
Inform [event code]	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"
port [port num]	It means to change tr069 listen port number.
cert_auth [on/off]	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.

sys sip_alg *[1]*

sys sip_alg *[0]*

Syntax Description

Parameter	Description
1	It means to turn on SIP ALG.
0	It means to turn off SIP ALG.

Example

```
> sys sip_alg ?
usage: sys sip_alg [value]
 0 - disable SIP ALG
 1 - enable SIP ALG
 current SIP ALG is disabled
```

Telnet Command: sys license

This command can process the system license.

sys license *licmsg*

sys license *licauth*

sys license *regser*

sys license *licera*

sys license *licifno*

sys license *lic_wiz [set/reg/qry]*

sys license *dev_chg*

sys license *dev_key*

Syntax Description

Parameter	Description
licmsg	It means to display license message.
licauth	It means the license authentication time setting.
regser	It means the license register server setting.
licera	It means to erase license setting.
licifno	It means license and signature download interface setting.
lic_wiz [set/reg/qry]	It means the license wizard setting. qry: query service support status set [idx] [trial] [service type] [sp_id] [start_date] [License Key] reg: register service in portal

dev_chg	It means to change the device key.
dev_key	It means to show device key.

Example

```
> sys license licifno

License and Signature download interface setting:
licifno [AUTO/WAN#]

Ex: licifno wan1

Download interface is "auto-selected" now.
```

Telnet Command: sys diag_log

This command is used for RD debug.

sys diag_log *[status| enable| disable| flush| lineno [w] | level [x] | feature [on|off] [y]| log]*

Syntax Description

Parameter	Description
status	It means to show the status of diagnostic log.
enable	It means to enable the function of diag_log.
disable	It means to disenable the function of diag_log.
flush	It means the flush log buffer.
lineno [w]	It means the total lines for displaying message. w - Available value ranges from 100 to 50000.
level[x]	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.
feature [on/off]	It is used to specify the function of the log. Supported features include SYS and DSL (Case-Insensitive). Default setting is “on” for “DSL”.
log	It means the dump log buffer.

Example

```
> sys diag_log status
 Status:
 diag_log is Enabled.
 lineno : 10000.
 level : 3.
 Enabled feature: SYS DSL
> sys diag_log log
0:00:02    [DSL] Current modem firmware: AnnexA_548006_544401
0:00:02    [DSL] Modem firmware feature: 5, ADSL_A, VDSL2
0:00:02    [DSL] xtseCfg=04 00 04 00 0c 01 00 07
```

```
0:00:02   [DSL] don't have last showtime mode!! set next mode to VDSL!!
0:00:02   [DSL] Status has changed: Stopped(0) -> FwWait(3)
0:00:02   [DSL] Status has changed: FwWait(3) -> Starting(1)
0:00:02   [DSL] Status has changed: Starting(1) -> Running(2)
0:00:02   [DSL] Status was switched: firmwareReady(3) to Init(5)
0:00:02   [DSL] Status was switched: Init(5) to Restart(10)
0:00:02   [DSL] Status was switched: Restart(10) to
FirmwareRequest(1)
0:00:02   [DSL] Line state has changed: 00000000 -> 000000FF
0:00:02   [DSL] Entering VDSL2 mode
0:00:03   [DSL] modem code: [05-04-08-00-00-06]
0:00:05   [DSL] Status was switched: FirmwareRequest(1) to
firmwareReady(3)
0:00:05   [DSL] Status was switched: firmwareReady(3) to Init(5)
0:00:05   [DSL] >> nXtseA=0d, nXtseB=00, nXtseV=07, nFwFeatures=5
0:00:05   [DSL] >> nHsToneGroupMode=0, nHsToneGroup=106,
nToneSet=43, nCamState
=2
0:00:05   [DSL] Line state has changed: 000000FF -> 00000100
0:00:05   [DSL] Line state has changed: 00000100 -> 00000200
0:00:05   [DSL] Status was switched: Init(5) to Train(6)
```

Telnet Command: testmail

This command is used to display current settings for sending test mail.

Example

```
> testmail
Send out test mail
 Mail Alert:[Disable]
 SMTP_Server:[0.0.0.0]
 Mail to:[]
 Return-Path:[]
```

Telnet Command: upnp off

This command can close UPnP function.

