Dray Tek

Vigor3910 Series

Multi-WAN Security Router

USER'S GUIDE

V1.0

Vigor3910 Series
Multi-WAN Security Router

User's Guide

Copyrights

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

Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows, Windows 95, 98, Me, NT, 2000, XP, Vista, 7, 10 and Explorer are trademarks of Microsoft Corp.
- Apple and Mac OS are registered trademarks of Apple Inc.
- Other products may be trademarks or registered trademarks of their respective manufacturers.

Safety Instructions

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

Warranty

- We warrant to the original end user (purchaser) that the router will be free from any defects in workmanship or materials for a period of two (2) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary 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.

Be a Registered Owner

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

Firmware & Tools Updates

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

  http://www.DrayTek.com

Table of Contents

Part I Installation

Installation

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

I-1 Introduction

This is a generic International version of the user guide. Specification, compatibility and features vary by region. For specific user guides suitable for your region or product, please contact local distributor.

Vigor3910 Series, a broadband router, integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

By adopting hardware-based VPN platform and hardware encryption of AES/DES/3DES, the router increases the performance of VPN greatly and offers several protocols (such as IPSec/PPTP/L2TP) with up to **100** VPN tunnels.

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

Object-based firewall is flexible and allows your network be safe.
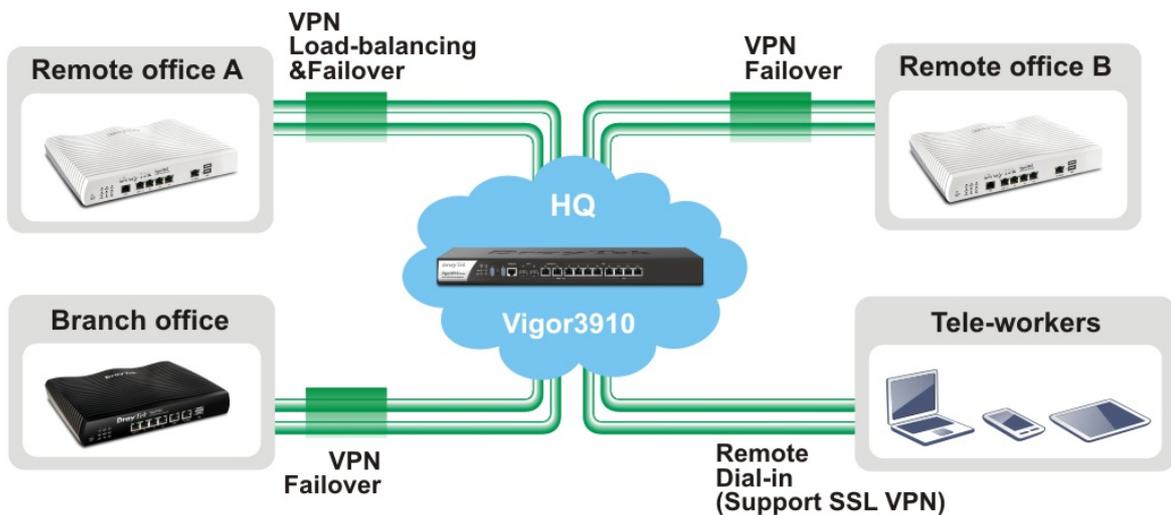
I-1-1 Indicators and Connectors

Before you use the Vigor router, please get acquainted with the LED indicators and connectors first.
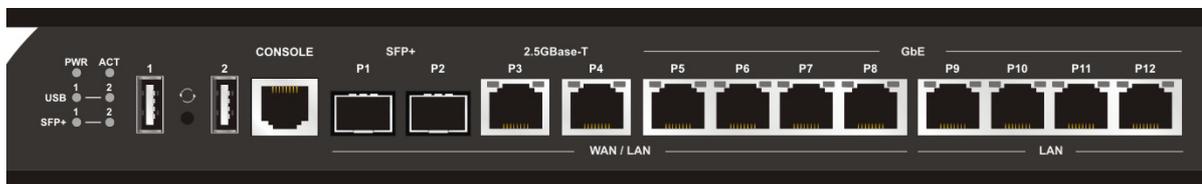
LED	Status	Explanation
PWR	On	The router is powered on.
	Off	The router is powered off.
ACT	Blinking	The system is active.
	Off	The system is hanged.
USB	On	The USB device is installed and ready.
	Off	No USB device is installed.
SFP+	On	The fiber connection is established.
	Blinking	The data is transmitting.
	Off	No fiber connection is established or the system is hanged.
P3~P12	On (Left)	The Ethernet link is established on corresponding port.
	Off (Left)	No Ethernet link is established.
	Blinking (L)	The data is transmitting.
	On (Right)	The Ethernet link is established on corresponding port with 1G Mbps or above.
	Off (Right)	The Ethernet link is established on corresponding port with less than 1G Mbps.

LED on Connector

DMZ	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps.
LAN	Left LED	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps
WAN1~WAN4	Left LED	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps

Interface	Description
USB1 / USB2	Connecter for the USB device.
Console	Provided for technician use.
SFP+ (P1~P2)	Connecter for SFP module with the rate of 10G/1G bps.
2.5GBase-T (P3~P4)	Connector for remote network devices or local network devices (WAN/LAN) with the rate of 2.5G/1G/100M/10M bps.
GbE P5~P8	Connectors for remote network devices or local network devices (WAN/LAN) with the rate of 1G/100M/10M bps.
GbE P9~P12	Connecter for local network devices (LAN) with the rate of 1G/100M/10M bps.
	The Factory Reset button is used to restore the default settings. Turn on the router (**ACT** LED is blinking). Press the hole and keep for more than 5 seconds. When you see the **ACT** LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
	Connecter for a power cord. ON/OFF - Power switch.

I-2 Hardware Installation

I-2-1 Installing Vigor Router

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

1. Connect a modem to any WAN port of Vigor3910 with Ethernet cable (RJ-45) to access Internet.

2. Connect the other end of the cable (RJ-45) to the Ethernet port on your computer (that device also can connect to other computers to form a small area network). The LAN LED for that port on the front panel will light up.

3. Connect a server/router (depends on your requirement) to any WAN port of Vigor3910 with Ethernet cable (RJ-45). The WAN LED will light up.

4. Connect the power cord to Vigor3910's power port on the rear panel, and the other side into a wall outlet.

5. Power on the device by pressing down the power switch on the rear panel. The PWR LED should be ON.

6. The system starts to initiate. After completing the system test, the ACT LED will light up and start blinking.

Below shows an outline of the hardware installation for your reference.
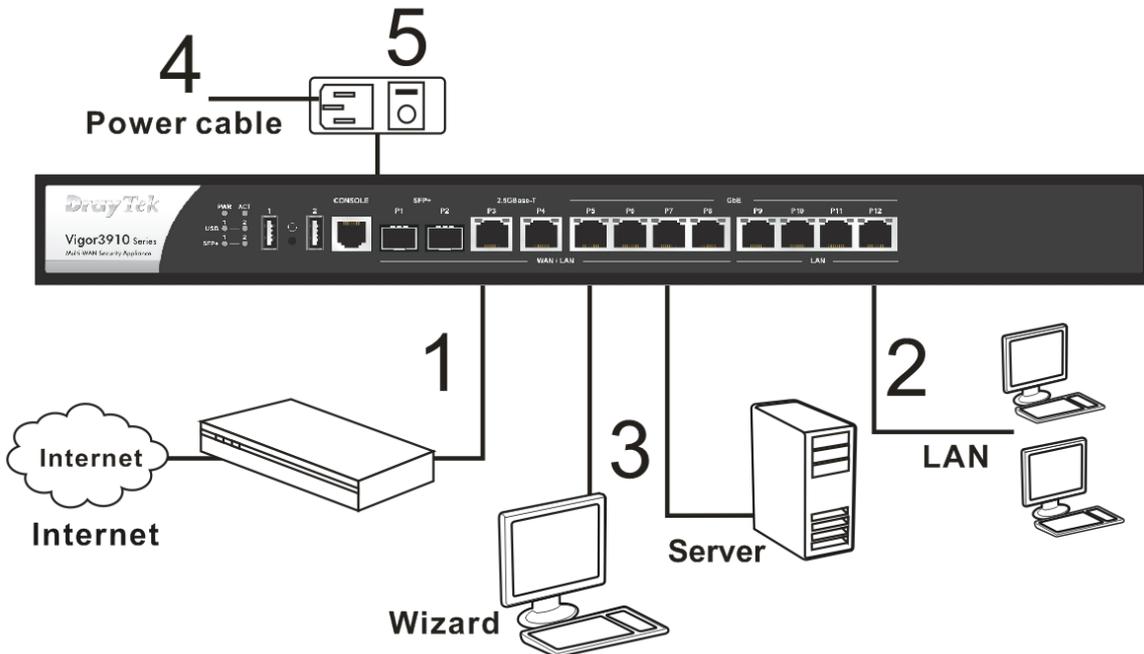
I-2-2 Rack-Mounted Installation

The Vigor3910 Series can be mounted on the wall by using standard brackets shown below.
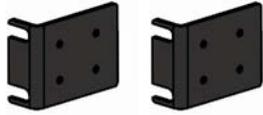
Attach the brackets to the chassis of a rack. The second bracket attaches the other side of the chassis.
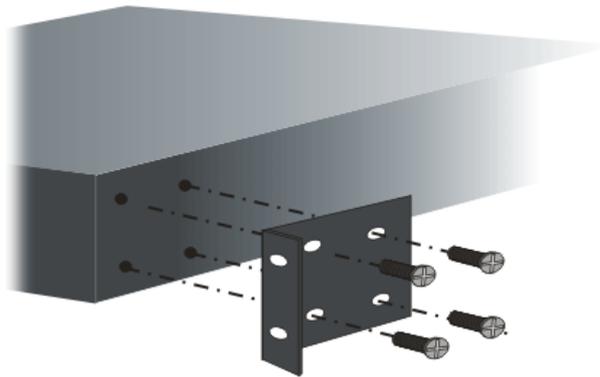
After the bracket installation, the Vigor3910 Series chassis can be installed in a rack by using four screws for each side of the rack.

Desktop Type Installation

Rubber pads are included with the Vigor3910 Series. These rubber pads improve the air circulation and decrease unnecessary rubbing on the desktop.

I-2-3 Installing USB Printer to Vigor Router

You can install a printer onto the router for sharing printing. All the PCs connected this router can print documents via the router. The example provided here is made based on Windows 7. For other Windows system, please visit **www.DrayTek.com**.
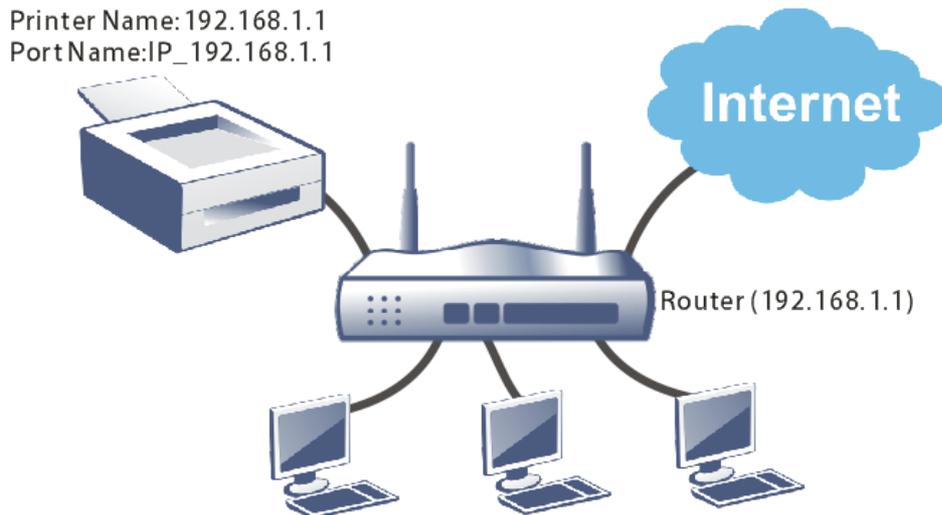
Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

1.   Connect the printer with the router through USB/parallel port.

2.   Open **All Programs>>Getting Started>>Devices and Printers**.
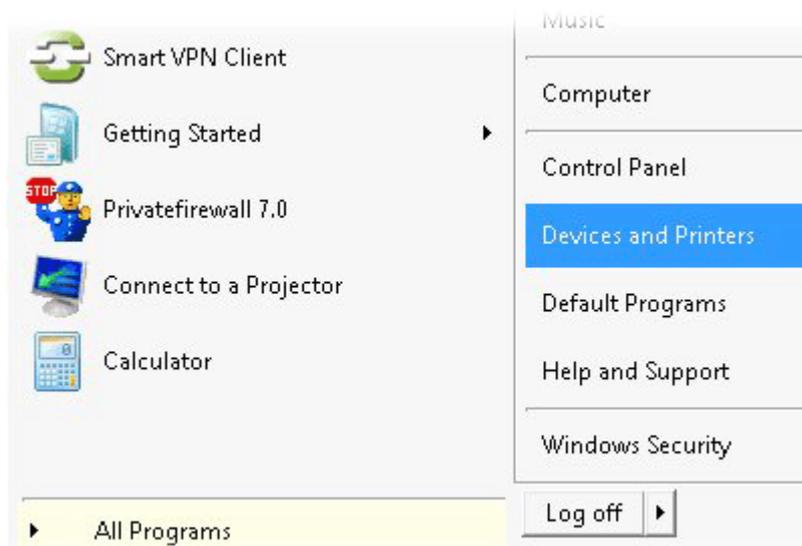
3.   Click **Add a printer**.

4. A dialog will appear. Click **Add a local printer** and click **Next**.
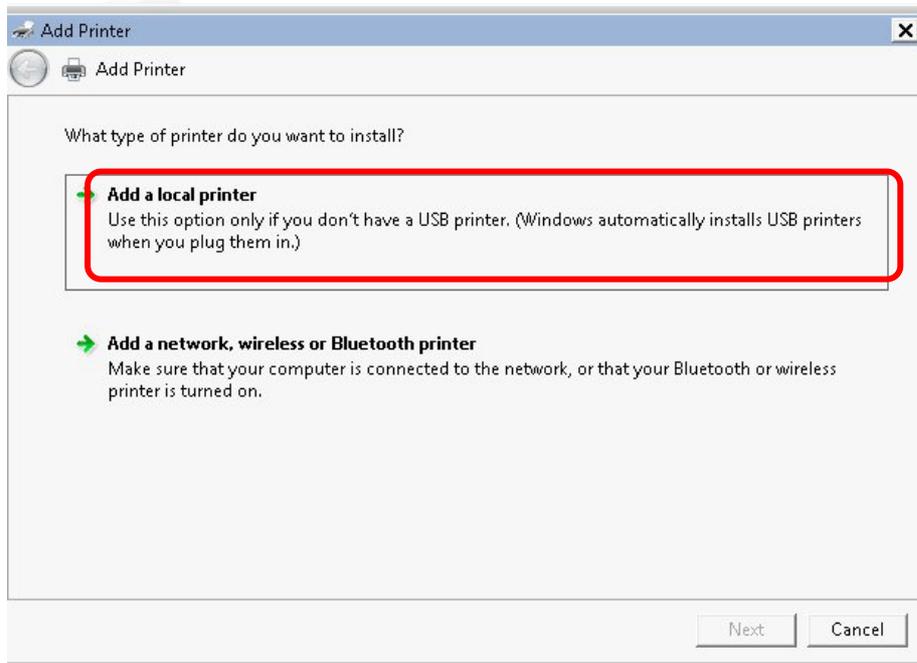
5. In this dialog, choose **Create a new port**. In the field of **Type of port**, use the drop down list to select **Standard TCP/IP Port**. Then, click **Next**.
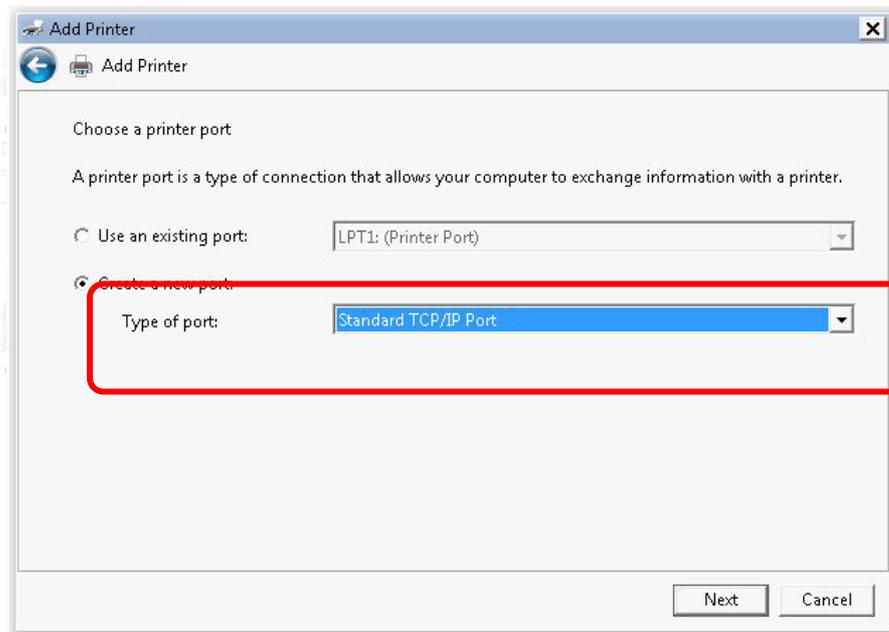
6. In the following dialog, type **192.168.1.1** (router's LAN IP) in the field of **Hostname or IP Address** and type **192.168.1.1** as the **Port name**. Then, click **Next**.

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

8. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.
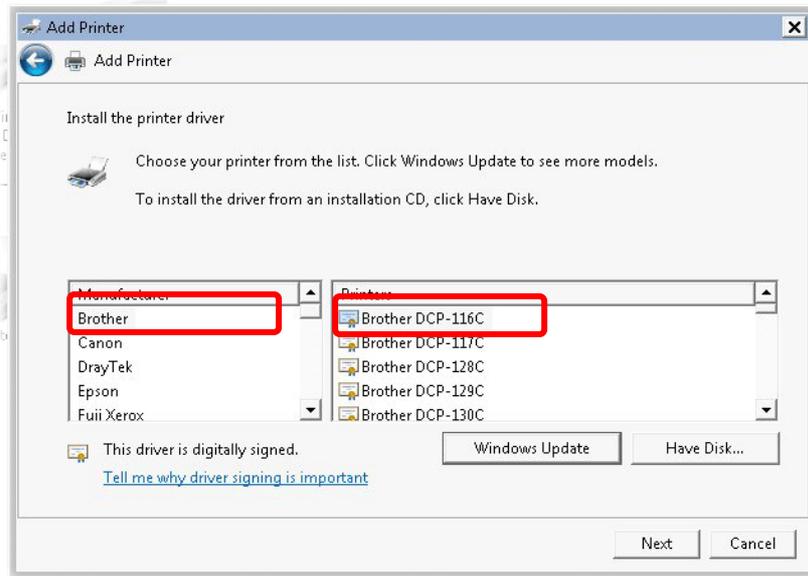
9. Type a name for the chosen printer. Click **Next.**
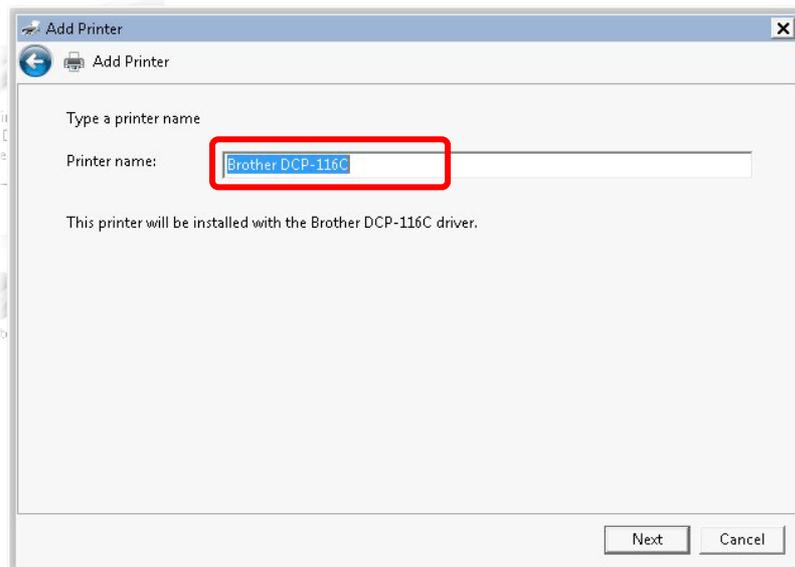
10. Choose **Do not share this printer** and click **Next**.
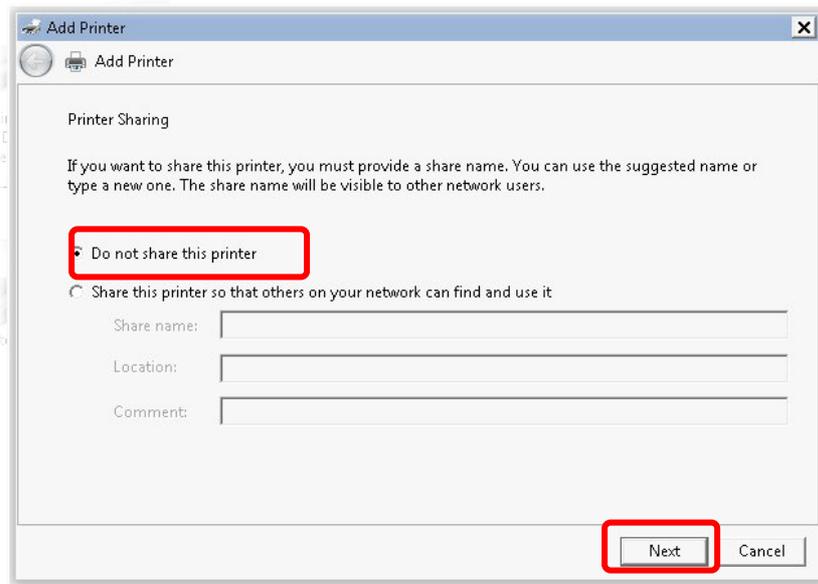
11. Then, in the following dialog, click **Finish**.
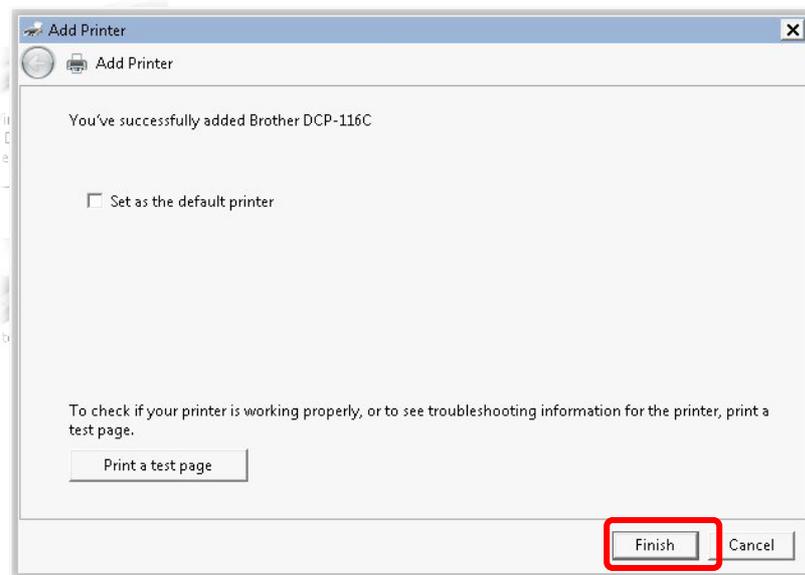
12. The new printer has been added and displayed under **Printers and Faxes**. Click the new printer icon and click **Printer server properties**.
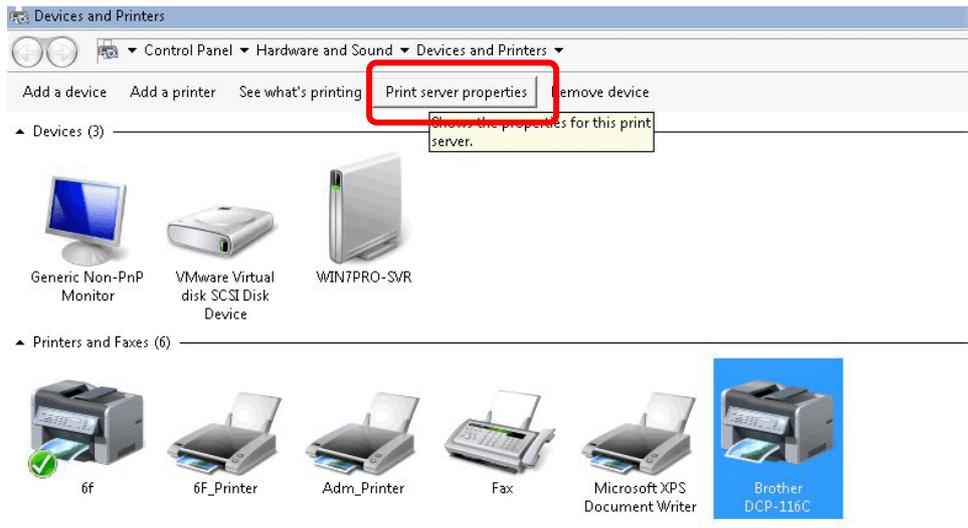
13. Edit the property of the new printer you have added by clicking **Configure Port**.
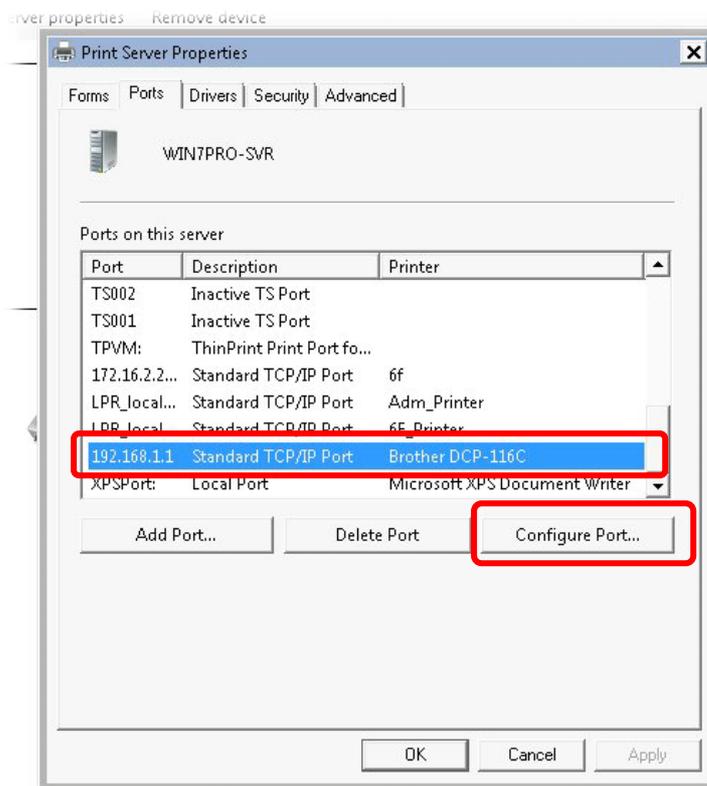
14. Select "**LPR**" on Protocol, type **p1** (number 1) as **Queue Name**. Then click **OK**. Next please refer to the red rectangle for choosing the correct protocol and LPR name.
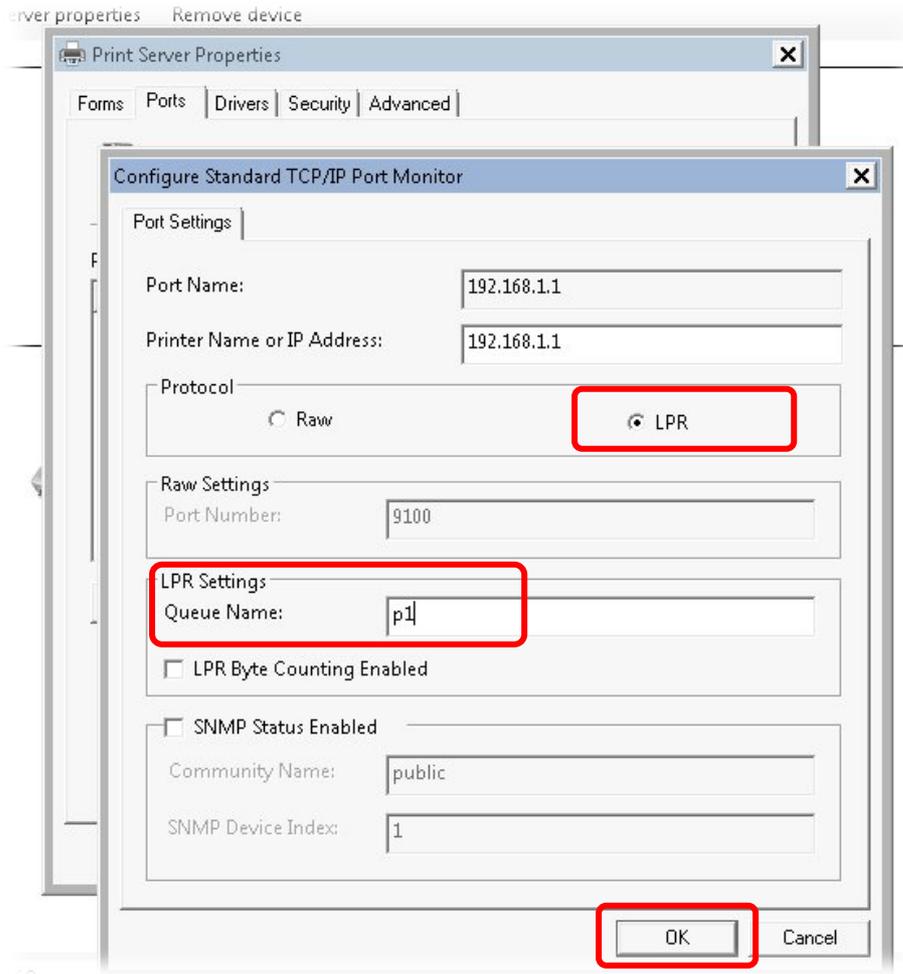
I-3 Accessing Web Page

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

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

2. Open a web browser on your PC and type **http://192.168.1.1**. The following window will be open to ask for username and password.
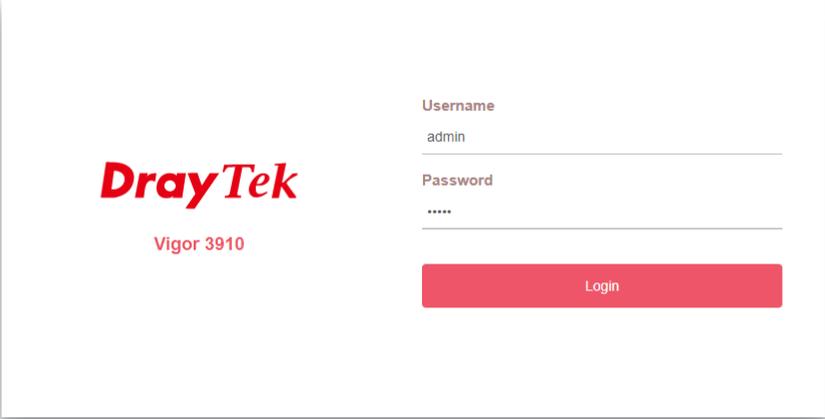
   Username
   admin

   Password
   •••••

   Login

   DrayTek

   Vigor 3910

   Copyright © 2000-2019DrayTek Corp. All Rights Reserved.

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

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

4. Now, the **Main Screen** will appear.
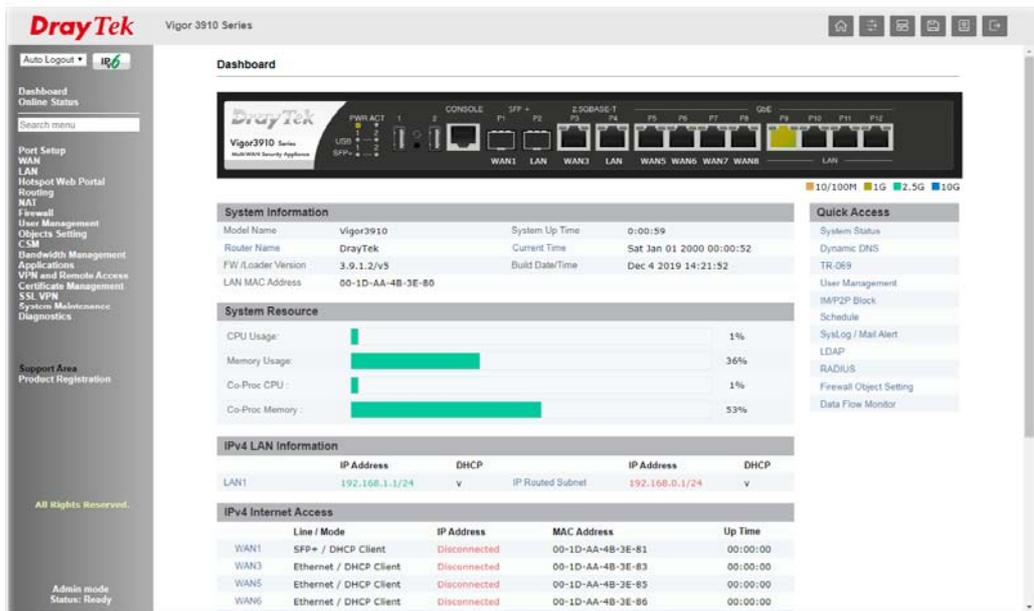
Info	The home page will be different slightly in accordance with the type of the router you have.

5. The web page can be logged out according to the chosen condition. The default setting is **Auto Logout**, which means the web configuration system will logout after 5 minutes without any operation. Change the setting for your necessity.
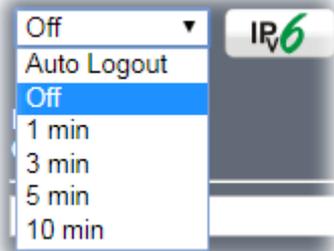
I-4 Changing Password

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

1. Open a web browser on your PC and type **http://192.168.1.1.** A pop-up window will open to ask for username and password.

2. Please type "admin/admin" as Username/Password for accessing into the web user interface with admin mode.

3. Go to **System Maintenance** page and choose **Administrator Password**.

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

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

5. Now, the password has been changed. Next time, use the new password to access the Web user interface for this router.
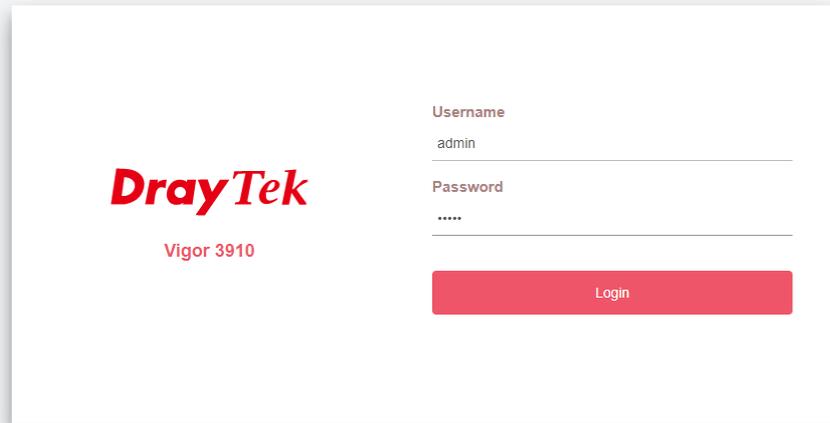
Copyright © 2000-2019DrayTek Corp. All Rights Reserved.

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

I-5 Dashboard

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

Click **Dashboard** from the main menu on the left side of the main page.
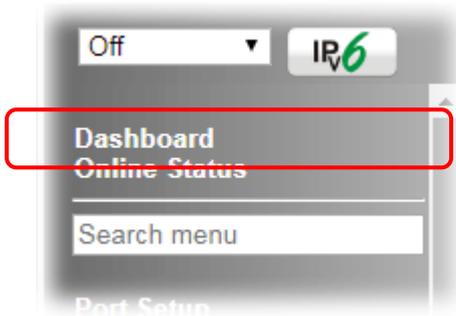
A web page with default selections will be displayed on the screen. Refer to the following figure:
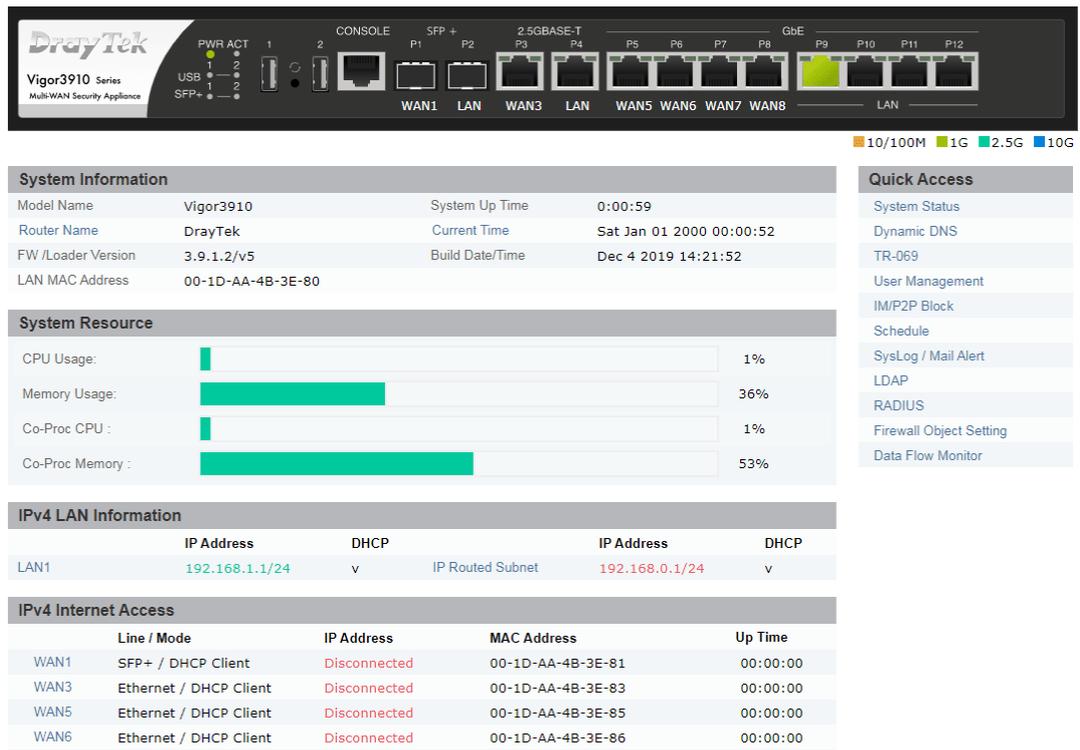
I-5-1 Virtual Panel

On the top of the Dashboard, a virtual panel (simulating the physical panel of the router) displays the physical interface connection. It will be refreshed every five seconds. When you move and click the mouse cursor on LAN, or WAN, related web setting page will be open for you to configure if required.
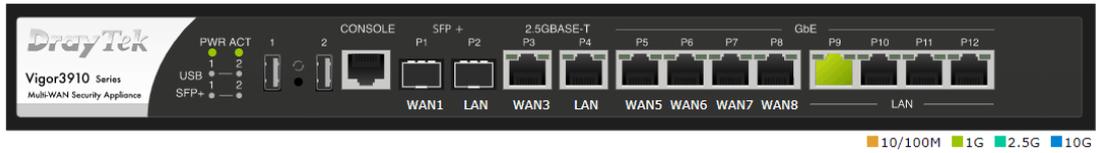
Port	Color	Description
LAN	Black	LAN port is disconnected.
	Orange	LAN port is connected at 10/100 Mbps.
	Green	LAN port is connected at 1 Gbps.
WAN	Black	WAN port is disconnected.
	Orange	WAN port is connected at 10/100 Mbps.
	Green	WAN port is connected at 1 Gbps.

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

I-5-2 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 DDNS, TR-069, User Management, IM/P2P Block, Schedule, Syslog/Mail Alert, LDAP, RADIUS, Firewall Object Setting and Data Flow Monitor are displayed here. Move your mouse cursor on any one of the items and click on it. The corresponding setting page will be open immediately.

Besides, LAN, IP Routed Subnet, WAN interfaces, VPN security settings such as Remote Dial-in User and LAN to LAN also can be accessed on this page easily. Scroll down the page to find them and move your mouse cursor on the item to open the configuration web page.

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

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

I-5-3 GUI Map

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

GUI Map

Dashboard		**Certificate Management**	
Online Status			Local Certificate
	Physical Connection		Trusted CA Certificate
	Virtual WAN		Certificate Backup
Port Setup			Self-Signed Certificate
WAN		**SSL VPN**	
	General Setup		General Setup
	Internet Access		User Account
	Multi-VLAN	**System Maintenance**	
LAN			System Status
	General Setup		TR-069
	VLAN		Administrator Password
	Bind IP to MAC		User Password
	PPPoE Server		Login Page Greeting
Hotspot Web Portal			Configuration Backup
	Profile Setup		Configuration Export
	Quota Management		SysLog / Mail Alert
Routing			Time and Date
	Static Route		SNMP
	Load-Balance/Route Policy		Management
	OSPF		Self-Signed Certificate
	BGP		Reboot System
NAT			Firmware Upgrade
	Port Redirection		Activation
	DMZ Host		Internal Service User List
	Open Ports		Dashboard Control
	Port Triggering	**Diagnostics**	
	ALG		Dial-out Triggering
Firewall			Routing Table
	General Setup		ARP Cache Table
	Filter Setup		IPv6 Neighbour Table
	Defense Setup		DHCP Table
	Diagnose		NAT Sessions Table

I-5-4 Web Console

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

Click the **Web Console** icon on the top of the main screen to open the following screen.
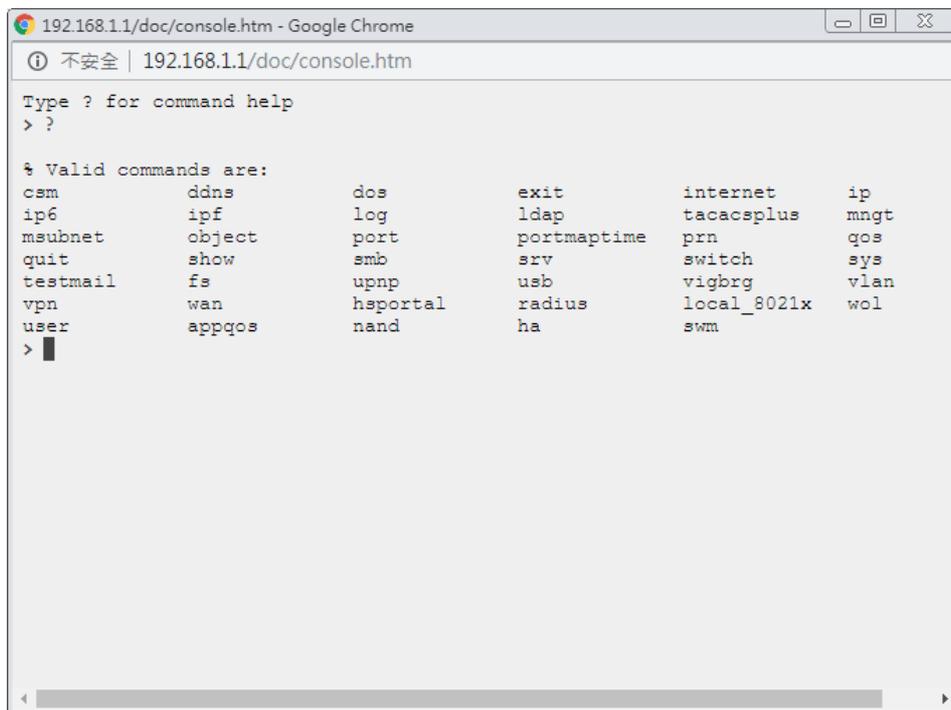
I-5-5 Config Backup
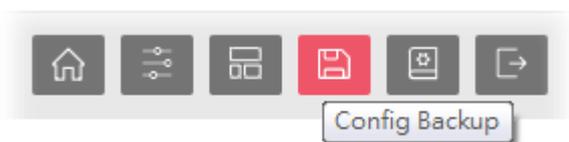
There is one way to store current used settings quickly by clicking the **Config Backup** icon. It allows you to backup current settings as a file. Such configuration file can be restored by using **System Maintenance>>Configuration Backup**.

Simply click the icon on the top of the main screen.

I-5-6 Manual Download
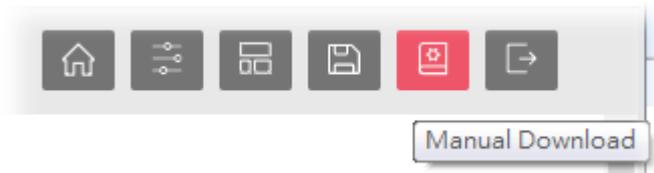
Click this icon to open online user's guide of Vigor router. This document offers detailed information for the settings on web user interface.

I-5-7 Logout
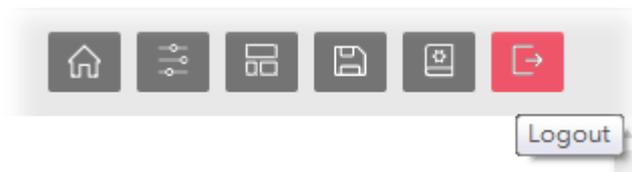
Click this icon to exit the web user interface.

I-5-8 Online Status

I-5-8-1 Physical Connection

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

Physical Connection for IPv4 Protocol

Physical Connection for IPv6 Protocol

Online Status

Physical Connection			System Uptime: 6days 7:14:46
IPv4		**IPv6**	

LAN Status
IP Address
FE80::21D:AAFF:FE4B:3E90/64 (Link)

TX Packets	RX Packets	TX Bytes	RX Bytes
2,360	1,288	184,088	113,150

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

WAN3 IPv6 Status
Enable	Mode	Up Time	
No	Offline	---	
IP			Gateway IP
---			---

WAN5 IPv6 Status
Enable	Mode	Up Time	
No	Offline	---	
IP			Gateway IP
---			---

WAN6 IPv6 Status
Enable	Mode	Up Time	
No	Offline	---	
IP			Gateway IP
---			---

WAN7 IPv6 Status
Enable	Mode	Up Time	
No	Offline	---	
IP			Gateway IP
---			---

WAN8 IPv6 Status
Enable	Mode	Up Time	
No	Offline	---	
IP			Gateway IP
---			---

Detailed explanation (for IPv4) is shown below:

Item	Description
LAN Status	**Primary DNS**-Displays the primary DNS server address for WAN interface.
	Secondary DNS -Displays the secondary DNS server address for WAN interface.
	IP Address-Displays the IP address of the LAN interface.
	TX Packets-Displays the total transmitted packets at the LAN interface.
	RX Packets-Displays the total received packets at the LAN interface.
WAN1 to WAN8 Status	**Enable – Yes** in red means such interface is available but not enabled. **Yes** in green means such interface is enabled.
	Line – Displays the physical connection (VDSL, ADSL, Ethernet, or USB) of this interface.
	Name – Display the name of the router.