Example

```
>upnp off
UPNP say bye-bye
```

Telnet Command: upnp on

This command can enable UPnP function.

Example

```
>upnp on
UPNP start.
```

Telnet Command: upnp nat

This command can display IGD NAT status.

Example

```
> upnp nat ?
******************  IGD NAT Status  ****************

((0))
InternalClient >>192.168.1.10<<, RemoteHost >>0.0.0.0<<
InternalPort >>21<<, ExternalPort >>21<<
PortMapProtocol >>TCP<<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
Ftp Example [MICROSOFT]
((1))
InternalClient >>0.0.0.0<<, RemoteHost >>0.0.0.0<<
InternalPort >>0<<, ExternalPort >>0<<
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
```

```
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
0<<

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

Telnet Command: upnp service

This command can display the information of the UPnP service. UPnP service must be enabled first.

Example

```
> upnp on
UPNP start.

> upnp service
>>>>> SERVICE TABLE1 <<<<<
  serviceType urn:schemas-microsoft-com:service:OSInfo:1
  serviceId   urn:microsoft-com:serviceId:OSInfo1
  SCPDURL     /upnp/OSInfo.xml
  controlURL  /OSInfo1
  eventURL    /OSInfoEvent1
  UDN         uuid:774e9bbe-7386-4128-b627-001daa843464

>>>>> SERVICE TABLE2 <<<<<
  serviceType
urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1
  serviceId   urn:upnp-org:serviceId:WANCommonIFC1
  SCPDURL     /upnp/WComIFCX.xml
  controlURL  /upnp?control=WANCommonIFC1
  eventURL    /upnp?event=WANCommonIFC1
  UDN         uuid:2608d902-03e2-46a5-9968-4a54ca499148
.
.
.
```

Telnet Command: upnp subscribe

This command can show all UPnP services subscribed.

Example

```
> upnp on
UPNP start.
> upnp subscribe
Vigor> upnp subscribe
>>>> (1) serviceType urn:schemas-microsoft-com:service:OSInfo:1

  ----- Subscribtion1 -------

    sid = 7a2bbdd0-0047-4fc8-b870-4597b34da7fb

    eventKey =1, ToSendEventKey = 1
```

```
    expireTime =6926

    active =1

    DeliveryURLs
=<http://192.168.1.113:2869/upnp/eventing/twtnpnsiun>

>>>> (2) serviceType
urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1

  ----- Subscribtion1 -------

    sid = d9cd47a5-d9c9-4d3d-8043-d03a82f27983

    eventKey =1, ToSendEventKey = 1
.
.
.
```

Telnet Command: upnp tmpvs

This command can display current status of temp Virtual Server of your router.

Example

```
Vigor> upnp tmpvs
******************  Temp virtual server status  ****************

((0))
real_addr  >>192.168.1.10<<, pseudo_addr >>172.16.3.229<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>TCP<<
time >>0<<

((1))
real_addr  >>0.0.0.0<<, pseudo_addr >>0.0.0.0<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>0<<
time >>0<<
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
```

Telnet Command: upnp wan

This command is used to specify WAN interface to apply UPnP.

upnp wan *[n]*

Syntax Description

Parameter	Description
n	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 cfgip

This command allows users to transfer a bridge modem into ADSL router by accessing into and adjusting specified IP address. Users can access into Web UI of the router to manage the router through the IP address configured here.

vigbrg cfgip *[IP Address]*

Syntax Description

Parameter	Description
IP Address	It means to type an IP address for users to manage the router.

Example

```
> vigbrg cfgip 192.168.1.15
> vigbrg cfgip ?
% Vigor Bridge Config IP,
% Now: 192.168.1.15
```

Telnet Command: vigbrg wan1on

This command is used to enable the bridge WAN1 management.

Example

```
> vigbrg wan1on
%Enable Vigor Bridge Wan1 management!
```

Telnet Command: vigbrg wan1off

This command is used to disable the bridge WAN1 management.

Example