Vigor3910 Series User's Guide

Item	Description
	Mode - Displays the type of WAN connection (e.g., PPPoE).
	Up Time - Displays the total uptime of the interface.
	IP - Displays the IP address of the WAN interface.
	GW IP - Displays the IP address of the default gateway.
	TX Packets - Displays the total transmitted packets at the WAN interface.
	TX Rate - Displays the speed of transmitted octets at the WAN interface.
	RX Packets - Displays the total number of received packets at the WAN interface.
	RX Rate - Displays the speed of received octets at the WAN interface.

Detailed explanation (for IPv6) is shown below:

Item	Description
LAN Status	**IP Address**- Displays the IPv6 address of the LAN interface..
	TX Packets-Displays the total transmitted packets at the LAN interface.
	RX Packets-Displays the total received packets at the LAN interface.
	TX Bytes - Displays the speed of transmitted octets at the LAN interface.
	RX Bytes - Displays the speed of received octets at the LAN interface.
WAN1 to WAN8 IPv6 Status	**Enable – No** in red means such interface is available but not enabled. **Yes** in green means such interface is enabled. No in red means such interface is not available.
	Mode - Displays the type of WAN connection (e.g., TSPC).
	Up Time - Displays the total uptime of the interface.
	IP - Displays the IP address of the WAN interface.
	Gateway IP - Displays the IP address of the default gateway.

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

I-5-8-2 Virtual WAN

Such page displays the virtual WAN connection information.

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

The field of Application will list i-9the purpose of such WAN connection.

I-6 Registering Vigor Router

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

1   Please login the web configuration interface of Vigor router by typing "**admin/admin**" as User Name / Password.
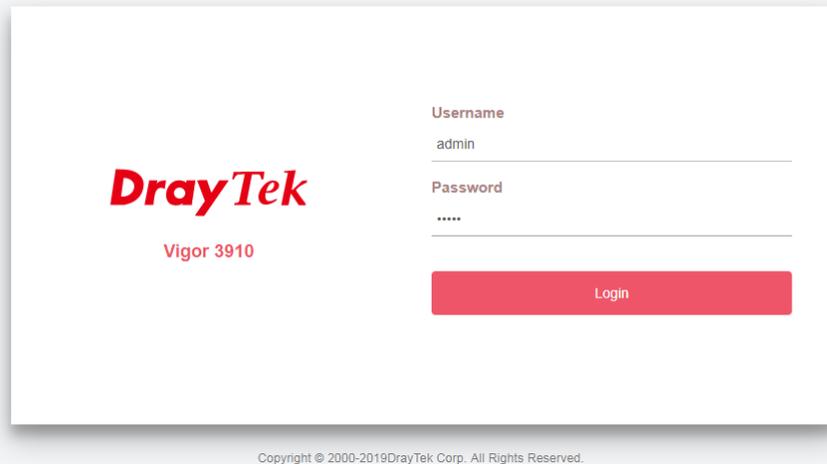
2   Click **Support Area>>Production Registration** from the home page.

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

Vigor3910 Series User's Guide
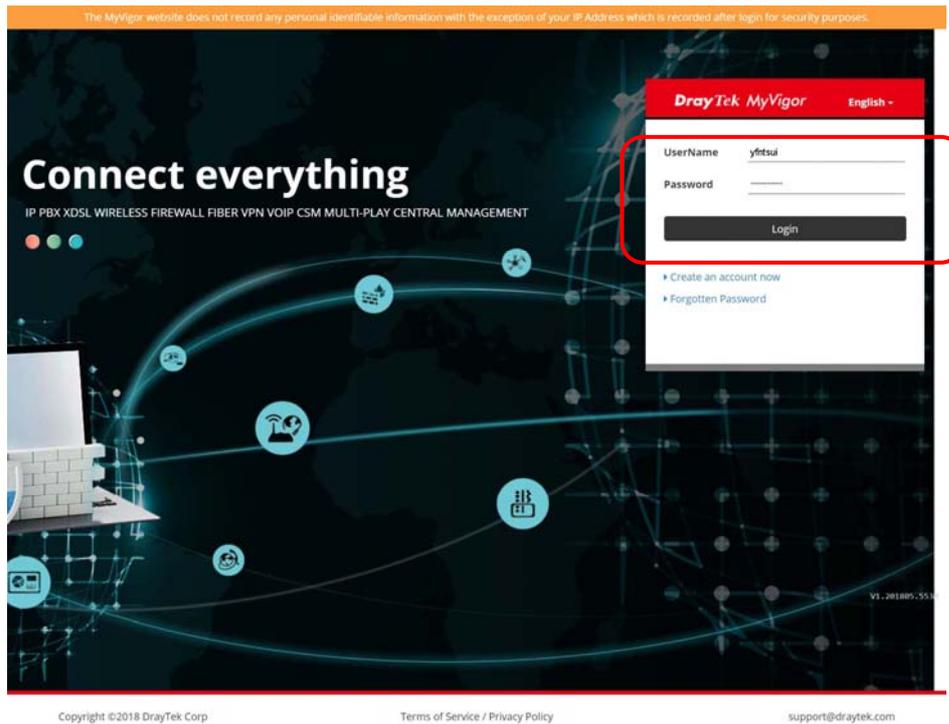
Info	If you haven't an accessing account, please refer to section Creating an Account for MyVigor to create your own one. Please read the articles on the Agreement regarding user rights carefully while creating a user account.

4   The following page will be displayed after you logging in MyVigor. Type a nickname for the router, then click **Add**.
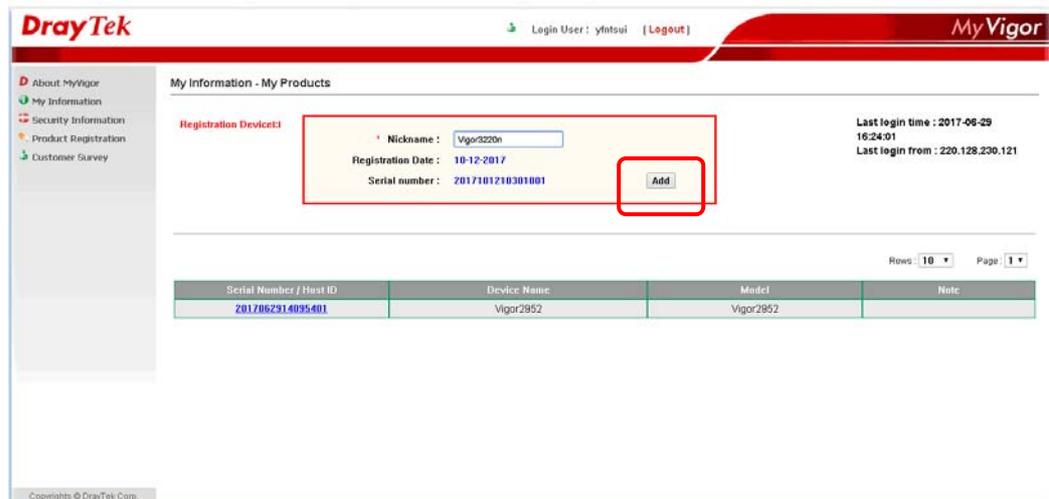
5   When the following page appears, your router information has been added to the database.

Your device has been successfully added to the database.

OK

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

Vigor3910 Series User's Guide

Part II Connectivity

WAN

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

LAN

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

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

NAT

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

Applications

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

Routing

Static Route, Load-Balance/Route Policy, OSPF, BGP

II-1 Port Setup

This page is used for configuring tranmission rate for LAN and WAN ports respectively.

Due to hardware restriction, the speed of P3 is the same as the speed of P4. So whenever P3 is changed, P4 is changed too and vice versa.

Available settings are explained as follows:

Item	Description
Port	Display the physical ports on Vigor router.
Function	P1 ~ P8 - These ports are switchable between WAN and LAN ports.
Speed	P1 ~ P2 - Available options include Auto, 10G and 1G. P3 ~ P4 - Available options include Auto and 2.5G. Due to the hardware limitation, the speed for P4 is the same as P3. P5 ~ P12- Available options include Auto, 1G, 100M, and 10 M.

II-2 WAN

It allows users to access Internet.

Basics of Internet Protocol (IP) Network

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

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

What are Public IP Address and Private IP Address

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

Get Your Public IP Address from ISP

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

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

Network Connection by 3G/4G USB Modem

For 3G/4G mobile communication through Access Point is popular more and more, Vigor3910 adds the function of 3G/4G network connection for such purpose. By connecting 3G/4G USB Modem to the USB port of Vigor3910, it can support LTE/HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G/4G standard (HSUPA, etc). Vigor3910n with 3G/4G USB Modem allows you to receive 3G/4G signals at any place such as your car or certain location holding outdoor activity and share the bandwidth for using by more people. Users can use LAN ports on the router to access Internet. Also, they can access Internet via 802.11(a/b/g/n/ac) wireless standard, and enjoy the powerful firewall, bandwidth management, and VPN features of Vigor3910n series.
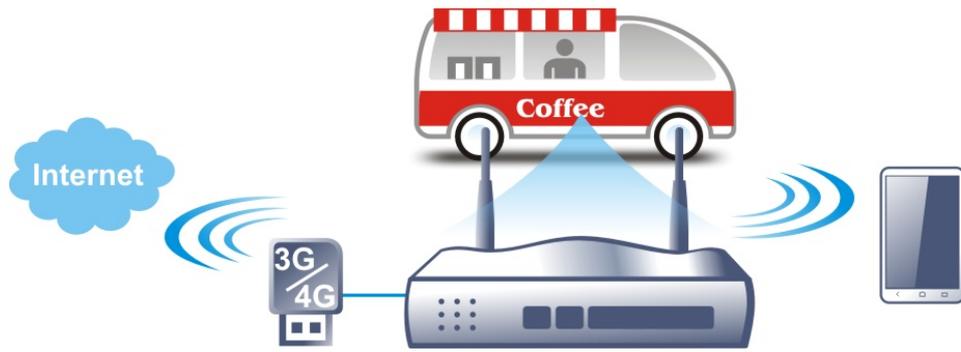
After connecting into the router, 3G/4G USB Modem will be regarded as the WAN3/WAN4 port. However, the original WAN1 and WAN2 still can be used and Load-Balance can be done in the router. Besides, 3G/4G USB Modem in WAN3/WAN4 also can be used as backup device. Therefore, when WAN1 and WAN2 are not available, the router will use 3.5G for supporting automatically. The supported 3G/4G USB Modem will be listed on DrayTek web site. Please visit www.draytek.com for more detailed information.

Web User Interface

II-2-1 General Setup

This section will introduce some general settings of Internet and explain the connection modes for WAN1~WAN8 in details.

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

This webpage allows you to set general setup for WAN# respectively.

Available settings are explained as follows:

Item	Description
Load Balance Mode	This option is available for multiple-WAN for getting enough bandwidth for each WAN port. If you know the practical bandwidth for your WAN interface, please choose the setting of **According to Line Speed**. Otherwise, please choose **Auto Weight** to let the router reach the best load balance. **IP Based** - The same source / destination IP pair will select the same WAN interface as policy. It is the default setting. **Session Based**- All of the WAN interfaces will be used (as out-going WAN) for passing through new sessions to get better transmission speed. Though good speed test result for throughput might be reached; however, some web site may not open smoothly, especially the site need authentication, e.g., FTP. If you have no strong demand about speed test result, keep default settings as IP based.
Index (WAN1 ~WAN8)	Click the WAN interface link under Index to access into the

	WAN configuration page.
Enable	Check the box to enable this WAN interface.
Physical Mode / Type / Port	Display the physical mode, physical type, and LAN port of this WAN interface.
Line Speed(Kbps) DownLink/UpLink	Display the downstream and upstream rate of this WAN interface.
Active Mode	Display whether this WAN interface is Active device or backup device. **Backup (WAN#)-** Display the backup WAN interface for this WAN when it is disabled.
Load Balance	**V** means the function of load balance for such WAN interface is enabled.

Info	In default, each WAN port is enabled.

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

To configure WAN interface settings, click the WAN# link to open the following page.

Available settings are explained as follows:

Item	Description
Enable	Choose **Yes** to invoke the settings for this WAN interface. Choose **No** to disable the settings for this WAN interface.
Display Name	Type the description for such WAN interface.
Physical Mode	Display the physical mode of such WAN interface.
Physical Type	You can change the physical type for WAN or choose **Auto**

	negotiation for determined by the system.
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 router will add specific VLAN number to all packets on the WAN while sending them out.
	Please type the tag value and specify the priority for the packets sending by WAN1.
	Disable – Disable the function of VLAN with tag.
	Tag value – Type the value as the VLAN ID number. The range is form 0 to 4095.
	Priority – Type the packet priority number for such VLAN. The range is from 0 to 7.
Active Mode	**Always On** - Choose **Always On** to make the WAN connection being activated always.
	Load Balance: Check this box to enable **auto** load balance function for this WAN interface.
	When the data traffic is large, the WAN interface with the function enabled will balance the data transmission automatically among all of the WAN interfaces in connection status.
	Failover – Choose it to make the WAN connection as a backup connection.
	● **WAN Failure** – When the active WAN failed, such WAN will be activated as the main network connection.
	● **Traffic Threshold** – When the data traffic of active WAN reaches the traffic threshold (specified here), the failover WAN will be enabled automatically to share the overloaded data traffic.
Active When	If you choose **Failover** as the **Active Mode**, the option of **Active When** will appear.
	● **Any of the selected WAN disconnect** – Such WAN connection will be activated when any selected WAN interface (checked below) disconnects.
	● **All of the selected WAN disconnect** – Such WAN connection will be activated only when all of selected WAN interfaces (checked below) disconnect.
	● **Check boxes for WAN1 to WAN5** – Specify the WAN interface by checking the WAN box.
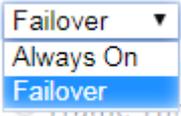
After finished the above settings, click **OK** to save the settings.

II-2-2 Internet Access

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

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode / Port	Access Mode		
WAN1		SFP+ / P1	Static or Dynamic IP ▼	Details Page	IPv6
WAN3		Ethernet / P3	Static or Dynamic IP ▼	Details Page	IPv6
WAN5		Ethernet / P5	Static or Dynamic IP ▼	Details Page	IPv6
WAN6		Ethernet / P6	Static or Dynamic IP ▼	Details Page	IPv6
WAN7		Ethernet / P7	Static or Dynamic IP ▼	Details Page	IPv6
WAN8		Ethernet / P8	Static or Dynamic IP ▼	Details Page	IPv6

[DHCP Client Option]

Available settings are explained as follows:

Item	Description
Index	Display the WAN interface.
Display Name	It shows the name of the WAN1 ~ WAN8 that entered in general setup.
Physical Mode / Port	It shows the physical connection for WAN(Ethernet) /port number according to the real network connection.
Access Mode	Use the drop down list to choose a proper access mode. The details page of that mode will be popped up. If not, click Details Page for accessing the page to configure the settings.
Details Page	This button will open different web page (based on IPv4) according to the access mode that you choose in WAN interface. Note that **Details Page** will be changed slightly based on physical mode.
IPv6	This button will open different web page (based on Physical Mode) to setup IPv6 Internet Access Mode for WAN interface. If IPv6 service is active on this WAN interface, the color of "IPv6" will become green.
DHCP Client Option	This button allows you to configure DHCP client options. DHCP packets can be processed by adding option number and data information when such function is enabled and configured.

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

Option number:100

Data: abcd

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

Interface – Specify the WAN interface(s) that will be overwritten by this function. WAN13 ~ WAN52 can be located under **WAN>>Multi-VLAN**.

Option Number – Type a number for such function.

DataType – Choose the type (ASCII or Hex) for the data to be stored.

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

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

II-2-2-1 Details Page for PPPoE in Etherenet WAN

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

WAN >> Internet Access

WAN 1

PPPoE	Static or Dynamic IP	IPv6

○ Enable   ⦿ Disable

ISP Access Setup

Username	Max: 63 characters
Password	Max: 62 characters

More Options ⊞

PPPoE Pass-through[1]

☐ For Wired LAN

WAN Connection Detection

Mode   `PPP Detect ▾`

MTU

`1492` (Max:1492)   `Path MTU Discovery`

PPP/MP Setup

PPP Authentication	`PAP or CHAP ▾`
Idle Timeout	`-1` second(s)
IP Assignment (IPCP)	○ Static ⦿ Dynamic
Fixed IP Address	

`WAN IP Alias`

Dial-Out Schedule

Index(1-15) in <u>Schedule</u> Setup:

`None ▾` => `None ▾`

=> `None ▾` => `None ▾`

TTL

☑ Change the TTL value

⦿ Default MAC Address

○ Use the following MAC Address

`00` : `1D` : `AA` : `21` : `28` : `59`

`OK`   `Cancel`

Note:

VPN feature may be affected when the value of MTU is changed, please also check your value of VPN mss by using "VPN mss set" command.

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

Available settings are explained as follows:

Item	Description
Enable/Disable	Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP.
	Username – Type in the username provided by ISP in this field.
	The maximum length of the user name you can set is 63 characters.
	Password – Type in the password provided by ISP in this field.
	The maximum length of the password you can set is 62 characters.
	More Options - It shows optional settings for configuration.
	● **Service Name** - Enter the description of the specific network service.
PPPoE Pass-through	The router offers PPPoE dial-up connection. Besides, you

	also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction. **For Wired LAN** – If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet. **Note**: To have PPPoA Pass-through, please choose PPPoA protocol and check the box(es) here. The router will behave like a modem which only serves the PPPoE client on the LAN. That's, the router will offer PPPoA dial-up connection.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. **Mode** – Choose **PPP Detect** or **Ping Detect** for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items. ● **Primary/Secondary Ping IP** – If you choose **Ping Detect** as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● **Ping Gateway IP** – If you choose **Ping Detect** as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● **TTL (Time to Live)** – Set TTL value of PING operation. ● **Ping Interval** – Type the interval for the system to execute the PING operation. ● **Ping Retry** – Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
MTU	It means Max Transmit Unit for packet. **Path MTU Discovery** – It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path. Click **Detect** to open the following dialog. N2Choose IP - Google Chrome 92.168.1.1/doc/pathmtu.htm Path MTU to: IPv4 Host ▾ MTU size start from 1500 (1000~1500) MTU reduce size by 8 (1~100) Detect **Note:** Path MTU discovery will reduce the MTU size for 3 times. Accept Cancel ● **Path MTU to** – Type the IP address as the specific transmit path. ● **MTU size start from** – Determine the starting point value of the packet. ● **MTU reduce size by**– It determines the decreasing size of MTU value. For example, the number specified in this field is "8". The maximum MTU size is "1500". After clicking the "detect" button, the system will

	calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically.
	● **Detect** – Click it to detect a suitable MTU value
	● **Accept**– After clicking it, the detected value will be displayed in the field of MTU.
PPP/MP Setup	**PPP Authentication** – Select **PAP only** or **PAP or CHAP** for PPP.
	Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action.
	IP Address Assignment Method (IPCP) - Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function.
	Fixed IP – Click **Yes** to use this function and type in a fixed IP address in the box of **Fixed IP Address**.
	WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 32 public IP addresses other than the current one you are using. Type the additional WAN IP address and check the Enable box. Then click **OK** to exit the dialog.
Dial-Out Schedule	You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application >> Schedule** web page and you can use the number that you have set in that web page.
TTL	**Change the TTL value** – Check the box to enable the TTL (Time to Live) for a packet transmitted through Vigor router.
	● **If enabled** - TTL value will be reduced (-1) when it passess through Vigor router. It will cause the client, accessing Internet through Vigor router, be blocked by certain ISP when TTL value becomes "0".
	● **If disabled** – TTL value will not be reduced. Then, when a packet passes through Vigor router, it will not be cancelled. That is, the client who sends out the packet will not be blocked by ISP.
	Default MAC Address – You can use **Default MAC Address** or specify another MAC address by typing on the boxes of MAC Address for the router.
	Specify a MAC Address – Type the MAC address for the router manually.

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

II-2-2-2 Details Page for Static or Dynamic IP in Etherenet WAN

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

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

WAN >> Internet Access

WAN 1

| PPPoE | Static or Dynamic IP | IPv6 |

◉ Enable   ○ Disable

IP Network Settings
◉ Obtain an IP address automatically
   More Options ⊞
○ Specify an IP address
   IP Address   [　　　]
   Subnet Mask   [　　　]
   Gateway IP Address   [　　　]
   [WAN IP Alias]

DNS Server IP Address
   Primary Server   8.8.8.8
   Secondary Server   8.8.4.4

WAN Connection Detection
   Mode   [ARP Detect ▼]

MTU
   [1500]   [Path MTU Discovery]

Keep WAN Connection
   ☐ Enable PING to keep alive
     PING to the IP   [　　　]
     PING Interval   [0] minute(s)

TTL
   ☑ Change the TTL value

RIP Routing
   ☐ Enable RIP

Bridge Mode
   ☐ Enable Bridge Mode
     Bridge Subnet   [LAN 1 ▼]

MAC Address
   ◉ Default MAC Address
   ○ Use the following MAC Address
     [00]:[1D]:[AA]:[21]:[28]:[59]

Note:
1. VPN feature may be affected when the value of MTU is changed, please also check your value of VPN mss by using "VPN mss set" command.
   We recommend to put the same decreased value on VPN mss. For example, reducing the MTU from 1500 -> 1400, then it will need to reduct 100 from mss value.
2. If enable firewall in bridge mode, IPv6 connection type would be change to DHCPv6 mode.
3. Bridge Subnet cannot be selected by Multi-WAN Interface at the same time.
4. If both Bridge Mode and Firewall are enabled, the settings under User Management will be ignored.

[OK] [Cancel]

Available settings are explained as follows:

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

IP Network Settings	This group allows you to obtain an IP address automatically and allows you type in IP address manually.
	Obtain an IP address automatically – Click this button to obtain the IP address automatically if you want to use **Dynamic IP** mode.
	More Options - It shows optional settings for configuration.
	● **Router Name**: Type in the router name provided by ISP.
	● **Domain Name**: Type in the domain name that you have assigned.
	● **Enable DHCP Client Identifier**: Check the box to specify username and password as the DHCP client identifier for some ISP.
	  - **Username**: Type a name as username. The maximum length of the user name you can set is 63 characters.
	  - **Password**: Type a password. The maximum length of the password you can set is 62 characters.

	Specify an IP address – Click this radio button to specify some data if you want to use **Static IP** mode.
	● **IP Address**: Type the IP address.
	● **Subnet Mask**: Type the subnet mask.
	● **Gateway IP Address**: Type the gateway IP address.
	WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 32 public IP addresses other than the current one you are using.
DNS Server IP Address	Type in the primary IP address for the router if you want to use **Static IP** mode. If necessary, type in secondary IP address for necessity in the future.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.
	Mode – Choose **ARP Detect**, **Ping Detect**, **Always On** or **Strict ARP Detect** for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items.
	● **Primary/Secondary Ping IP** – If you choose **Ping Detect** as detection mode, you have to type Primary or Secondary IP address in this field for pinging.
	● **Ping Gateway IP** – If you choose **Ping Detect** as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off.
	● **TTL (Time to Live)** – Set TTL value of PING operation.
	● **Ping Interval** – Type the interval for the system to execute the PING operation.
	● **Ping Retry** – Type the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
MTU	It means Max Transmit Unit for packet.
	Path MTU Discovery – It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path.
	Click **Detect** to open the following dialog.
	● **Path MTU to** – Type the IP address as the specific transmit path.
	● **MTU size start from** – Determine the starting point value of the packet. Default setting is 1500.
	● **MTU reduce size by**– It determines the decreasing size of MTU value. For example, the number specified in this field is "8". The maximum MTU size is "1500".

	After clicking the "detect" button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically.
	● **Detect** - Click it to detect a suitable MTU value
	● **Accept**- After clicking it, the detected value will be displayed in the field of MTU.
Keep WAN Connection	Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time. Check **Enable PING to keep alive** box to activate this function.
	PING to the IP - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive.
	PING Interval - Enter the interval for the system to execute the PING operation.
TTL	**Change the TTL value –** Check the box to enable the TTL (Time to Live) for a packet transmitted through Vigor router.
	● **If enabled** - TTL value will be reduced (-1) when it passess through Vigor router. It will cause the client, accessing Internet through Vigor router, be blocked by certain ISP when TTL value becomes "0".
	● **If disabled** – TTL value will not be reduced. Then, when a packet passes through Vigor router, it will not be cancelled. That is, the client who sends out the packet will not be blocked by ISP.
RIP Protocol	Routing Information Protocol is abbreviated as RIP（RFC1058）specifying how routers exchange routing tables information. Click **Enable RIP** for activating this function.
Bridge Mode	**Enable Bridge Mode** - If the function is enabled, the router will work as a bridge modem.
	● **Enable Firewall** – It is available when Bridge Mode is enabled. When both Bridge Mode and Firewall check boxes are enabled, the settings configured (user profiles) under User Management will be ignored. And all of the filter rules defined and enabled in Firewall menu will be activated.
	Bridge Subnet - Make a bridge between the selected LAN subnet and such WAN interface.
MAC Address	**Default MAC Address**: Click this radio button to use default MAC address for the router.
	Specify a MAC Address: Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the **Specify a MAC Address** and enter the MAC address in the MAC Address field.

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

II-2-2-3 Details Page for IPv6 – Offline in Ethernet WAN

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

II-2-2-4 Details Page for IPv6 – PPP in Ethernet WAN

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

No need to type any other information for PPP mode.

Available settings are explained as follows:

Item	Description
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. **Mode** – Choose **Always On** or **Ping Detect** for the system to execute for WAN detection. **Always On** means no detection will be executed. The network connection will be on always. ● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging.

Vigor3910 Series User's Guide

	TTL (Time to Live) –If you choose Ping Detect as detection mode, you have to type TTL value.
RIPng Protocol	RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.

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

Online Status

Physical Connection			System Uptime: 0:2:32
IPv4		IPv6	

LAN Status
IP Address
2001:B010:7300:201:21D:AAFF:FEA6:2568/64 (Global)
FE80::21D:AAFF:FEA6:2568/64 (Link)

TX Packets	RX Packets	TX Bytes	RX Bytes
7	4	690	328

WAN2 IPv6 Status   >> Drop PPP

Enable	Mode	Up Time	
Yes	PPP	0:02:08	

IP   **Gateway IP**
2001:B010:7300:201:21D:AAFF:FEA6:256A/128 (Global) FE80::90:1A00:242:AD52
FE80::1D:AAFF:FEA6:256A/128 (Link)

DNS IP
2001:B000:168::1
2001:B000:168::2

TX Packets	RX Packets	TX Bytes	RX Bytes
7	9	544	1126

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

II-2-2-5 Details Page for IPv6 – TSPC in Etherenet WAN

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

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

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

WAN >> Internet Access

WAN 1

PPPoE	Static or Dynamic IP	IPv6

Internet Access Mode
Connection Type   TSPC ▼

TSPC Configuration
Username   Max: 63 characters
Password   Max: 63 characters
Tunnel Broker

WAN Connection Detection
Mode   Ping Detect ▼
Ping IP/Hostname
TTL(1-255,0:Auto)   0

OK   Cancel

Available settings are explained as follows:

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

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

II-2-2-6 Details Page for IPv6 – AICCU in Ethernet WAN

Available settings are explained as follows:

Item	Description
Always On	Check this box to keep the network connection always.
Username	Type the name obtained from the broker. Please apply new account at http://www.sixxs.net/. It is suggested for you to apply another username and password.
	The maximum length of the name you can set is 19 characters.
Password	Type the password assigned with the user name.
	The maximum length of the password you can set is 19 characters.
Tunnel Broker	It means a server of AICCU. The server can provide IPv6 tunnels to sites or end users over IPv4.
	Type the address for the tunnel broker IP, FQDN or an optional port number.
Tunnel ID	One user account may have several tunnels. And, each tunnel shall have one specified tunnel ID (e.g., T115394).
	Type the ID offered by Tunnel Broker.
Subnet Prefix	Type the subnet prefix address obtained from service provider.
	The maximum length of the prefix you can set is 128 characters.

WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect.
	Mode - Choose **Always On** or **Ping Detect** for the system to execute for WAN detection.
	● **Ping IP/Hostname** - If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging.
	● **TTL (Time to Live)** –If you choose **Ping Detect** as detection mode, you have to type TTL value.

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

II-2-2-7 Details Page for IPv6 – DHCPv6 Client in Ethernet WAN

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

Available settings are explained as follows:

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

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

II-2-2-8 Details Page for IPv6 – Static IPv6 in Ethernet WAN

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. **Update** - Click it to modify an existed entry. **Delete –** Click it to remove an existed entry.
Current IPv6 Address Table	Display current interface IPv6 address.
Static IPv6 Gateway Configuration	**IPv6 Gateway Address** - Type your IPv6 gateway address here.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. **Mode –** Choose **Always On**, **NS Detect** or **Ping Detect** for the

	system to execute for WAN detection. **Always On** means no detection will be executed. The network connection will be on always.
	● **Ping IP/Hostname** - If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging.
	● **TTL (Time to Live)** –If you choose **Ping Detect** as detection mode, you have to type TTL value.
RIPng Protocol	RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.
Bridge Mode	**Enable Bridge Mode** - If the function is enabled, the router will work as a bridge modem.
	Enable Firewall – It is available when Bridge Mode is enabled. When both Bridge Mode and Firewall check boxes are enabled, the settings configured (user profiles) under User Management will be ignored. And all of the filter rules defined and enabled in Firewall menu will be activated.
	Bridge Subnet - Make a bridge between the selected LAN subnet and such WAN interface.

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

II-2-2-9 Details Page for IPv6 – 6in4 Static Tunnel in Ethernet WAN

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

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

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

Available settings are explained as follows:

Item	Description

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

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

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

Online Status

Physical Connection   System Uptime: 0day 0:4:16

IPv4	IPv6

LAN Status

IP Address

2001:4DD0:FF00:83E4:21D:AAFF:FE83:11B4/64 (Global)
FE80::21D:AAFF:FE83:11B4/64 (Link)

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

WAN1 IPv6 Status

Enable	**Mode**	**Up Time**	
Yes	6in4 Static Tunnel	0:04:07	

IP			**Gateway IP**

2001:4DD0:FF10:83E4::2131/64 (Global)   ---
FE80::C0A8:651D/128 (Link)

TX Packets	**RX Packets**	**TX Bytes**	**RX Bytes**
3	26	211	2302

II-2-2-10 Details Page for IPv6 – 6rd in Ethernet WAN

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.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. **Mode** - Choose **Always On** or **Ping Detect** for the system to execute for WAN detection. **Always On** means no detection will be executed. The network connection will be on always. ● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging. ● **TTL (Time to Live)** –If you choose **Ping Detect** as detection mode, you have to type TTL value.

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

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

Online Status

Physical Connection	System Uptime: 0day 0:9:15

IPv4	IPv6

LAN Status

IP Address

2001:E41:A865:1D00:21D:AAFF:FE83:11B4/64 (Global)
FE80::21D:AAFF:FE83:11B4/64 (Link)

TX Packets	RX Packets	TX Bytes	RX Bytes
15	113	1354	18040

WAN1 IPv6 Status

Enable	Mode	Up Time	
Yes	6rd	0:09:06	

IP			Gateway IP

2001:E41:A865:1D01:21D:AAFF:FE83:11B5/128
(Global)
FE80::C0A8:651D/128 (Link)   ---

TX Packets	RX Packets	TX Bytes	RX Bytes
13	29	967	2620

Vigor3910 Series User's Guide

II-2-3 Multi-VLAN

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

Channel 1 to 8 have the following fixed assignments and cannot be altered.

Channels 13 through 52 can be configured as virtual WANs.

General

The system allows you to set up to eight channels used as multi-VLAN.

Available settings are explained as follows:

Item	Description
Channel	Display the number of each channel. Channels 1~8 are used by the Internet Access web user interface and can not be configured here. Channels 13 ~ 52 are configurable.
Enable	Display whether the settings in this channel are enabled (checked) or not (unchecked).
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 (13~52) to get the following web page:

Available settings are explained as follows:

Item	Description
Enable Channel 13~52	Enable – Click it to enable the configuration of this channel. Disable –Click it to disable the configuration of this channel.
WAN Type	The connections and interfaces created in every channel may select a specific WAN type to be built upon. In the Multi-VLAN application, only the Ethernet WAN type is available. The user will be able to select the physical WAN interface the channel shall use here.
General Settings	VLAN Tag – Type the value as the VLAN ID number. Valid settings are in the range from 1 to 4095. The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value. Priority – Choose the number to determine the packet priority for such VLAN. The range is from 0 to 7.
Open 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/TR-069). If you choose Management, the configuration for this

	VLAN will be effective for Web configuration/telnet/TR-069.
	● **IPTV** - The IPTV configuration will allow the WAN interface to send IGMP packets to IPTV servers.
	WAN Setup - Choose **PPPoE/PPPoA** or **Static or Dynamic IP** as the protocol.
	Load Balance - Check the box to enable the load balance function for the selected channel.
ISP Access Setup	If **PPPoE/PPPoA** is selected, you have to configure the settings listed under **ISP Access Setup**. Enter your allocated username, password and authentication parameters according to the information provided by your ISP.
	● **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.
	ISP Address from ISP - Specifies how the WAN IP address of the channel configured.
	● **Fixed IP**
	➢ **Yes** - IP address entered in the Fixed IP Address field will be used as the IP address of the virtual WAN.
	➢ **No** - Virtual WAN IP address will be assigned by the ISP's PPPoE/PPPoA server.
WAN IP Network Settings	If **Static or Dynamic IP** is selected, you have to configure the settings listed under **WAN IP Network Settings**.
	● **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 necessary, type in secondary IP address for necessity in the future.

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

II-3 LAN

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

The most generic function of Vigor router is NAT. It creates a private subnet of your own. As mentioned previously, the router will talk to other public hosts on the Internet by using public IP address and talking to local hosts by using its private IP address. What NAT does is to translate the packets from public IP address to private IP address to forward the right packets to the right host and vice versa. Besides, Vigor router has a built-in DHCP server that assigns private IP address to each local host. See the following diagram for a briefly understanding.
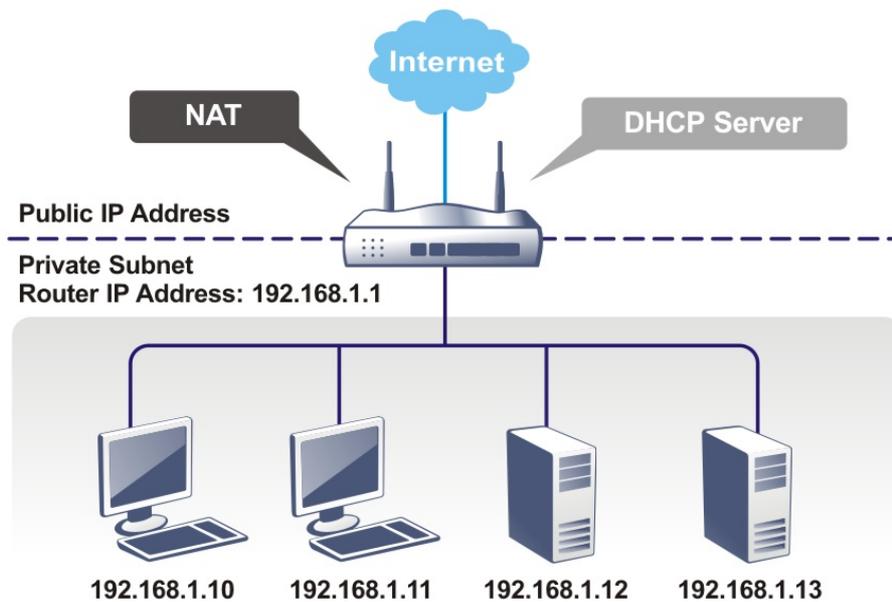
In some special case, you may have a public IP subnet from your ISP such as 220.135.240.0/24. This means that you can set up a public subnet or call second subnet that each host is equipped with a public IP address. As a part of the public subnet, the Vigor router will serve for IP routing to help hosts in the public subnet to communicate with other public hosts or servers outside. Therefore, the router should be set as the gateway for public hosts.
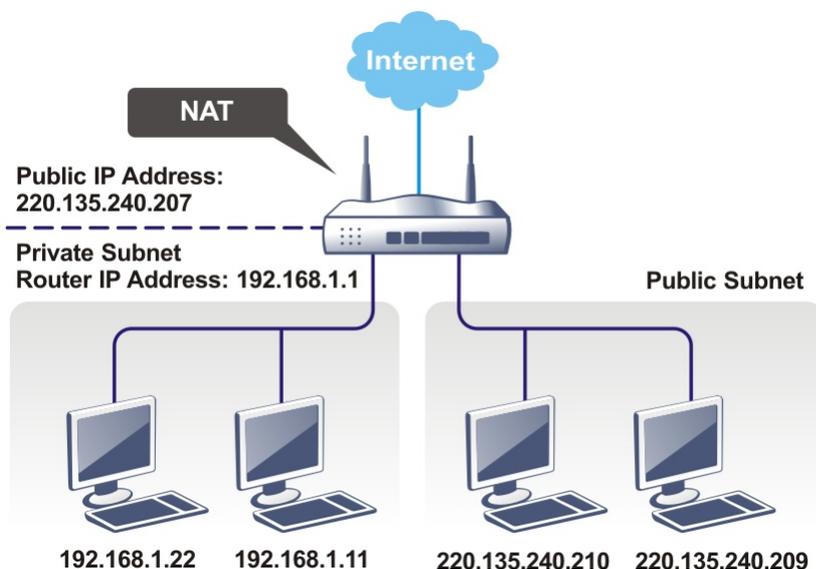
What is Routing Information Protocol (RIP)

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

What is Static Route

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

What are Virtual LANs and Rate Control

You can group local hosts by physical ports and create up to 8 virtual LANs. To manage the communication between different groups, please set up rules in Virtual LAN (VLAN) function and the rate of each.
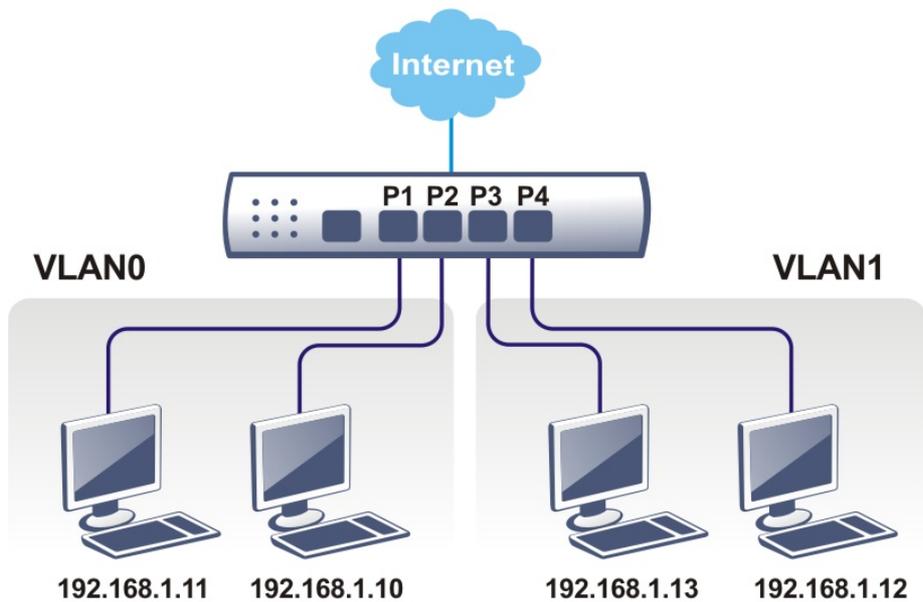
Web User Interface
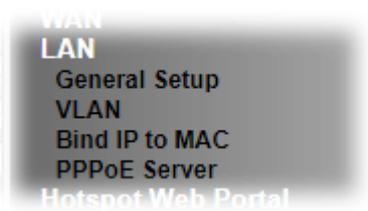
II-3-1 General Setup

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

There are several subnets provided by the router which allow users to divide groups into different subnets (LAN1 – LAN50). In addition, different subnets can link for each other by configuring **Inter-LAN Routing**. At present, LAN1 setting is fixed with NAT mode only. LAN2 – LAN50 can be operated under **NAT** or **Route** mode. IP Routed Subnet can be operated under Route mode.

Available settings are explained as follows:

Item	Description
General Setup	Allow to configure settings for each subnet respectively.
	Index - Display all of the LAN items.
	Enable - Basically, LAN1 status is enabled in default. LAN2 –LAN50 and IP Routed Subnet can be configured after enabling via LAN>>VLAN.
	DHCP- LAN1 is configured with DHCP in default. If required, please check the DHCP box for each LAN.
	IP Address - Display the IP address for each LAN item. Such information is set in default and you can not modify it.
	Details Page - Click it to access into the setting page. Each

	LAN will have different LAN configuration page. **Each LAN must be configured in different subnet.**
	IPv6 – Click it to access into the settings page of IPv6.
DHCP Server Options	DHCP packets can be processed by adding option number and data information when such function is enabled.
	For detailed information, refer to later section.
Force router to use "DNS Server IP address"…	Force Vigor router to use DNS servers configured in LAN port instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).
Inter-LAN Routing	Check the box to link two or more different subnets (LAN and LAN).
	Inter-LAN Routing allows different LAN subnets to be interconnected or isolated.
	It is only available when the VLAN functionality is enabled. Refer to section II-3-2 VLAN on how to set up VLANs.
	In the Inter-LAN Routing matrix, a selected checkbox means that the 2 intersecting LANs can communicate with each other.

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

Info	To configure a subnet, select its Detials Page button to bring up the LAN **Details Page**.

II-3-1-1 Details Page for LAN1 – Ethernet TCP/IP and DHCP Setup

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

LAN >> General Setup

LAN 1 Ethernet TCP / IP and DHCP Setup	LAN 1 IPv6 Setup
Network Configuration	**DHCP Server Configuration**
For NAT Usage	○ Disable ● Enable Server ○ Enable Relay Agent
IP Address `192.168.1.1`	Start IP Address `192.168.1.10`
Subnet Mask `255.255.255.0 / 24 ▼`	IP Pool Counts `200` (max. 1021)
[LAN IP Alias]	Gateway IP Address `192.168.1.1`
	Lease Time `86400` (s)
RIP Protocol Control `Disable ▼`	☑ Clear DHCP lease for inactive clients periodically
	DNS Server IP Address
	Primary IP Address
	Secondary IP Address

Note: Change IP Address or Subnet Mask in Network Configuration will also change <u>HA</u> LAN1 Virtual IP to the same domain IP.

[OK]

Available settings are explained as follows:

Item	Description
Network Configuration	For NAT Usage,

IP Address - This is the IP address of the router. (Default: 192.168.1.1).

Subnet Mask - The subnet mask, together with the IP Address field, indicates the maximum number of clients allowed on the subnet. (Default: 255.255.255.0/ 24).

LAN IP Alias –Such feature allows specifying multiple gateways (under a switch) with different WAN interfaces for accessing the Internet via the Vigor router.

RIP Protocol Control,

Enable –When Enabled, the router will attempt to exchange routing information with neighbouring routers using the Routing Information Protocol.

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

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

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

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

● **Start IP Address -** The beginning LAN IP address that is given out to LAN DHCP clients.

● **IP Pool Counts -** The maximum number of IP addresses to be handed out by DHCP. The default value is 200. Valid range is between 1 and 1021. The actual number of IP addresses available for assignment is the IP Pool Counts, or 1021 minus the last octet of the Start IP Address, whichever is smaller.

● **Gateway IP Address -** The IP address of the gateway,

	which is the host on the LAN that relays all traffic coming into and going out of the LAN. The gateway is normally the router, and therefore the Gateway IP Address should be identical to the IP Address in the **Network Configuration** section above.
	● **Lease Time** - The maximum duration DHCP-issued IP addresses can be used before they have to be renewed.
	● **Clear DHCP lease for inactive clients periodically -** If selected, the router sends ARP requests recycles IP addresses previously assigned to inactive DHCP clients to prevent exhaustion of the IP address pool.
	Note: When Clear DHCP lease for inactive clients periodically is enabled, router will do the following:
	■ Check activities of DHCP clients by ARP requests every minute when the available DHCP IP addresses are less than 30
	■ Clear DHCP lease when the client is not responding ARP replies.
	Enable Relay Agent – When selected, all DHCP requests are forwarded to a DHCP server outside of the LAN subnet, and whose address is specified in the DHCP Server IP Address field.
	● **DHCP Server IP Address –** It is available when **Enable Relay Agent** is checked. Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.
DNS Server IP Address	DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.
	Primary IP Address -You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server.
	Secondary IP Address - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server.
	The default DNS Server IP address can be found via Online Status:
	If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.
	If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable) connection.

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

Private IP addresses can be assigned automatically to LAN clients using Dynamic Host Configuration Protocol (DHCP), or manually assigned. The DHCP server can either be the

router (the most common case), or a separate server, that hands out IP addresses to DHCP clients.

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

II-3-1-2 Details Page for LAN1 – IPv6 Setup

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

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

Available settings are explained as follows:

Item	Description
Enable IPv6	Check the box to enable the configuration of LAN 1 IPv6 Setup.
WAN Primary Interface	Use the drop down list to specify a WAN interface for IPv6.
Static IPv6 Address	**IPv6 Address** –Type static IPv6 address for LAN. **Prefix Length** – Type the fixed value for prefix length. **Add** – Click it to add a new entry. **Delete** – Click it to remove an existed entry.
Unique Local Address (ULA) configuration	Unique Local Addresses (ULAs) are private IPv6 addresses assigned to LAN clients. **Off** - ULA is disabled. **Manually ULA Prefix** - LAN clients will be assigned ULAs generated based on the prefix manually entered. **Auto ULA Prefix** - LAN clients will be assigned ULAs using an automatically-determined prefix. Off ▼ Off Auto ULA Prefix Manually ULA Prefix
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.
Management	Configures the Managed Address Configuration flag (M-bit) in Route Advertisements. ● **Off** - No configuration information is sent using Route Advertisements. ● **SLAAC(stateless)** - M-bit is unset. ● **DHCPv6(stateful)** - M-bit is set, which indicates to LAN clients that they should acquire all IPv6 configuration information from a DHCPv6 server. The DHCPv6 server can either be the one built into the Vigor2860, or a separate DHCPv6 server. SLAAC(stateless) ▼ SLAAC(stateless) DHCPv6(stateful) Off
Other Option(O-bit)	When selected, the **Other Configuration** flag is set, which indicates to LAN clients that IPv6 configuration information besides LAN IPv6 addresses is available from a DHCPv6 server. Setting the M-bit (see **Management** above) has the same effect as implicitly setting the O-bit, as DHCPv6 supplies all IPv6 configuration information, including what is indicated as available when the O-bit is set.
DHCPv6 Server	**Enable Server** –Click it to enable DHCPv6 server. DHCPv6
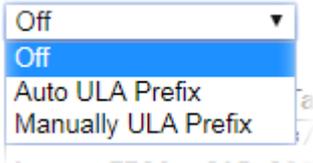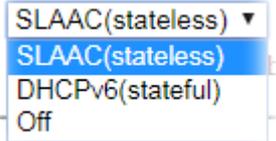
Configuration	Server could assign IPv6 address to PC according to the Start/End IPv6 address configuration. **Disable Server** –Click it to disable DHCPv6 server. **IPv6 Address Random Allocation –** After check the box, Vigor router will assign the IPv6 randamly to the client. **Auto IPv6 range -** After check the box, Vigor router will assign the IPv6 range automatically and sequencely to the client. ● **Start IPv6 Address / End IPv6 Address** –Type the start and end address for IPv6 server. ● **Advance setting** – Click the Edit button to configure advanced IPv6 settings for DHCPv6 server.
Advance setting	The Advanced Settings page has additional settings for Router Advertisement and enabling multiple WANs for IPv6 traffic. **Router Advertisement Server** – Click **Enable** to enable router advertisement server. The router advertisement daemon sends Router Advertisement messages, specified by RFC 2461, to a local Ethernet LAN periodically and when requested by a node sending a Router Solicitation message. These messages are required for IPv6 stateless auto-configuration.