```
> vigbrg wan1off
%Disable Vigor Bridge Wan1 management!
```

Telnet Command: wan ppp_mru

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

wan ppp_mru *<WAN interface number> <MRU siz >*

Syntax Description

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

Example

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

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

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

Telnet Command: wan mtu

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

wan mtu *[value]*

Syntax Description

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

Example

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

Telnet Command: wan DF_check

This command allows you to enable or disable the function of DF (Don’t fragment)

wan DF_check *[on]*

wan DF_check *[off]*

Syntax Description

Parameter	Description
on/off	It means to enable or disable DF.

Example

```
> wan DF_check on
%DF bit check enable!
```

Telnet Command: wan disable

This command allows you to disable WAN connection.

Example

```
> wan disable WAN
%WAN disabled.
```

Telnet Command: wan enable

This command allows you to disable wan connection.

Example

```
> wan enable WAN
%WAN1 enabled.
```

Telnet Command: wan forward

This command allows you to enable or disable the function of WAN forwarding. The packets are allowed to be transmitted between different WANs.

wan forward *on/off*

Syntax Description

Parameter	Description
on/off	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.

wan vdsl *[show basic]*

wan vdsl*[fbk_mode]*

Syntax Description

Parameter	Description
Show basic	It means to display current VDSL status.
Fbk_mode	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 Ping a specified IP to detect the WAN connection (static IP or PPPoE mode).

wan detect *[wan1][on/off/always_on]*

wan detect *[wan1]***target** *[ip addr]*

wan detect *[wan1]***ttl** *[1-255]*

wan detect status

Syntax Description

Parameter	Description
on	It means to enable ping detection. The IP address of the target shall be set.
off	It means to enable ARP detection (default).
always_on	disable link detect, always connected(only support static IP)
target	It means to set the ping target.
ip addr	It means the IP address used for detection. Type an IP address in this field.
ttl	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.
status	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.

wan lb *[wan1/wan2] on*

wan lb *[wan1/wan2] off*

Syntax Description

Parameter	Description
wan1/wan2	It means to specify which WAN will be applied with load balance.
on	It means to make WAN1/WAN2 as the member of load balance.
off	It means to cancel WAN1/WAN2 as the member of load balance.

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 2~4.

wan mvlan *[pvc_no/status/save/enable/disable] [on/off/clear/tag tag_no] [service type/vlan priority] [px ...]*

Syntax Description

Parameter	Description
pvc_no	It means index number of PVC. There are 8 PVC (0, Channel-1, to 7, Channel-8) allowed to be configured. However, only 2 to 7 are available for configuration.
status	It means to display the whole Bridge status.
save	It means to save the configuration into flash of Vigor router.
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.
px	It means LAN port. Available setting number is from 2 to 4. Port number 1 is locked for NAT usage.

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 0 p2 p3 p4
 PVC  Bridge   p1   p2   Service Type    Tag      Priority
 ------------------------------------------------------------------
   7    ON     0    1       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.

wan multifno *[channel #] [WAN interface #]*

wan multifno *status*

Syntax Description

Parameter	Description
channel #	There are 4 (?) channels including VLAN and PVC. Available settings are: 1=Channel 1 3=Channel 3 4=Channel 4 5=Channel 5
WAN interface #	Type a number to indicate the WAN interface. *1=WAN1*
status	It means to display current bridge status.

Example

```
> wan multifno 5 1
% Configured channel 5 uplink to WAN1
> wan multifno status
% Channel 3 uplink ifno: 3
% Channel 4 uplink ifno: 3
% Channel 5 uplink ifno: 3
% Channel 6 uplink ifno: 3
% Channel 7 uplink ifno: 3
>
```

Telnet Command: wan vlan

This command allows you to tag packets on WAN VLAN with specified number.

wan vlan wan *[#]* **tag** *[value]*

wan vlan wan *[#] [enable|disable]*

wan vlan stat

Syntax Description

Parameter	Description
#	It means the number of WAN interface. 1: means WAN1 2: means WAN2.
value	It means the number to be tagged on packets. The range of the value is between 32 ~ 4095.
enable|disable	It means to enable or disable the WAN interface for VLAN.
stat	It means to display the table of WAN VLAN status.

Example

```
> > wan vlan stat
%Interface    Pri     Tag    Enabled
%=====================================
% WAN1 (ADSL)   0      0
% WAN1 (VDSL)   0      0
%WAN2         0      0
```