Vigor3910 Series User's Guide   69

	Disable - Click it to disable router advertisement server.
	Hop Limt - The value is required for the device behind the router when IPv6 is in use.
	Min/Max Interval Time (sec) - It defines the interval (between minimum time and maximum time) for sending RA (Router Advertisement) packets.
	Default Lifetime (sec) -Within such period of time, Vigor router can be treated as the default gateway.
	Default Preference - It determines the priority of the host behind the router when RA (Router Advertisement) packets are transmitted.
	MTU - It means Max Transmit Unit for packet. If **Auto** is selected, the router will determine the MTU value for LAN.
	RIPng Protocol -RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.
	Extension WAN - In addition to the default WAN used for IPv6 traffic specified in the WAN Primary Interface in the LAN IPv6 Setup page, additional WANs can be selected to carry IPv6 traffic by enabling them in the Extension WAN section.
	Available WAN - Additional WANs available but not currently selected to carry IPv6 traffic.
	Selected WAN - Additional WANs selected to carry IPv6 traffic.

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

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

LAN >> General Setup

TCP/IP and DHCP Setup for IP Routed Subnet

Network Configuration
- ○ Enable ◉ Disable
- For Routing Usage
  - IP Address: 192.168.0.1
  - Subnet Mask: 255.255.255.0 / 24 ▼
- RIP Protocol Control: Disable ▼

DHCP Server Configuration
- Start IP Address: [   ]
- IP Pool Counts: 0 (max. 32)
- Lease Time: 259200 (s)
- ☐ Use LAN Port ☑ P11 ☑ P12
- ☑ Use MAC Address

Index	Matched MAC Address	given IP Address

MAC Address : [ ]:[ ]:[ ]:[ ]:[ ]:[ ]

[Add] [Delete] [Edit] [Cancel]

[OK]

Available settings are explained as follows:

Item	Description
Network Configuration	**Enable/Disable** - Click **Enable** to enable such configuration; click **Disable** to disable such configuration. **For Routing Usage,** **IP Address** - This is the IP address of the router. (Default: 192.168.1.1). **Subnet Mask -** The subnet mask, together with the IP Address field, indicates the maximum number of clients allowed on the subnet. (Default: 255.255.255.0/ 24). **RIP Protocol Control,** **Enable –** When Enabled, the router will attempt to exchange routing information with neighbouring routers using the Routing Information Protocol.
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network. If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location. **Start IP Address** - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254. **IP Pool Counts -** Enter the maximum number of PCs that you

	want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253. **Lease Time** - Enter the time to determine how long the IP address assigned by DHCP server can be used. **Use LAN Port –** Specify an IP for IP Route Subnet. If it is enabled, DHCP server will assign IP address automatically for the clients coming from P1. Please check the box of P1. **Use MAC Address -** Check such box to specify MAC address. **MAC Address:** Enter the MAC Address of the host one by one and click **Add** to create a list of hosts which can be assigned, deleted or edited from above pool. Set a list of MAC Address for 2nd DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2nd subnet won't get an IP address belonging to 1st subnet. **Add –** Type the MAC address in the boxes and click this button to add. **Delete** – Click it to delete the selected MAC address. **Edit** – Click it to edit the selected MAC address. **Cancel** – Click it to cancel the job of adding, deleting and editing.

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

II-3-1-4 DHCP Server Option

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

Available settings are explained as follows:

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

	system.
Enable	If selected, DHCP option entry is enabled.
	If unselected, DHCP option entry is disabled.
Interface	LAN interface(s) to which this entry is applicable.
Next Server IP Address/SIAddr	Overrides the DHCP Next Server IP address (DHCP Option 66) supplied by the DHCP server.
Option Number	DHCP option number (e.g., 100).
DataType	Type of data in the Data field:
	ASCII Character - A text string. Example: /path.
	Hexadecimal Digit - A hexadecimal string. Valid characters are from 0 to 9 and from a to f. Example: 2f70617468.
	Address List - One or more IPv4 addresses, delimited by commas.
Data	Data of this DHCP option.
Add	To add a DHCP option entry modeled after an existing entry, click the model entry in **Customized List**. The data entry fields will be populated with values from the model entry. After making all necessary changes for the new entry, click **Add** to create it.
Update	To modify an existing DHCP option entry, click on it in **Customized List**. The data entry fields will be populated with the current values from the entry. After making all necessary changes, click **Update** to save the changes.
Delete	To delete a DHCP option entry, click on it in **Customized List**, and then click **Delete**.
Reset	Clear the current settings.

II-3-2 VLAN

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

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

Tagged VLAN

The tagged VLANs (802.1q) can mark data with a VLAN identifier. This identifier can be carried through an onward Ethernet switch to specific ports. The specific VLAN clients can also pick up this identifier as it is just passed to the LAN. You can set the priorities for LAN-side QoS. You can assign each of VLANs to each of the different IP subnets that the router may also be operating, to provide even more isolation. The said functionality is **tag-based multi-subnet**.

LAN >> VLAN Configuration

VLAN Configuration

☐ Enable

	P2	P4	P9	P10	P11	P12	Subnet	Enable	VID	Priority
	LAN Port							**VLAN Tag**		
VLAN0	☐	☐	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN1	☐	☐	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN2	☐	☐	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN3	☐	☐	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN4	☐	☐	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN5	☐	☐	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN6	☐	☐	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN7	☐	☐	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN8	☐	☐	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN9	☐	☐	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN10	☐	☐	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN11	☐	☐	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN12	☐	☐	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN13	☐	☐	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN14	☐	☐	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN15	☐	☐	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN16	☐	☐	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN17							LAN 1 ▼		0	0 ▼

ⓘ

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

Available settings are explained as follows:

Item	Description
Enable	Click it to enable VLAN configuration.
LAN Port	Check the boxes to group them under the selected VLAN.

Subnet	Choose one of them to make the selected VLAN mapping to the specified subnet only. For example, LAN1 is specified for VLAN0. It means that PCs grouped under VLAN0 can get the IP address(es) that specified by the subnet.
VLAN Tag	**Enable** – Check the box to enable the function of VLAN with tag.
	The router will add specific VLAN number to all packets on the LAN while sending them out.
	Please type the tag value and specify the priority for the packets sending by LAN.
	VID – Type the value as the VLAN ID number. The range is form 0 to 4095. VIDs must be unique.
	Priority – Valid values are from 0 to 7, where 1 has the lowest priority, followed by 0, and finally from 2 to 7 in increasing order of priority.
Permit untagged device in P12 to access router	Select to allow untagged hosts connected to LAN port P12 to access the router. In case you have incorrectly configured VLAN functionality, you will still be able to access the router via the Web UI, and telnet and SSH shells to adjust the configuration.

The Vigor router supports up to 50 VLANs. Within the grid of VLANs (vertical columns) and LAN interfaces (horizontal rows), all hosts within the same VLAN (horizontal row) are visible to one another.

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

II-3-3 Bind IP to MAC

This function is used to bind the IP and MAC address in LAN to have a strengthening control in network. With the Bind IP to MAC feature you can reserve LAN IP addresses for LAN clients. Each reserved IP address is associated with a Media Access Control (MAC) address.

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

Available settings are explained as follows:

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

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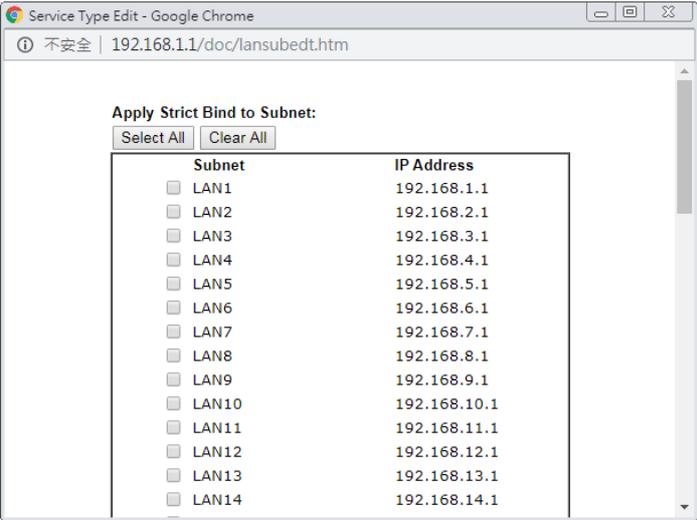
Upload From File	Click **Browse···** to select an IP Bind List backup file. Click **Restore** to restore the backup and overwrite the existing list.

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

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

II-3-4 PPPoE Server

LAN users can access into Internet through built-in PPPoE server on Vigor router. PPPoE server is a mechanism which can authenticate LAN users (configured in **User Management>>User Profile**) and prevent ARP attack completely.

LAN >> PPPoE Server

PPPoE Server

PPPoE Server:	⦿ Disable ◯ Enable
Primary DNS:	0.0.0.0
Secondary DNS:	0.0.0.0

OK

Available settings are explained as follows:

Item	Description
PPPoE Server	Enable – Activate the built-in PPPoE Server. Disable – Disable the built-in PPPoE Server.
Primary DNS / Secondary DNS	Type the IP address(es) of Primary /Secondary DNS server for PPPoE Client(s) in LAN.

II-4 NAT

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

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

The benefit of the NAT includes:

● **Save cost on applying public IP address and apply efficient usage of IP address.** NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.

● **Enhance security of the internal network by obscuring the IP address.** There are many attacks aiming victims based on the IP address. Since the attacker cannot be aware of any private IP addresses, the NAT function can protect the internal network.

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

Web User Interface

II-4-1 Port Redirection

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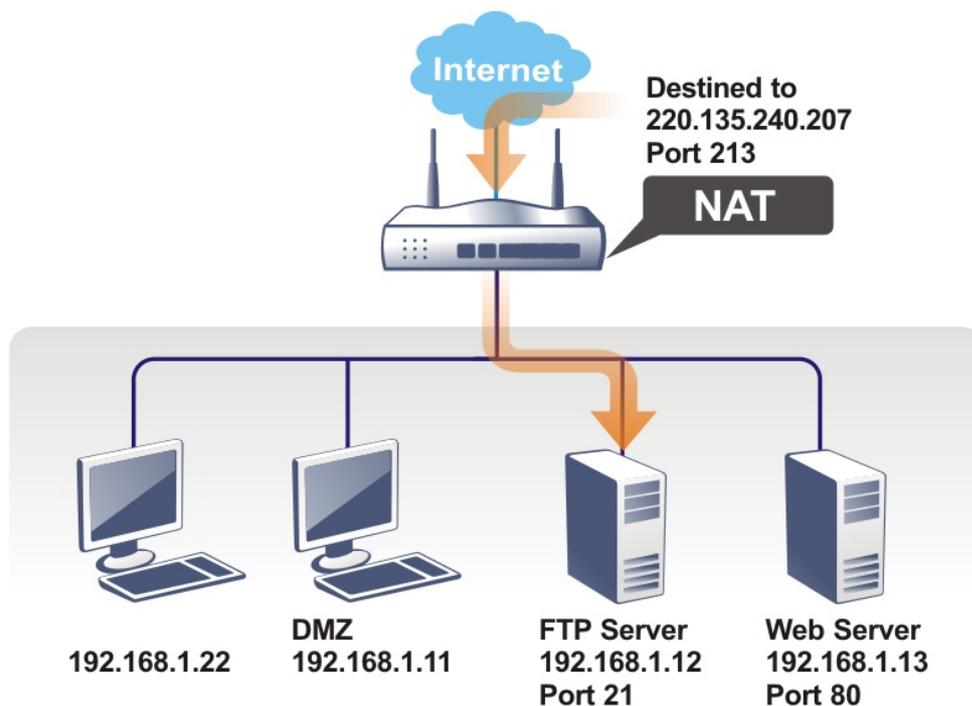
The port redirection can only apply to incoming traffic.

To use this function, please go to **NAT** page and choose **Port Redirection** web page. The **Port Redirection Table** provides 520 port-mapping entries for the internal hosts.

NAT >> Port Redirection

Port Redirection   50 ▼ rules per page | Set to Factory Default |

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

Each item is explained as follows:

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

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

NAT >> Port Redirection

Index No. 1

☐ Enable

Mode	Single ▼
Service Name	
Protocol	TCP ▼
WAN Interface	ALL ▼
Public Port	0
Source IP	IP Object ▼ None ▼
	Any
	IP Object
Private IP	IP Group
Private Port	

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

OK   Clear   Cancel

Available settings are explained as follows:

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

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

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

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

II-4-2 DMZ Host

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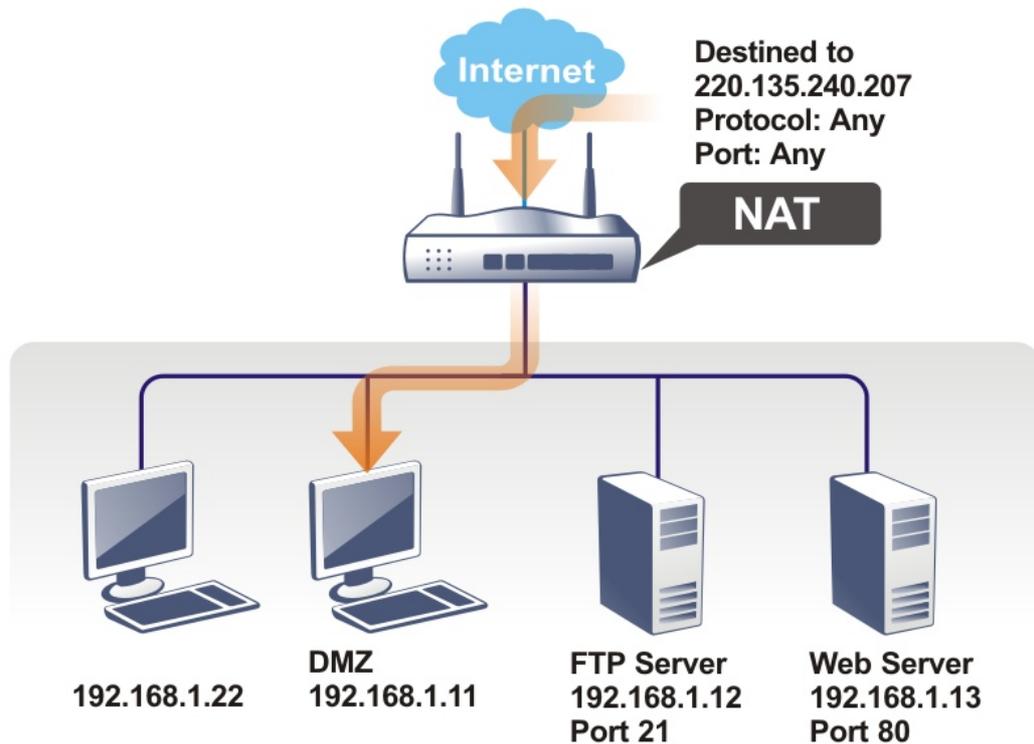
The security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

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

Available settings are explained as follows:

Item	Description
WAN 1 None ▼ None Private IP	Choose **Private IP** or **None** first.
Private IP	Enter the private IP address of the DMZ host, or click Choose PC to select one.
Choose IP	Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host. http://19... 192.168.1.10 192.168.1.18 When you have selected one private IP from the above dialog, the IP address will be shown on the screen. Click **OK** to save the setting.

DMZ Host for other WAN interface is slightly different with WAN1. **Active True IP** selection is available for WAN1 only.

See the following figure.

NAT >> DMZ Host Setup

DMZ Host Setup

WAN1	WAN3	WAN5	WAN6	WAN7	WAN8

WAN 3

Enable	Private IP	
☐	0.0.0.0	Choose IP

OK

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

NAT >> DMZ Host Setup

DMZ Host Setup

WAN1	WAN3	WAN5	WAN6	WAN7	WAN8

WAN 1

Index	Enable	Aux. WAN IP	Private IP	
1.	☐	---	0.0.0.0	Choose IP
2.	☐	192.168.1.56	0.0.0.0	Choose IP

OK   Clear

Available settings are explained as follows:

Item	Description
Enable	Check to enable the DMZ Host function.
Private IP	Enter the private IP address of the DMZ host, or click Choose PC to select one.
Choose IP	Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host. http://19... 192.168.1.10 192.168.1.18 When you have selected one private IP from the above dialog, the IP address will be shown on the screen. Click **OK** to save the setting.

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

II-4-3 Open Ports

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

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

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

NAT >> Open Ports

Open Ports Setup | Set to Factory Default |

Index	Enable	Comment	WAN Interface	Aux. WAN IP	Source IP	Local IP Address
1.	☐				Any	
2.	☐				Any	
3.	☐				Any	
4.	☐				Any	
5.	☐				Any	
6.	☐				Any	
7.	☐				Any	
8.	☐				Any	
9.	☐				Any	
10.	☐				Any	
11.	☐				Any	
12.	☐				Any	
13.	☐				Any	
14.	☐				Any	
15.	☐				Any	
16.	☐				Any	
17.	☐				Any	
18.	☐				Any	
19.	☐				Any	
20.	☐				Any	

<< 1-20 | 21-40 | 41-60 | 61-80 | 81-100 | 101-120 | 121-140 | 141-160 | 161-180 | 181-200 | 201-220 | 221-240 | 241-260 >>   Next >>

[OK]   [Cancel]

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 the box to enable the open port profile.
Comment	Specify the name for the defined network service.
WAN Interface	Display the WAN interface used by such index.
Aux. WAN IP	Display the IP alias setting used by such index. If no IP alias setting exists, such field will not appear.

Source IP	Display the source IP address.
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.

NAT >> Open Ports >> Edit Open Ports

Index No. 1

☑ Enable Open Ports

Comment: _____

WAN Interface: WAN1 ▼

WAN IP: 192.168.1.56 ▼

Source IP: IP Object ▼ None ▼
 Any
 IP Object
 IP Group

Private IP: _____ Choose IP

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

OK   Clear   Cancel

Available settings are explained as follows:

Item	Description
Enable Open Ports	Check to enable this entry.
Comment	Make a name for the defined network application/service.
WAN Interface	Specify the WAN interface that will be used for this entry.
WAN IP	Specify the WAN IP address that will be used for this entry. This setting is available when WAN IP Alias is configured.
Source IP	Use the drop down list to specify an IP object. Or click IP Object link to create a new one for applying.
Private IP	Enter the private IP address of the local host or click **Choose PC** to select one. **Choose IP -** Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select the appropriate IP address of the local host in the list.
Protocol	Specify the transport layer protocol. It could be **TCP**, **UDP**, or ----- (none) for selection.
Start Port	Specify the starting port number of the service offered by the local host.
End Port	Specify the ending port number of the service offered by the local host.

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

NAT >> Open Ports

Open Ports Setup | Set to Factory Default |

Index	Enable	Comment	WAN Interface	Aux. WAN IP	Source IP	Local IP Address
1.	☑	Swtich	WAN1	192.168.1.56	Any	192.168.1.10
2.	☐				Any	
3.	☐				Any	
4.	☐				Any	
5.	☐				Any	
6.	☐				Any	
7.	☐				Any	
8.	☐				Any	

II-4-4 Port Triggering

Port Triggering is a variation of open ports function.

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

● Once the OK button is clicked and the configuration has taken effect, "open port" keeps the ports opened forever.

● Once the OK button is clicked and the configuration has taken effect, "port triggering" will only attempt to open the ports once the triggering conditions are met.

● The duration that these ports are opened depends on the type of protocol used. The "default" durations are shown below and these duration values can be modified via telnet commands.

TCP: 86400 sec.

UDP: 180 sec.

IGMP: 10 sec.

TCP WWW: 60 sec.

TCP SYN: 60 sec.

NAT >> Port Triggering

Port Triggering | Set to Factory Default |

Index	Enable	Comment	Triggering Protocol	Source IP	Triggering Port	Incoming Protocol	Incoming Port
1.	☐			Any			
2.	☐			Any			
3.	☐			Any			
4.	☐			Any			
5.	☐			Any			
6.	☐			Any			
7.	☐			Any			
8.	☐			Any			
9.	☐			Any			
10.	☐			Any			
11.	☐			Any			
12.	☐			Any			
13.	☐			Any			
14.	☐			Any			
15.	☐			Any			
16.	☐			Any			
17.	☐			Any			
18.	☐			Any			
19.	☐			Any			
20.	☐			Any			

<< 1-20 | 21-40 >>   Next >>

OK   Cancel

Available settings are explained as follows:

Item	Description
Index	Indicate the relative number for the port triggering profile. You should click the appropriate index number to edit or clear the corresponding entry.
Enable	Check the box to enable the Port Triggering profile.
Comment	Display the text which memorizes the application of this rule.
Triggering Protocol	Display the protocol of the triggering packets.
Source IP	Display the source IP address.
Triggering Port	Display the port of the triggering packets.
Incoming Protocol	Display the protocol for the incoming data of such triggering profile.
Incoming Port	Display the port for the incoming data of such triggering profile.

Click the index number link to open the configuration page.

NAT >> Port Triggering

No. 1

☐ Enable

Service	User Defined ▾
Comment	
Source IP	IP Object ▾ None ▾
Triggering Protocol	--- ▾
Triggering Port	
Incoming Protocol	--- ▾
Incoming Port	

--- (dropdown open)
TCP
UDP
TCP/UDP

Note:
The Triggering Port and Inc[ ] should be input like this :
123-456,777-789 (legal),123-456,789 (legal), but 123-456-789 (illegal).

[OK] [Clear] [Cancel]

Available settings are explained as follows:

Item	Description
Enable	Check to enable this entry.
Service	Choose the **predefined** service to apply for such trigger profile.
Comment	Type the text to memorize the application of this rule.
Source IP	Select any IP address, IP object or IP group as the source IP.
Triggering Protocol	Select the protocol (TCP, UDP or TCP/UDP) for such triggering profile.
Triggering Port	Type the port or port range for such triggering profile.
Incoming Protocol	When the triggering packets received, it is expected the incoming packets will use the selected protocol. Select the protocol (TCP, UDP or TCP/UDP) for the incoming data of such triggering profile.
Incoming Port	Type the port or port range for the incoming packets.

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

II-4-5 ALG

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

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

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

NAT >> ALG

ALG (Application Layer Gateway) | Set to Factory Default |

☑ Enable ALG

☐ Enable	Protocol	Listen Port		TCP	UDP
☐	SIP	5060	(1~65535)	☑	☑
☐	RTSP	554	(1~65535)	☑	☑

OK

Available settings are explained as follows:

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

II-5 Applications

Dynamic DNS

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

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

LAN DNS / DNS Forwarding

The LAN DNS lets the network administrators host servers with privacy and security. When the network administrators of your office set up FTP, Mail or Web server inside LAN, you can specify specific private IP address (es) to correspondent servers. Thus, even the remote PC is adopting public DNS as the DNS server, the LAN DNS resolution on Vigor3910 Series will respond the specified private IP address.

Schedule

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

RADIUS/TACACS+

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

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

LDAP /Active Directory Setup

Lightweight Directory Access Protocol (LDAP) is a communication protocol for using in TCP/IP network. It defines the methods to access distributing directory server by clients, work on directory and share the information in the directory by clients. The LDAP standard is established by the work team of Internet Engineering Task Force (IETF).

As the name described, LDAP is designed as an effect way to access directory service without the complexity of other directory service protocols. For LDAP is defined to perform, inquire and modify the information within the directory, and acquire the data in the directory securely, therefore users can apply LDAP to search or list the directory object, inquire or manage the active directory.

UPnP

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

Wake on LAN

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

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

Web User Interface

II-5-1 Dynamic DNS

Enable the Function and Add a Dynamic DNS Account

1. Assume you have a registered domain name from the DDNS provider, say *hostname.dyndns.org*, and an account with username: *test* and password: *test*.

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

Available settings are explained as follows:

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

Auto-Update interval	Set the time for the router to perform auto update for DDNS service.
Index	Click the number below Index to access into the setting page of DDNS setup to set account(s).
Enable	Check the box to enable such account.
WAN Interface	Display the WAN interface used.
Domain Name	Display the domain name that you set on the setting page of DDNS setup.

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

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

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

Index : 1

☑ Enable Dynamic DNS Account

WAN Interface	WAN1 First ▼
Service Provider	User-Defined ▼
Provider Host	changeip.org
Service API	/dynamic/dns/update.asp? u=jo▮▮▮&p=jo▮▮▮▮▮&hostname=j▮▮▮.changeip.org&ip=###IP###&c md=update&offline=0
Auth Type	basic ▼
Connection Type	Http ▼
Server Response	
Login Name	chronic6653 (max. 64 characters)
Password	•••••••••• (max. 23 characters)
☐ Wildcards	
☐ Backup MX	
Mail Extender	
Determine WAN IP	Internet IP ▼

OK   Clear   Cancel

Available settings are explained as follows:

Item	Description
Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
WAN Interface	**WANx First** - While connecting, the router will use WANx as the first channel for such account. If WANx fails, the router will use another WAN interface instead. **WANx Only** - While connecting, the router will use WANx as the only channel for such account.
Service Provider	Select the service provider for the DDNS account.
Service Type	Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field.
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.
Determine WAN IP	If a Vigor router is installed behind any NAT router, you can enable such function to locate the real WAN IP. When the WAN IP used by Vigor router is private IP, this function can detect the public IP used by the NAT router and use the detected IP address for DDNS update.

There are two methods offered for you to choose:

● **WAN IP** - If it is selected and the WAN IP of Vigor router is private, DDNS update will take place right away.

● **Internet IP** – If it is selected and the WAN IP of Vigor router is private, it will be converted to public IP before DDNS update takes place.

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

DrayDDNS Settings

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

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

Available settings are explained as follows:

Item	Description
Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
Service Provider	Choose **DrayTek Global** as the service provider.
Status	Display if the license is actvtaed or not.
Determine WAN IP	If a Vigor router is installed behind any NAT router, you can enable such function to locate the real WAN IP. When the WAN IP used by Vigor router is private IP, this function can detect the public IP used by the NAT router and use the detected IP address for DDNS update. There are two methods offered for you to choose: ● **WAN IP** - If it is selected and the WAN IP of Vigor router is private, DDNS update will take place right away. ● **Internet IP** – If it is selected and the WAN IP of Vigor router is private, it will be converted to public IP before DDNS update takes place.
WAN Interfaces	**WANx** - While connecting, the router will use WANx as the channel for such account.

Let's Encrypt certificate	**Auto Update** - Check the box to make the system update the certificate automatically.

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 router.

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.

II-5-2 LAN DNS / DNS Forwarding

The LAN DNS lets the network administrators host servers with privacy and security. When the network administrators of your office set up FTP, Mail or Web server inside LAN, you can specify specific private IP address (es) to correspondent servers. Thus, even the remote PC is adopting public DNS as the DNS server, the LAN DNS resolution on Vigor3910 Series will respond the specified private IP address.
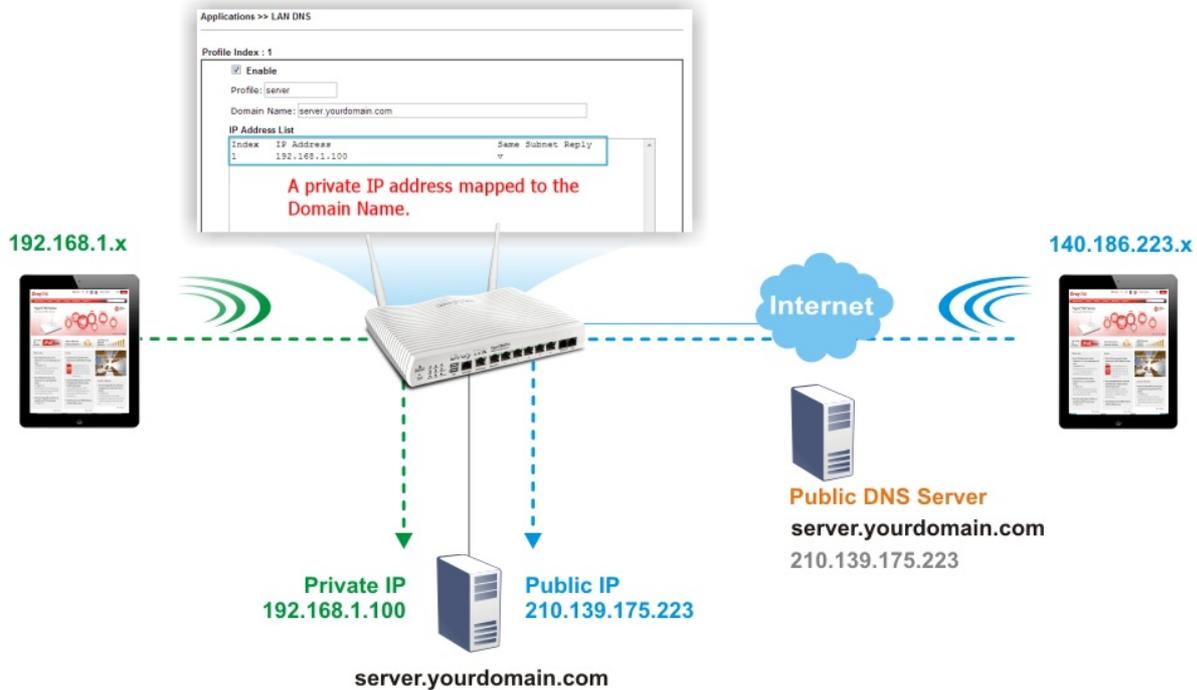
Simply click **Application>>LAN DNS/DNS Forwarding** to open the following page.

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profiles and recover to factory settings.
Index	Click the number below Index to access into the setting page.

Enable	Check the box to enable the selected profile.
Profile	Display the name of the LAN DNS profile.
Domain Name	Display the domain name of the LAN DNS profile.
Forwarding	Display that such profile is conditional DNS forwarding or not.
DNS Server	Display the IP addres of the DNS Server.

You can set up to 120 LAN DNS profiles.

To create a LAN DNS profile:

1. Click any index, say Index No. 1.

2. The detailed settings with index 1 are shown below.

Applications >> LAN DNS / DNS Forwarding

LAN DNS	Conditional DNS Forwarding

Profile Index : 1

☐ **Enable**

Profile: [_____]

Domain Name: [_____]

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

CNAME(Alias Domain Name): [Add]

IP Address List

Index	IP Address	Same Subnet Reply

[Add] [Delete]

[OK] [Clear]

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable such profile.
Profile	Type a name for such profile. **Note:** If you type a name here for LAN DNS and click **OK** to save the configuration, the name also will be applied to conditional DNS forwarding automatically.
Domain Name	Type the domain name for such profile.
CNAME (Alias Domain Name)	CNAME is abbreviation of Canonical name record. Such option is used to record the domain name or the host alias. **Add** – Click it to add a new host with specified reference. **Delete** – Click it to remove the setting.
IP Address List	The IP address listed here will be used for mapping with the domain name specified above. In general, one domain name

	maps with one IP address. If required, you can configure two IP addresses mapping with the same domain name.
	Add – Click it to open a dialog to type the host's IP address.
	• **Only responds to the DNS….** – Different LAN PCs can share the same domain name. However, you have to check this box to make the router identify & respond the IP address for the DNS query coming from different LAN PC.
	Delete – Click it to remove an existed IP address on the list.
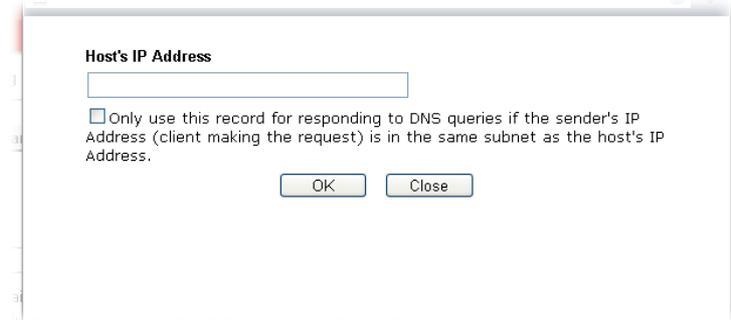
3. Click **OK** button to save the settings.

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

Available settings are explained as follows:

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

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

6. A new LAN DNS profile has been created.

II-5-3 DNS Security

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

II-5-3-1 General Setup

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

Available settings are explained as follows:

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

II-5-3-2 Domain Diagnose

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

Available settings are explained as follows:

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

II-5-4 Schedule

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

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

Available settings are explained as follows:

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

Comment	Display the name of the time schedule.
Time	Display the valid time period by time bar.
Frequency	Display which day(s) will be always on and which day(s) will be always off of the schedule profile by color boxes.
	⬤ - If it lights in green, it means such schedule is active.

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

To add a schedule:

1. Click any index, say Index No. 1.

2. The detailed settings of the call schedule with index 1 are shown below.

Applications >> Schedule

Index No. 1 Current System Time   2000 Jan 1 Sat 4 : 51 : 56 | **System time set** |

☑ Enable Schedule Setup

    Comment   [   ]
    Start Date (yyyy-mm-dd)   2000 ▼ - 1 ▼ - 1 ▼
    Start Time (hh:mm)   0 ▼ : 0 ▼
    Duration Time (hh:mm)   0 ▼ : 0 ▼
    End Time (hh:mm)   00   : 00
    Action   Force On ▼

    How Often
    ◯ Once
    ⦿ Weekdays
         ☐ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☐ Sat
    ◯ Monthly, on date 1 ▼
    ◯ Cycle duration: 1 ▼ days (Cycle will start on the Start Date.)

Note:
Comment can only contain A-Z a-z 0-9 , . { } - _ ( ) ^ $! ~ ` |

        [OK]   [Clear]   [Cancel]

Available settings are explained as follows:

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

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.
	● **Monthly, on date –** The router will only execute the action applied such schedule on the date (1 to 28) of a month.
	● **Cycle duration –** Type a number as cycle duration. Then, any action applied such schedule will be executed per several days. For example, "3" is selected as cycle duration. That means, the action applied such schedule will be executed every three days since the date defined on the Start Date.

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

Example

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

Office Hour:

(Force On)

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

1.   Make sure the PPPoE connection and **Time Setup** is working properly.

2.   Configure the PPPoE always on from 9:00 to 18:00 for whole week.

3.   Configure the **Force Down** from 18:00 to next day 9:00 for whole week.

4.   Assign these two profiles to the PPPoE Internet access profile. Now, the PPPoE Internet connection will follow the schedule order to perform **Force On** or **Force Down** action according to the time plan that has been pre-defined in the schedule profiles.

II-5-5 RADIUS/TACACS+

Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization, and accounting, which is widely used in enterprise networks. It is the most common authentication method to manage the clients' access to the wireless network, the Internet and the VPN.

The router supports external TACACS+ and internal and external RADIUS servers for user authentication. To configure TACACS+ or RADIUS servers, from the Main Menu select **Applications >> RADIUS/TACACS+**.

II-5-5-1 External RADIUS

Vigor Router supports the RADIUS client function. The built-in RADIUS client feature allows the router to authenticate the remote dial-in VPN users, the wireless connections through 802.1X and the access to the Internet.

When it operates as the RADIUS client, Vigor Router needs to work with an External Radius server, and the External RADIUS Server setting should be configured here.

Item	Description
RADIUS Server Status Log	Display the record of current status of RADIUS server.
Enable	Select to enable the profile.
Comment	Displays the comment of the profile.
Primary Server	Displays the IP address of the primary server.
Secondary Server	Display the IP address of the secondary server.

Click any index number to open the following page. It is used to configure settings for external RADIUS server. Then users of the Vigor router will be authenticated by this server for the network application.

Applications >> RADIUS/TACACS+ >> Profile 1

Available settings are explained as follows:

Item	Description
Enable this profile	Check to enable RADIUS client profile. **Comment** - Enter a brief description for this profile.
Primary Server	**Primary Server** - Enter the IP address of RADIUS server. **Authentication Port** - The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138. **Secret** - The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret. The maximum length of the shared secret you can set is 36 characters. **Retry** - Set the number of attempts to perform reconnection with RADIUS server. If the connection (with the Primary Server) still fails, stop the connection attempt and begin to make connection with the secondary server.
Secondary Server	**Secondary Server** - Enter the IP address of RADIUS server. **Authentication Port** - The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138. **Secret** - The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret. The maximum length of the shared secret you can set is 36 characters. **Retry** - Set the number of attempts to perform reconnection. If the connection (with the Secondary Server) still fails, stop the connection attempt. The client authentication would be determined as "failed".

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

II-5-5-2 Internal RADIUS

Except for being a built-in RADIUS client, Vigor router also can be operated as a RADIUS server which performs security authentication by itself. This page is used to configure settings for internal RADIUS server. Then users of Vigor router will be authenticated by Vigor router directly.

Available settings are explained as follows:

Item	Description
Enable	Select to enable the router's internal RADIUS server.
Authentication Port	The UDP port for authentication message.
RADIUS Client Access List	Only clients that meet the criteria configured in the access list are allowed to access the RADIUS server.
	Index - The index number of the client entry.
	Enable - Select to enable this client entry.
	Shared Secret - A text string that is known to both the router's RADIUS server and the RADIUS client that is used to

	authenticate messages sent between them. Maximum length is 36 characters.
	IP Address – Enter the base address of the IP block.
	IP Mask – Enter the IP mask to configure the size of the IP block.
	IPv6 Address – Enter the base address of the IPv6 block.
	IPv6 Length - Enter the prefix length of the IPv6 block.
Authentication	Select the authentication protocol(s) to be used.
	PAP Only – Only the Password Authentication Protocol will be used to validate users.
	PAP/CHAP/MS-CHAP/MS-CHAPv2 – PAP, CHAP (Challenge-Handshake Authentication Protocol), and Microsoft versions of CHAP can be used to validate users.
User Profile	During the process of security authentication, user account and user password will be required for identity authentication. Before configuring such page, create at least one user profile in **User Management>>User Profile** first.
	Select All – Click to move all user profiles under the Available List to the Authentication List.
	Clear All- Click to remove all user profiles from the Authentication List.
	Available List – User profiles (created in **User Management >> User Profile**) that have not been added to the authentication list.
	Authentication List – User profiles (created in **User Management >> User Profile**) that have been added to the authentication list. Users can log in using these profiles.

To add a User Profile to the RADIUS server, select it under Available List, then click the

[»] button. To remove a User Profile from the RADIUS server, select it under Selected

Authentication List, then click the [«] button.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To reset all settings to blank, click **Clear**.

II-5-5-3 External TACACS+

It means Terminal Access Controller Access-Control System Plus (TACACS+). It is another protocol for authentication and works as the RADIUS does. Click the **External TACACS+** to open the following page:

Applications >> RADIUS/TACACS+

External RADIUS	Internal RADIUS	External TACACS+

☐ Enable

Server IP Address

Destination Port   49

Type   ASCII ▼

Shared Secret   Max: 36 characters

Confirm Shared Secret

[OK] [Clear] [Cancel]

Available settings are explained as follows:

Item	Description
Enable	Select to enable the use of the external TACACS+ server.
Server IP Address	Enter the IP address of TACACS+ server.
Destination Port	The UDP port used by the TACACS+ server.
Shared Secret	A text string that is known to both the TACACS+ server and client (the router) is used to authenticate messages sent between them. Maximum length is 36 characters.
Confirm Shared Secret	Enter the Shared Secret for confirmation.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To reset all settings to blank, click **Clear**.

II-5-6 Active Directory/ LDAP

Lightweight Directory Access Protocol (LDAP) is a communication protocol for using in TCP/IP network. It defines the methods to access distributing directory server by clients, work on directory and share the information in the directory by clients. The LDAP standard is established by the work team of Internet Engineering Task Force (IETF).

As the name described, LDAP is designed as an effect way to access directory service without the complexity of other directory service protocols. For LDAP is defined to perform, inquire and modify the information within the directory, and acquire the data in the directory securely, therefore users can apply LDAP to search or list the directory object, inquire or manage the active directory.

General Setup

This page allows you to enable the function and specify general settings for LDAP server.

Applications >> Active Directory /LDAP

General Setup	Active Directory / LDAP Profiles		Set to Factory Default

☐ Enable
Bind Type   [Simple Mode ▼]
Server Address   [   ]
Destination Port   [389]   ☐ Use SSL
Regular DN   [   ]
Regular Password   [   ]

[OK]   [Cancel]

Available settings are explained as follows:

Item	Description
Enable	Check to enable such function.
Bind Type	There are three types of bind type supported. ● **Simple Mode** – Just simply do the bind authentication without any search action. ● **Anonymous** – Perform a search action first with Anonymous account then do the bind authentication. ● **Regular Mode**– Mostly it is the same with anonymous mode. The different is that, the server will firstly check if you have the search authority. For the regular mode, you'll need to type in the **Regular DN** and **Regular Password**.
Server Address	Enter the IP address of LDAP server.
Destination Port	Type a port number as the destination port for LDAP server.
Use SSL	Check the box to use the port number specified for SSL.
Regular DN	Type this setting if **Regular Mode** is selected as **Bind Type**.

Regular Password	Specify a password if **Regular Mode** is selected as **Bind Type**.

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

Active Directory / LDAP Profiles

You can configure eight AD/LDAP profiles. These profiles would be used with User Management for different purposes in management.

Applications >> Active Directory /LDAP

General Setup	Active Directory / LDAP Profiles		Set to Factory Default	
Index	**Name**	**Distinguished Name**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		

Click any index number link to open the following page.

Applications >> Active Directory /LDAP>>Server Profiles

Index No. 1

Name	RD1
Common Name Identifier	UD1
Base Distinguished Name	
Additional Filter	
Group Distinguished Name	

Note:
Please type in your additional filter for BaseDN search request. For example, "gidNumber=500" for OpenLDAP, and "msNPAllowDialin=TRUE" for AD.

[OK] [Cancel]

Available settings are explained as follows:

Item	Description
Name	Type a name for such profile. The length of the user name is limited to 19 characters.
Common Name Identifier	Type or edit the common name identifier for the LDAP server. The common name identifier for most LDAP server is "cn".
Additional Filter	Type the condition for additional filter.
Base Distinguished Name / Group Distinguished Name	Type or edit the distinguished name used to look up entries on the LDAP server. Sometimes, you may forget the Distinguished Name since it's too long. Then you may click the button to list all the account information on the AD/LDAP Server to assist you finish

	the setup.

After finished the above settings, click **OK** to save and exit this page. A new profile has been created.

II-5-7 IGMP

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

II-5-7-1 General Setting

Applications >> IGMP

General setting	Working status

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

Interface	WAN1 ▾
IGMP version	Auto ▾
General Query Interval	125 (seconds)
Add PPP header	☐
(Encapsulate IGMP in PPPoE)	
Enable IGMP syslog	☐

OK   Cancel

Available settings are explained as follows:

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

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

II-5-7-2 Working Group

Applications >> IGMP

| General setting | Working status |

| Refresh |

Multicast Group Table

| Index | Group ID | P2 | P4 | P9 | P10 | P11 | P12 |

IGMP Device Table

| Index | MAC Address | IP Address | Interface | IGMP Version |

Available settings are explained as follows:

Item	Description
Refresh	Click this link to renew the working multicast group status.
Group ID	This field displays the ID port for the multicast group. The available range for IGMP starts from 224.0.0.0 to 239.255.255.254.
P2 to P12	It indicates the LAN port used for the multicast group.

II-5-8 Wake on LAN

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

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

Applications >> Wake on LAN

Wake on LAN

Wake by:	IP Address ▼
IP Address:	MAC Address
MAC Address:	IP Address
	[ ].[ ].[ ].[ ]:[ ]:[ ] [Wake Up!]
Result	

Note:
Wake on LAN integrates with <u>Bind IP to MAC</u> function; only bound PCs can wake up through IP.

Available settings are explained as follows:

Item	Description
Wake by	Two types provide for you to wake up the binded IP. ● **MAC Address** - If you choose Wake by **MAC Address**, you have to enter the correct MAC address of the host in MAC Address boxes. ● **IP Address** - It is available when **LAN** >>**Bind IP to MAC** is enabled. If you choose **Wake by IP Address**, select an IP address.
IP Address	The IP addresses that have been configured in **LAN>>Bind IP to MAC** will be shown in this drop down list. Choose the IP address from the drop down list that you want to wake up.
MAC Address	Enter any one of the MAC address of the bound PCs.
Wake Up	Click this button to wake up the selected IP. See the following figure. The result will be shown on the box.

II-5-9 SMS / Mail Alert Service

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

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

SMS Provider

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

Applications >> SMS / Mail Alert Service

	SMS Alert		Mail Alert			Set to Factory Default
Index	**Enable**	**SMS Provider**	**Recipient Number**	**Notify Profile**	**Schedule(1-15)**	
1	☐	1 - ??? ▾		1 - ??? ▾		
2	☐	1 - ??? ▾		1 - ??? ▾		
3	☐	1 - ??? ▾		1 - ??? ▾		
4	☐	1 - ??? ▾		1 - ??? ▾		
5	☐	1 - ??? ▾		1 - ??? ▾		
6	☐	1 - ??? ▾		1 - ??? ▾		
7	☐	1 - ??? ▾		1 - ??? ▾		
8	☐	1 - ??? ▾		1 - ??? ▾		
9	☐	1 - ??? ▾		1 - ??? ▾		
10	☐	1 - ??? ▾		1 - ??? ▾		

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

[OK]   [Cancel]

Available settings are explained as follows:

Item	Description
Enable	Check the box to enable such profile.
SMS Provider	Use the drop down list to choose SMS service provider. You can click **SMS Provider** link to define the SMS server.
Recipient Number	Type the phone number of the one who will receive the SMS.
Notify Profile	Use the drop down list to choose a message profile. The recipient will get the content stated in the message profile. You can click the **Notify Profile** link to define the content of the SMS.
Schedule (1-15)	Type the schedule number that the SMS will be sent out. You can click the **Schedule(1-15)** link to define the schedule.

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

Mail Server

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

Available settings are explained as follows:

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

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

II-5-10 Bonjour

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

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

To enable the Bonjour service, click **Application>>Bonjour** to open the following page. Check the box(es) of the server service(s) that you want to share to the LAN clients.
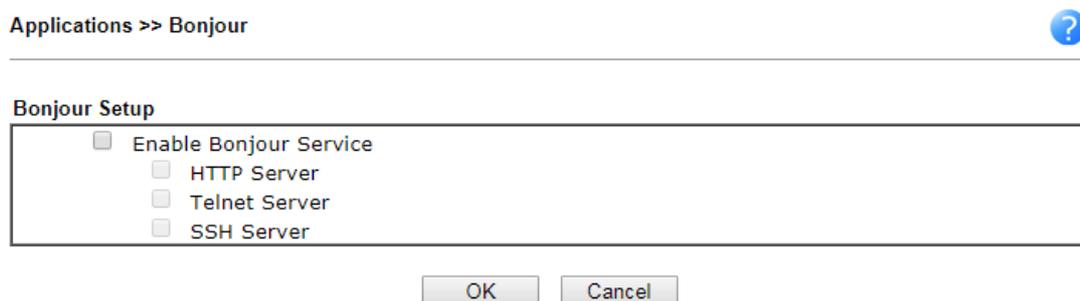
Below shows an example for applying the bonjour feature that Vigor router can be used as the FTP server.

1. Here, we use Firefox and DNSSD to discover the service in such case. Therefore, just ensure the Bonjour client program and DNSSD for Firefox have been installed on the computer.
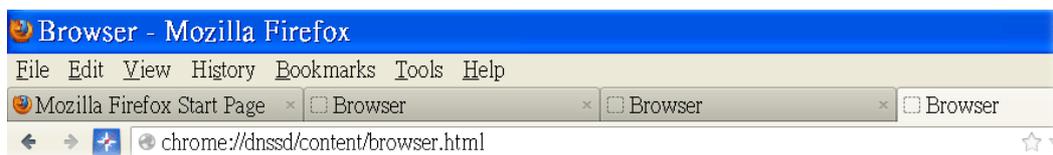
2. Open the web browse, Firefox. If Bonjour and DNSSD have been installed, you can open the web page (DNSSD) and see the following results.
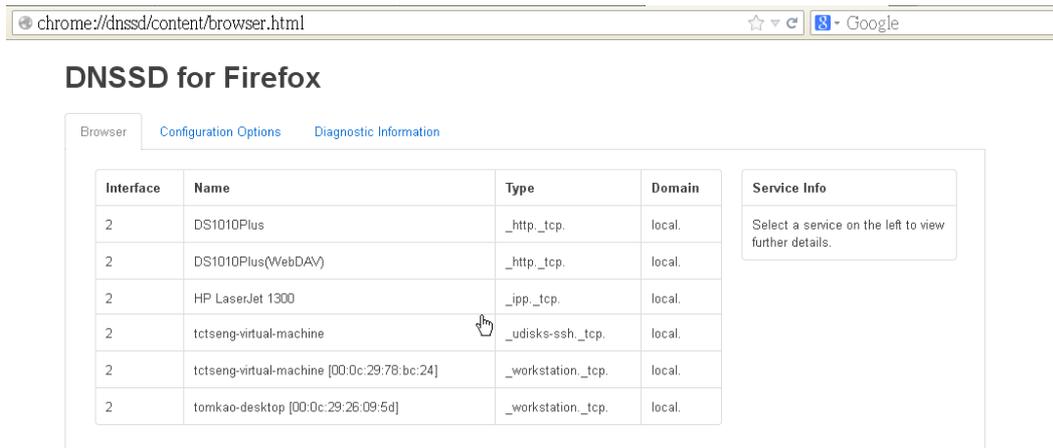
3. Open **System Maintenance>>Management**. Type a name (e.g., DrayTek) as the Router Name and click **OK**.
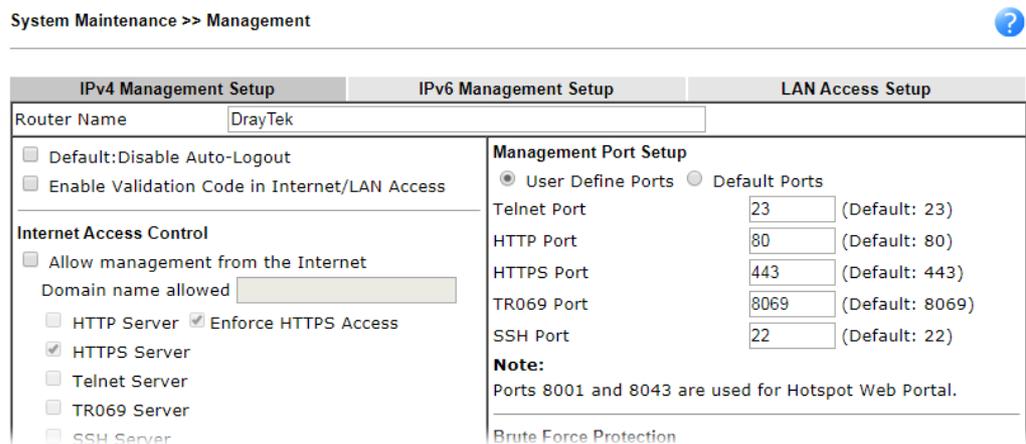
4. Next, open **Applications>>Bonjour**. Check the service that you want to use via Bonjour.
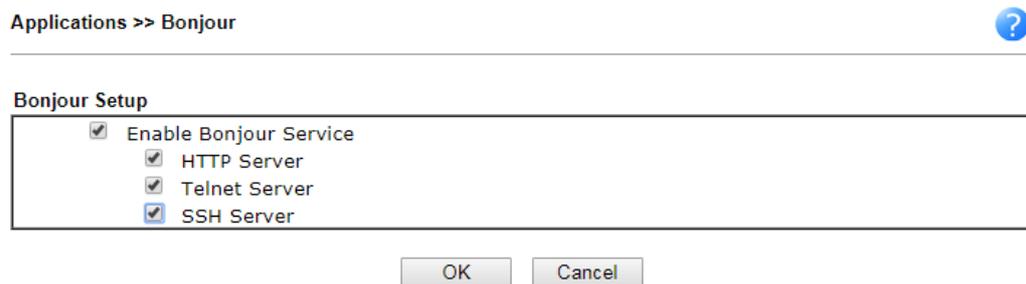
5. Open the DNSSD page again. The available items will be changed as the follows. It means the Vigor router (based on Bonjour protocol) is ready to be used as a printer server, FTP server, SSH Server, Telnet Server, and HTTP Server.

chrome://dnssd/content/browser.html

DNSSD for Firefox

Interface	Name	Type	Domain	Service Info
2	DS1010Plus	_http._tcp.	local.	Select a service on the left to view further details.
2	DS1010Plus(WebDAV)	_http._tcp.	local.	
2	HP LaserJet 1300	_ipp._tcp.	local.	
2	Vigor Router	_ftp._tcp.	local.	
2	Vigor Router	_http._tcp.	local.	
2	Vigor Router	_printer._tcp.	local.	
2	Vigor Router	_ssh._tcp.	local.	
2	Vigor Router	_telnet._tcp.	local.	
2	tctseng-virtual-machine	_udisks-ssh._tcp.	local.	
2	tctseng-virtual-machine [00:0c:29:78:bc:24]	_workstation._tcp.	local.	
2	tomkao-desktop [00:0c:29:26:09:5d]	_workstation._tcp.	local.	

6. Now, any page or document can be printed out through Vigor router (installed with a printer).
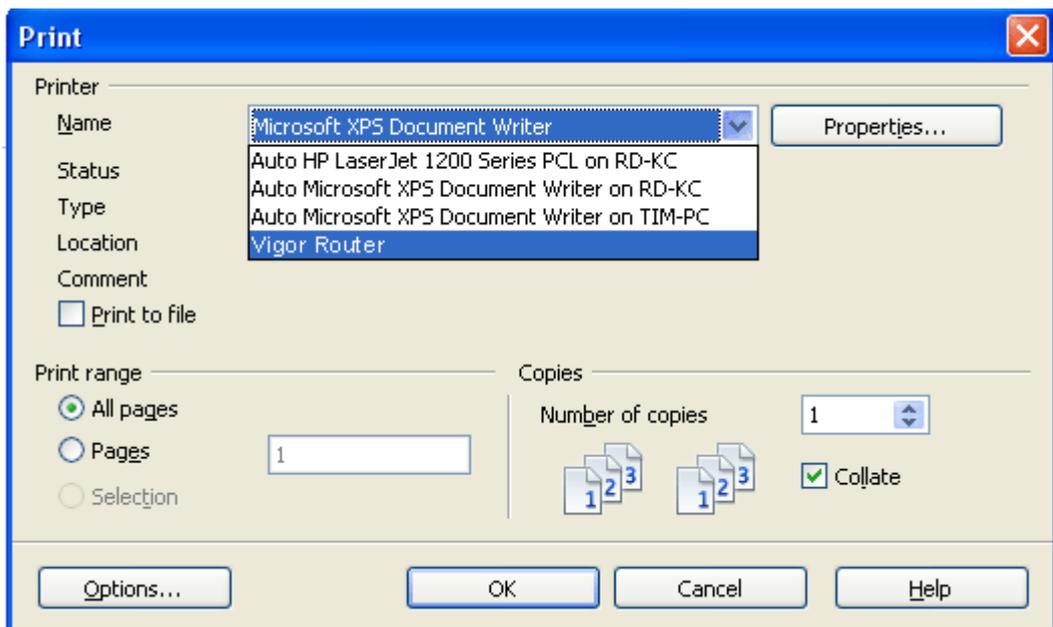
II-5-11 High Availability

The High Availability (HA) feature of the router provides redundancy of network resources, and reduces downtime in case of component failure. The level of sophistication of HA is determined by availability requirements and tolerance of system interruptions. Systems that provide near full-time availability typically have redundant hardware and software.

The HA of the Vigor3910 Series is designed to avoid single points-of-failure. When failures occur, the failover process transfers the network load handled by the failed component (the primary router) to the backup component (the secondary router), and the availability of network resources are preserved and partially failed transactions are recovered. In a matter of seconds the system returns to normal operation.

In order to set up High Availability, at least 2 DrayTek routers have to be configured in the following manner:

- Enable High Availability on both the primary and secondary routers.

- Set a high priority ID on the primary router, and a lower priority ID on the secondary router.

- Configure identical redundancy methods, group IDs, and authentication keys on both routers.

- Set the management interface of both routers to the same subnet.

- Enable virtual IP on both routers for each subnet in use. Make sure the virtual IPs are identical on both routers.

II-5-11-1 General Setup

Open **Applications>>High Availability** to get the following page.

Available settings are explained as follows:

Item	Description
Enable High Abailablity	Check this box to enable HA function.
Redundancy Method	Select the redundancy method for high availability.
	Hot-Standby -
	Such method is suitable when there is only one ISP account. When this method is selected,
	● During normal operation the secondary router will be idling. When the primary router fails to operate normally, the secondary router(s) will take over.
	● WAN settings of the primary and secondary routers are identical.
	Note: When Hot-Standby is used, the wireless LAN function on secondary router will be "disabled" directlly. Clients can not connect to the secondary router any more.
	Active-Standby -
	This method is suitable when there are multiple simultaneously active ISP connections. When this method is selected,
	● All WANs on the secondary routers can be up at the same time. LANs that are not configured under high availability can be routed to secondary routers.
	● WAN settings of primary and secondary routers are independently configured.
	● Config Sync may be enabled to synchronize most configuration settings between the primary and secondary routers.
	● All routers must be set to the same redundancy method.
Group ID	Type a value (1~255).
	In LAN environment, multiple routers can be devided into several groups. Each router must be specified with one group ID. Different routers with the same ID value will be categoried into the same group.
	Only one of the routers in the same group will be selected as the primary router.
Priority ID	Type a value (1~30).
	Different routers must be configured with different IDs.
	All routers within a group must be assigned a priority ID. Within a group, the router with the largest priority ID (i.e., the highest priority) will be the primary router. When multiple routers in a group are assigned the same priority ID, routers with lower LAN IP addresses (configured on the LAN >> General Setup page) have higher priority.
Authentication Key	Enter an authentication key up to 31 characters long. This is used to encrypt the DARP (DrayTek Address Redundancy Protocol) traffic to guard against malicious attacks.
Protocol	Select the IP protocol to be used for DARP.
Management Interface	Select the interface to be used for DARP negotiation between routers. Only interfaces which are enabled in **LAN>>General Setup** are available for selection.

	However, LAN1 is always enabled.
Update DDNS	**Enable –** Check the box to update the DDNS server for the secondary device when the primary router fails. If the primary device fails, and the secondary device must take over the job of data transmitting and receiving. Then the system will update the DDNS server to make the user connect to the specified domain name.
Syslog	**Enable –** Check the box to record required information on Syslog.
LAN1 ~ LAN50	**Enable –** Check the box to enable the interface. **Virtual IP -** Display the default IP address for each LAN. If rquired, modify the IP address for the LAN port device.

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

II-5-11-2 Config Sync

This page is used to specify the synchronization time for such Vigor router and only available when **Hot-Standby** method is specified and High Availability is enabled.

Applications >> High Availability

☑ Enable High Availability
Redundancy Method [Active-Standby ▼]

| General Setup | **Config Sync** | | Status | Set to Factory Default |

☐ Enable Config Sync (Max. Sync to 10 routers)

Config Sync Interval:

Day [0 ▼]
Hour [0 ▼]
Minute [15 ▼]

Exclude the following settings from config sync:
☑ WAN Settings

Note:
This feature requires that both routers are the same series, and the High Availability must be enabled for Config Sync to operate.

[OK] [Cancel]

Available settings are explained as follows:

Item	Description
Enable Config Sync (Max. Sync to 10 routers)	Check this box to enable configuration synchronization. To sync configuration from primary to secondary router, both primary and seconday routers need to enable "config sync". Note that config sync can be enabled by **Hot-Standby** redundancy method only.
Config Sync Interval	**Day / Hour / Minute** - Primary router will sync its configuration to secondary router based on the time interval set here.
Exclude the following settings from config sync	Settings selected in this field will be excluded when executing configuration synchronization. This setting is

	available when the Redundancy Method is set to "Hot Standby".

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

When the configuration method is set to "Hot Standby", the following settings will not be synchronized:

● WAN (user selectable)

● LAN

● LAN IPv6

● router name

● admin and user passwords.

Example:

Take the following picture as an example. The upper Vigor3910 is regarded as primary device, the lower Vigor3910 is regarded as secondary device. When primary Vigor3910 Series is broken down, the secondary device could replace the primary role to take over all jobs as soon as possible. However, once the primary device is working again, the secondary device would be changed to original role to stand by.
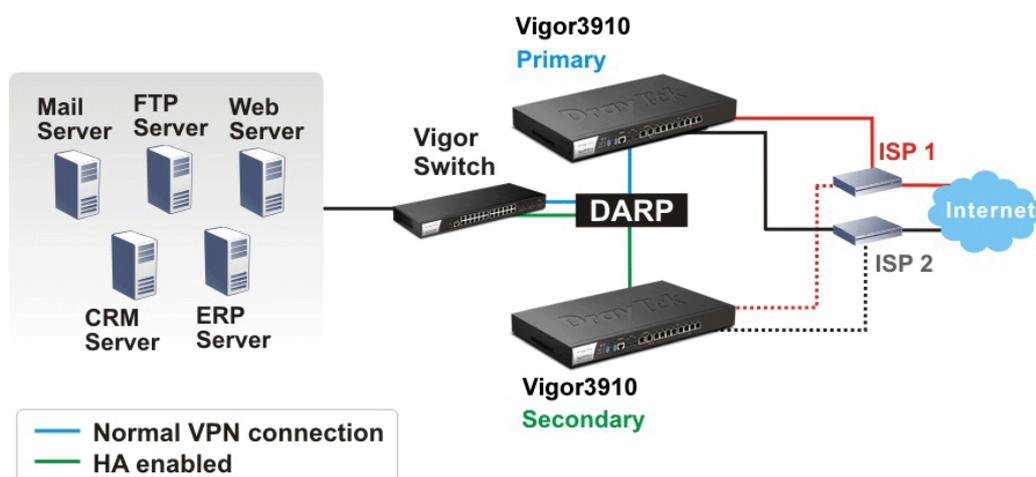
Application Notes

A-1 How to Implement the LDAP/AD Authentication for User Management?

For simplifying the configuration of LDAP authentication for User Access Management, we implement "Group" feature.

There is no need to pre-configure user profile for each user on Vigor router anymore. We only need to configure the Groups DN, then the Vigor router (e.g., Vigor 2860 series) can pass the authentication to LDAP server with the pre-defined Group path.

Below shows the configuration steps:

1. Access into the web user interface of the Vigor router.

2. Open **Applications**>>**Active Directory /LDAP** to get the following page for configuring LDAP related settings.

There are three types of bind type supported:

- **Simple Mode** – Just simply do the bind authentication without any search action.

- **Anonymous** – Perform a search action first with Anonymous account then do the bind authentication.

- **Regular Mode**– Mostly it is the same with anonymous mode. The different is that, the server will firstly check if you have the search authority.
  For the regular mode, you'll need to type in the **Regular DN** and **Regular Password**.

3. Create LDAP server profiles. Click the **Active Directory /LDAP** tab to open the profile web page and click any one of the index number link.

   If we have two groups "**RD1**" and "**SHRD**" on LDAP server, we can configure two LDAP server profiles with different Group Distinguished Name.

Applications >> Active Directory /LDAP>>Server Profiles

Index No. 1

Name	rd1
Common Name Identifier	uid
Base Distinguished Name	ou=people,dc=ms,de=draytek,dc=com
Additional Filter	cn=shrd,ou=group,dc=msg
Group Distinguished Name	

Note:
Please type in your additional filter for BaseDN search request. For example, "gidNumber=500" for OpenLDAP, and "msNPAllowDialin=TRUE" for AD.

[OK] [Cancel]

and

Applications >> Active Directory /LDAP>>Server Profiles

Index No. 2

Name	shrd
Common Name Identifier	uid
Base Distinguished Name	ou=people,dc=ms,dc=draytek,dc=com
Additional Filter	cn=shrd,ou=group,dc=ms,dc=draytek,dc
Group Distinguished Name	

Note:
Please type in your additional filter for BaseDN search request. For example, "gidNumber=500" for OpenLDAP, and "msNPAllowDialin=TRUE" for AD.

[OK] [Cancel]

4. Click **OK** to save the settings above.

5. Open **User Management>>General Setup**. Select **User-Based** as the **Mode** option.

User Management >> General Setup

General Setup

Mode Selection:

○ **Rule-Based** is a management method based on IP address. Administrator may set different firewall rules to different IP address.

● **User-Based** is a management method based on user profiles. Administrator may set different firewall rules to different user profiles.

Notice for User-Based mode:

• In User-Based mode, **Active Rules** in Firewall will be applied to all LAN clients, packets that matches the Active Rules will be blocked or pass immediately, no user authentication is required.

• Only **Inactive Rules** in Firewall can be set for individual user profile. In User-Based mode, packets that do not match Active Rules will need authentication, and the Inactive Rule applied to the specific user profile will then take effect.

Authentication page:

Web Authentication: ● HTTPS ○ HTTP

Login Page Logo: [Default ▼]

6. Then open **VPN and Remote Access>>PPP General Setup** to **check** the profile(s) that will be authenticated with LDAP server.

After above configurations, users belong to either "rd1" or "shrd" group can access Internet after inputting their credentials on LDAP server.

A-2 How to use DrayDDNS?

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

Set up DrayDDNS on DrayOS Router

1. Go to **Applications** >> **Dynamic DNS Setup**. Enable Dynamic DNS Setup.

2. Go to **Wizards** >> **Service Activation Wizard** page, wait for the router to connect to MyVigor server, then:

    (a) Select **DT-DDNS**.

    (b) Enter the desired Domain Name.

(c)   Make sure you have read the License Agreement. Check **I have read and accept the above Agreement**, then click **Next**.

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

4.   MyVigor server will reply with the service activation information.

DrayTek Service Activation

Service Name	Start Date	Expire Date	Status
Web Content filter	---	---	Not Activated
APP Enforcement	---	---	Not Activated
DDNS	2018-01-18	2019-01-18	DT-DDNS

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

Copyright © DrayTek Corp. All Rights Reserved.

5. Vigor router will contact with MyVigor server, then get the DrayDDNS license as well as the domain name back, and create the DDNS profile automatically. Please go to **Applications** >> **Dynamic DNS Setup** page to make sure the router has created the DDNS profile.

Applications >> Dynamic DNS Setup

Dynamic DNS Setup | **Set to Factory Default** |

☑ Enable Dynamic DNS Setup   [View Log] [Force Update]

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

Accounts:

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

[OK]   [Clear All]

Note that, if your router does not get the domain after you activating the license, it may due to the router does not trigger the process, which to connect and get the license from MyVigor server. You may reboot the router to trigger the process.

Modify DrayDDNS Domain Name

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

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

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

Index : 1

☑ Enable Dynamic DNS Account

Service Provider	DrayDDNS (Global) ▼
Status	**Activated** [Start Date:**2018-01-19** Expire Date:**2019-01-19**]
Domain Name	demo . drayddns.com Edit domain
Determine WAN IP	WAN IP ▼ ☑ IPv4 ☐ IPv6
WAN Interfaces	☑ WAN 1 ☑ WAN 2 ☑ WAN 3 ☑ WAN 4

OK   Clear   Cancel

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

My Information - My Products

Device Information

Device Name : FAE2860
Serial Number : 2016   0205
Model : Vigor2860 Series

Rename   Transfer   Back

Device's Service   Expired License

Service	Provider	Action	Status	Start Date	Expired Date	Note
WCF	BPjM	Activate	● On	-	-	-
WCF	Cyren	Trial	● On	-	-	-
APPE	DT-APPE	Activate	● On	-	-	-
DDNS	DT-DDNS	Renew	● On	2018-01-19	2019-01-19	Edit DDNS settings

3. Input the desired **Domain name** and click **Update**.

Edit DDNS Settings

Domain Name	modification .drayddns.com
Current IP	192.168.100.100 Get PC's Internet IP
Last Update	2018-01-22 14:26:29
Status	**Update success**

Update   Delete   Reset

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

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

Index : 1

☑ Enable Dynamic DNS Account

Service Provider	DrayDDNS (Global) ▼
Status	**Activated [Start Date:2018-01-19 Expire Date:2019-01-19]**
Domain Name	demo . drayddns.com [Sync domain]
Determine WAN IP	WAN IP ▼ ☑ IPv4 ☐ IPv6
WAN Interfaces	☑ WAN 1 ☑ WAN 2 ☑ WAN 3 ☑ WAN 4

[OK]   [Clear]   [Cancel]

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

Applications >> Dynamic DNS Setup

Dynamic DNS Setup | **Set to Factory Default** |

☑ Enable Dynamic DNS Setup   [View Log] [Force Update]

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

Accounts:

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

II-6 Routing

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

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

Load Balance

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

Specify Interface

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

Address Mapping

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

Priority

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

Failover to/Failback

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

Other routing

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

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

Web User Interface
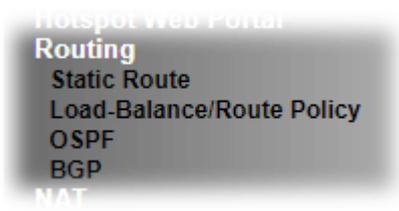
II-6-1 Static Route

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

II-6-1-1 Static Route for IPv4

Available settings are explained as follows:

Item	Description
Index	The number (1 to 30) under Index allows you to open next page to set up static route.
Enable	Check the box to enable such profile.
Destination Address	Displays the destination address of the static route.
Set to Factory Default	Clear all of the settings and return to factory default settings.
Viewing Routing Table	Displays the routing table for your reference. Diagnostics >> View Routing Table Current Running Routing Table IPv6 Routing Table | Refresh | Key: C - connected, S - static, R - RIP, * - default, ~ - private C~ 192.168.1.0/ 255.255.255.0 directly connected LAN1

Add Static Routes to Private and Public Networks

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

● use the Main Router to surf the Internet.

● create a private subnet 192.168.10.0 using an internal Router A (192.168.1.2)

● create a public subnet 211.100.88.0 via an internal Router B (192.168.1.3).

● have set Main Router 192.168.1.1 as the default gateway for the Router A 192.168.1.2.

Before setting Static Route, user A cannot talk to user B for Router A can only forward recognized packets to its default gateway Main Router.
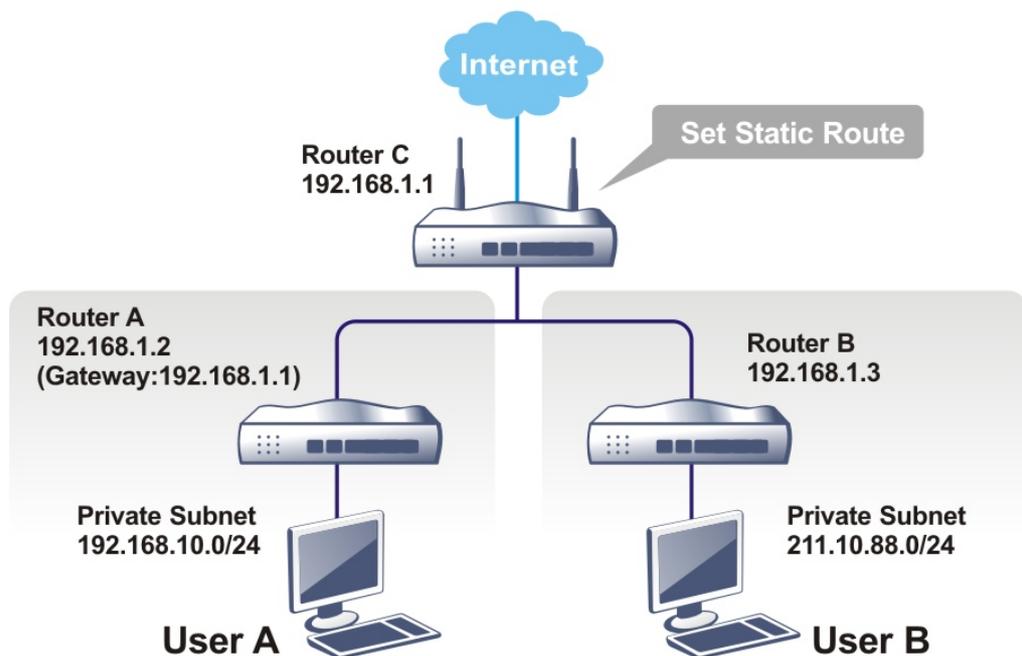
1. Go to **LAN** page and click **General Setup**, select 1st Subnet as the **RIP Protocol Control**. Then click the **OK** button.

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

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.
Gateway IP Address	Type the gateway IP addres 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. Click **OK**.

Vigor3910 Series User's Guide

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

II-6-1-2 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.
Enable	Check the box to enable such profile.
Destination Address	Displays the destination address of the static route.
Set to Factory Default	Clear all of the settings and return to factory default settings.
Viewing IPv6 Routing Table	Displays the routing table for your reference.

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

LAN >> Static Route Setup

Index No. 1

☐ Enable

Destination IPv6 Address / Prefix Len   [::   ] / [0   ]

Gateway IPv6 Address   [   ]

Network Interface   [LAN1 ▼]

[OK]   [Cancel]   [Delete]

Available settings are explained as follows:

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

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

II-6-2 Load-Balance /Route Policy

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

II-6-2-1 General Setup

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

Routing >> Load-Balance/Route Policy

Available settings are explained as follows:

Item	Description
Index	Click the number of index to access into the configuration web page.
Enable	Check this box to enable this policy.
Protocol	Display the protocol used for this policy.
Interface	Display the interface to send packets to once the policy is matched.
Priority	Display the priority value for such route policy profile.
Src IP Start	Display the IP address for the start of the source IP.
Src IP End	Display the IP address for the end of the source IP.
Dest IP Start	Display the IP address for the start of the destination IP.
Dest IP End	Display the IP address for the end of the destination IP.
Dest Port Start	Display the IP address for the start of the destination port.
Dest Port End	Display the IP address for the end of the destination port.
Move UP/Move Down	Use **Up** or **Down** link to move the order of the policy.
Wizard Mode	Allow to configure frequently used (simple and basic) settings of route policy via three setting pages.
Advance Mode	Allow to configure detailed settings of route policy.

To use **Wizard Mode**, simple do the following steps:

1. Click the **Wizard Mode** radio button.

2. Click **Index 1**. The setting page will appear as follows:

Available settings are explained as follows:

Item	Description
Source IP	**Any** – Any IP can be treated as the source IP. **Src IP Start** - Type the source IP start for the specified WAN interface. **Src IP End** - Type the source IP end for the specified WAN interface. If this field is blank, it means that all the source IPs inside the LAN will be passed through the WAN interface.
Destination IP	**Any** – Any IP can be treated as the destination IP. **Dest IP Start**- Type the destination IP start for the specified WAN interface. **Dest IP End** - Type the destination IP end for the specified WAN interface. If this field is blank, it means that all the destination IPs will be passed through the WAN interface. **Country Object** - Choose a country object. All the traffic from destination IPs in that country is allowed pass through the WAN interface.

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

Available settings are explained as follows:

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

Interface Address	It is available only when WAN is selected as Interface. There might be a lot of alias IP address, it is necessary to assign one alias IP for the interface setting.

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

Load-Balance/Route Policy

Index: 1 NAT or Routing

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

The current setting is:
- ⦿ Force NAT
- ◯ Force Routing

[< Back] [Next >] [Finish] [Cancel]

Available settings are explained as follows:

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

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

Load-Balance/Route Policy

Index: 1 Configuration Summary

Criteria

Source IP   Any
Destination IP   192.168.1.6 ~ 192.168.1.56

Interface

WAN3

More options

Force NAT

[< Back] [Next >] [Finish] [Cancel]

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

Load-Balance/Route Policy

Load-Balance/Route Policy   10 ▼ rules per page | **Set to Factory Default** |

Index	Enable	Protocol	Interface	Priority	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End	Move Up	Move Down
1	☑	Any	WAN3	200	Any	Any	192.168.1.6	192.168.1.56	Any	Any		**Down**
2	☐	Any	WAN1	200	Any	Any	Any	Any	Any	Any	**UP**	**Down**
3	☐	Any	WAN1	200	Any	Any	Any	Any	Any	Any	**UP**	**Down**

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

1. Click the **Advance Mode** radio button.

2. Click **Index 2** to access into the following page.

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable this policy.
Comment	Type a brief explanation for this profile.
Criteria	
Protocol	Use the drop-down menu to choose a proper protocol for the WAN interface.
Source	**Any** – Any IP can be treated as the source IP. **IP Range** – Define a range of IP address as source IP addresses. ● **Start** - Type an address as the starting IP for such profile. ● **End** - Type an address as the ending IP for such profile. **IP Subnet** – Define a subnet containing IP address and mask address. ● **Network** – Type an IP address here. ● **Mask** – Use the drop down list to choose a suitable mask for the network. **IP Object / IP Group**– Use the drop down list to choose a

Vigor3910 Series User's Guide

	preconfigured IP object/group.
Destination	**Any** – Any IP can be treated as the destination IP.
	IP Range – Define a range of IP address as destination IP addresses.
	● **Start -** Type an address as the starting IP for such profile.
	● **End -** Type an address as the ending IP for such profile.
	IP Subnet – Define a subnet containing IP address and mask address.
	● **Network** – Type an IP address here.
	● **Mask** – Use the drop down list to choose a suitable mask for the network.
	Domain Name – Specify a domain name as the destination.
	● **Select** – Click it to choose an existing domain name defined in Objects Setting>>String Object.
	● **Delete** – Remove current used domain name.
	● **Add** – Create a new domain name as the destination.
	IP Object / IP Group– Use the drop down list to choose a preconfigured IP object/group.
	Country Object – Use the drop dwon list to choose a preconfigured object. Then all IPs within that country will be treated as the destination IP.
Destination Port	**Any** – Any port number can be treated as the destination port.
	Dest Port Range –
	● **Start -** Type the destination port start for the destination IP.
	● **End -** Type the destination port end for the destination IP. If this field is blank, it means that all the destination ports will be passed through the WAN interface.
Send via if criteria Matched	
Interface	Use the drop down list to choose a WAN or LAN interface or VPN profile. Packets match with the above criteria will be transferred to the interface chosen here.
Gateway	**Specific gateway** is used only when you want to forward the packets to the desired gateway. Usually, Default Gateway is selected in default.
Packet Forwarding to WAN via	When you choose WAN (e.g., WAN1) as the Interface for packet transmission, you have to specify the way the packet forwarded to. Choose **Force NAT** or **Force Routing**.
Failover to	Check this button to lead the data passing through specific interface (WAN/LAN/VPN/Route Policy) automatically when the selected interface (defined in **Send via if criteria matched**) is down.
	● **WAN/LAN –** Use the drop down list to choose an interface as an auto failover interface.
	● **VPN –** Use the drop down list to choose a VPN tunnel as a failover tunnel.
	● **Route Policy –** Use the drop down list to choose an existed route policy profile.
Priority	

Priority	Packets will be transmitted based on all routes or Route Policy. Vigor router will determine which rule will be adopted for transmitting the packet according to the priority of Static Route and Route Policy.
	The greater the value is, the lower the priority is. Default value for route policy is "200" which means it has higher priority than the default route.

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

Routing >> Load-Balance/Route Policy

Load-Balance/Route Policy   10 ▾ rules per page | Set to Factory Default | Diagnose |

Index	Enable	Comment	Protocol	Interface	Priority	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End	Move Up	Move Down
1	☑		Any	WAN1	200	Any	Any	Any	Any	Any	Any		Down
2	☑	test	TCP/UDP	WAN1	200	172.16.0.0	172.16.255.255	192.168.1.61	192.168.1.66	Any	Any	UP	Down
3	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
4	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
5	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
6	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
7	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
8	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
9	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
10	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down

<< 1-10 | 11-20 | 21-30 | 31-40 | 41-50 | 51-60 | 61-70 | 71-80 | 81-90 | 91-100 | 101-110 | 111-120 | 121-130 | 131-140 | 141-150 | 151-160 | 161-170 | 171-180 | 181-190 | 191-200 | 201-210 | 211-220 | 221-230 | 231-240 | 241-250 >>   Next >>

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

OK

II-6-2-2 Diagnose for Route Policy

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

Click the **Diagnose** link on **Routing>>Load-Balance/Route Policy** or the **Diagnose** button on the configuration page based on **Advanced Mode**.

Diagnostics >> Route Policy Diagnosis

Test how the packets will be routed

Mode   ◉ Analyze a single packet
       ○ Analyze multiple packets by uploading an input file

Packet Information
Protocol   ICMP ▾
Src IP   Specify an IP ▾   192.168.1.2
Dst IP   Specify an IP ▾   192.168.1.11
Dst Port   Any Port ▾

Analyze

Analysis

the packet   →   LAN   Vigor3910   LAN1   →   The packet was sent via LAN1 according to the Static route "192.168.1.0/255.255.255.0 LAN1"

Matched Route

Matched	Priority
192.168.1.0/255.255.255.0 LAN1	150

Matched Policy

Matched	Priority	failovered
Route Policy 1	200	No

or

Load-Balance/Route Policy >> Diagnose

Test how the packets will be routed

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

Input File
選擇檔案 未選擇任何檔案   (**download** an example input file)

Analyze

Available settings are explained as follows:

Item	Description
Mode	**Analyze how a packet will be sent** – Choose such mode to make Vigor router analyze how a single packet will be sent by a route policy. **Analyze how multiple packets**... - Choose such mode to make Vigor router analyze how multiple packets in a specified file will be sent by a route policy.
Packet Information	Specify the nature of the packets to be analyzed by Vigor router. **ICMP/UDP/TCP/ANY**- Specify a protocol for diagnosis. **Src IP** – Type an IP address as the source IP. **Dst IP** – Type an IP address as the destination IP. **Dst Port** – Use the drop down list to specify the destination port. **Analyze** – Click it to perform the job of analyzing. The analyzed result will be shown on the page. If required, click **export analysis** to export the result as a file.
Input File	**Select** – Click the download link to get a blank example file. Then, click such button to select that blank ".csv" file for saving the result of analysis. **Analyze** – Click it to perform the job of analyzing. The analyzed result will be shown on the page. If required, click **export analysis** to export the result as a file.

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

II-6-3 OSPF

OSPF(Open Shortest Path First), running within the AS, is a routing protocol based on IP protocol. It uses the algorithm of SPF (Shortest Path First) to calculate the route metric. It is suitable for large network and complicated data exchange. Vigor3910 supports up to OSPF version 2(only for IPv4).

The Autonomous System (AS) used in OSPF can be divided into several **areas**. Usually, Area 0 will be used as OSPF backbone which distributing the routing information among areas.

When you need faster convergence than distance vector, want to support much larger networks or want to have less susceptible to bad routing information, you can enable OSPF feature to fit your request. Note that both routers must support OSPF function at the same time to build the OSPF connection.

Open **Routing** >> **OSPF** to get the following page.

Available settings are explained as follows:

Item	Description
Local	
Enable OSPF	Check the box to enable the function.

Profile	
Enable	Check it to enable and configure an OSPF profile.
Index	1 to 8 indicates profile 1 to profile 8.
Interface	Choose a LAN / WAN interface to apply the settings configured for this profile.
Area	An AS will be divided into several areas. Each area must be assigned with a dedicated number.
MD5 Auth	Enable/disable the MD5 authentication mechanism for such profile.
Password	Enter characters as the password for MD5 authentication.
Key ID (1-255)	Specify the IP address of such Vigor router. Such ID will help Vigor router to be identified in an autonomous system. However, if no address is specified, then an IP address of the active interface will be used by system automatically.
Neighborhoods	Displays current neighbors status in BGP routing environment.

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

II-6-4 BGP

BGP means Border Gateway Protocol. It is a standardized exterior gateway protocol which can exchange routing and reachability information between autonomous systems (AS) on Internet.

The protocol TCP is used by two routers supporting BGP for data transmission. They can exchange the BGP routing information for each other. A BGP router is the "neighbor" of other BGP routers. Define the IP address, AS number for the router is essential for TCP connection of BGP routing information exchange.

AS, the abbreviation of Autonomous System, is a group interconnected with multiple IP addresses. Each AS shall be assigned with one AS number (ASN). The ASN is is a unique identifier for AS to distinguish each network group in the whole interconnected network. It can be operated by one or several ISPs and follows the routing policies made by ISP.
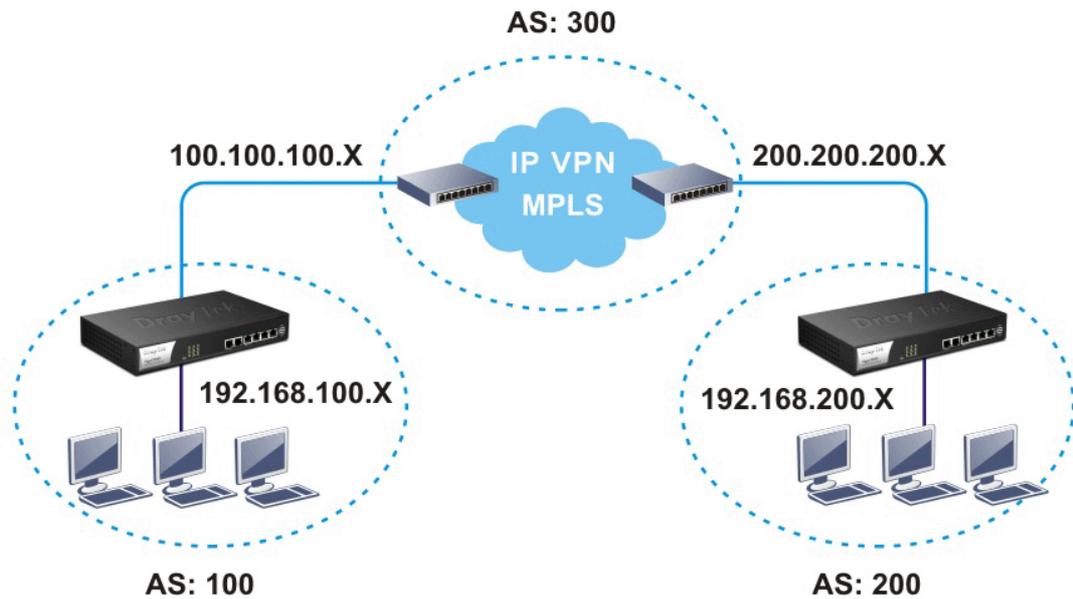
II-6-4-1 Basic Settings

Set general settings for for local router and neighboring routers.

Available settings are explained as follows:

Item	Description
Local	
Enable BGP	Check the box to enable basic BGP function for local router.
Local AS Number	Set the AS number for local router.
Hold Time	Set the time interval (in seconds) to determine the peer is dead when the router is unable to receive any keepalive message from the peer within the time.
Connect Retry Time	If the router fails to connect to neighboring router, it requires a period of time to reconnect. Set the time interval to do reconnection.
Router ID	Specify the LAN subnet for the router.
Neighbor	
Index	Click the index number link to configure neighbor profile.
Enable	Check the box to enable the basic BGP function for neighboring router.
AS Number	Display the AS Number for neighboring router.
Profile Name	Display the name of the neighboring profile.
IP Address	Display the IP address specified for the neighboring profile.
MD5 Auth	Display the status (enable or disable) of MD5 Auth.
Status	Display the connection status for local router and neighboring router.

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

II-6-4-2 Static Network

This page allows you to configure up to eight neighboring routers for exchanging the routing information with the local router.

Routing >> BGP

	Basic Settings		Static Network		View Routing Table	
Select	Index	IP Address	Subnet Mask
☐	1		255.255.255.254 / 31 ▾
☐	2		255.255.255.254 / 31 ▾
☐	3		255.255.255.254 / 31 ▾
☐	4		255.255.255.254 / 31 ▾
☐	5		255.255.255.254 / 31 ▾
☐	6		255.255.255.254 / 31 ▾
☐	7		255.255.255.254 / 31 ▾
☐	8		255.255.255.254 / 31 ▾
☐	9		255.255.255.254 / 31 ▾
☐	10		255.255.255.254 / 31 ▾
☐	11		255.255.255.254 / 31 ▾
☐	12		255.255.255.254 / 31 ▾
☐	13		255.255.255.254 / 31 ▾
☐	14		255.255.255.254 / 31 ▾
☐	15		255.255.255.254 / 31 ▾
☐	16		255.255.255.254 / 31 ▾

Available settings are explained as follows:

Item	Description
Select	Check the box to enable the configuration for the selected index entry.
IP Address	Enter the IP address for a router.
Subnet Mask	Choose the mask value for the IP address.

Application Notes

A-1 How to Customize a Secure Route between VPN Router and Remote Router by Using Route Policy

Example 1:

In the following figure, a LAN to LAN VPN tunnel is built between DrayTek VPN router (e.g., Vigor3910 Series) and the remote router. Firewall Router can receive all of the traffic coming from remote PC which wants to access into Internet; and send back the packets to Remote Router through VPN Router.
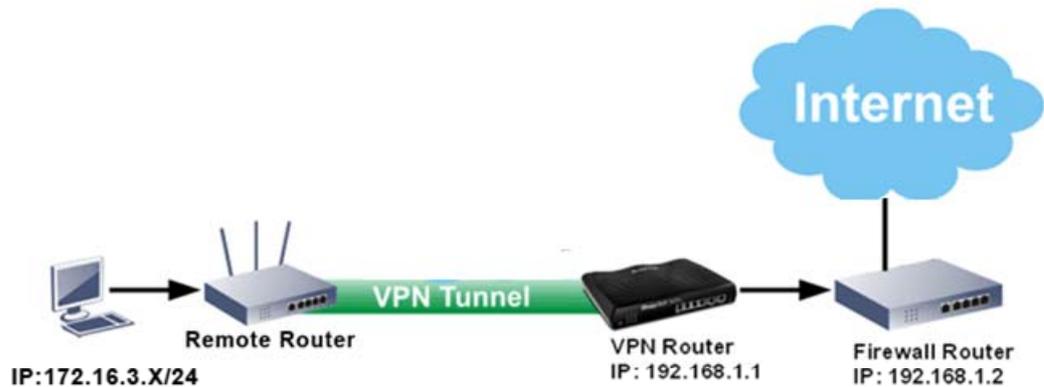
1. Establish a **VPN tunnel** between VPN Router and the Remote Router.

2. Change to default route for the router located in Remote Router.

3. Access into the web user interface of the router in VPN Router. Then, open **Routing >> Load-Balance / Route Policy** and click **Advance Mode.**

4. Click any **Index** number link (e.g., 1 in this case). Configure the settings as follows.

Now, if you want such route policy will be applied by Vigor router with higher priority, please adjust the value of **Priority** for such route policy. In general, default route is specified with the lowest priority for it value is fixed as "250". And Routes in Routing Table are fixed as "150". You can adjust the value for such route policy with lower value, e.g., 100 to ensure it will be applied to packets transmission with the highest priority.

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

6. To route the packets coming from the Firewall Router back to the remote router, access into the web user interface of the Firewall Router. Then, set "192.168.1.1/24" as the gateway IP address and set "172.16.3.0/24" as the destination IP address.

Example 2:

Below shows a scenario that local users behind Vigor router A want to access into a remote service (e.g., YouTube) which is blocked or restricted by local Service Provider in area with restrictions. A policy route can be created by the side of Router A to break through the Internet censorship circumvention.
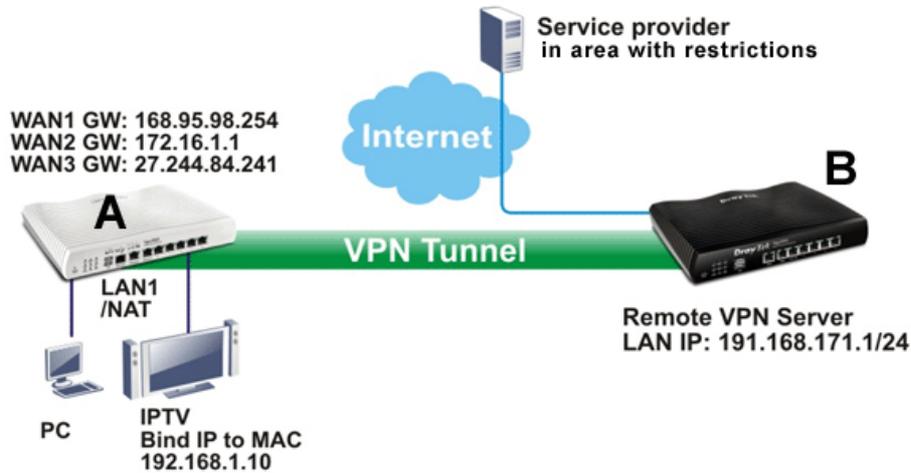
A VPN tunnel has been established between Router A and router B.

1. Access into the web user interface of Router A.

2. Open **Routing** >> **Load-Balance/Route Policy** and click **Advance Mode**.

3. Click any index number (e.g., #1 in this case).

4. In the following web page, check **Enable**; type "192.168.1.10" as **Src IP Range**; type "213.57.89.100" as the **Destination IP** for the remote VPN server; and choose VPN as the **Interface** setting.

5. Click **OK** to save the settings.

This page is left blank.

Part III VPN

VPN

A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link.

SSL VPN

It is a form of VPN that can be used with a standard Web browser.

Certificate Management

A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Here Vigor router support digital certificates conforming to standard X.509.

III-1 VPN and Remote Access

A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link.

The VPN built is suitable for:

● Communication between home office and customer

● Secure connection between Teleworker, staff on business trip and main office

● Exchange data between remote office and main office

● POS between chain store and headquarters

Web User Interface

III-1-1 Remote Access Control

Enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should disable the VPN service of Vigor Router to allow VPN tunnel pass through, as well as the appropriate NAT settings, such as DMZ or open port.
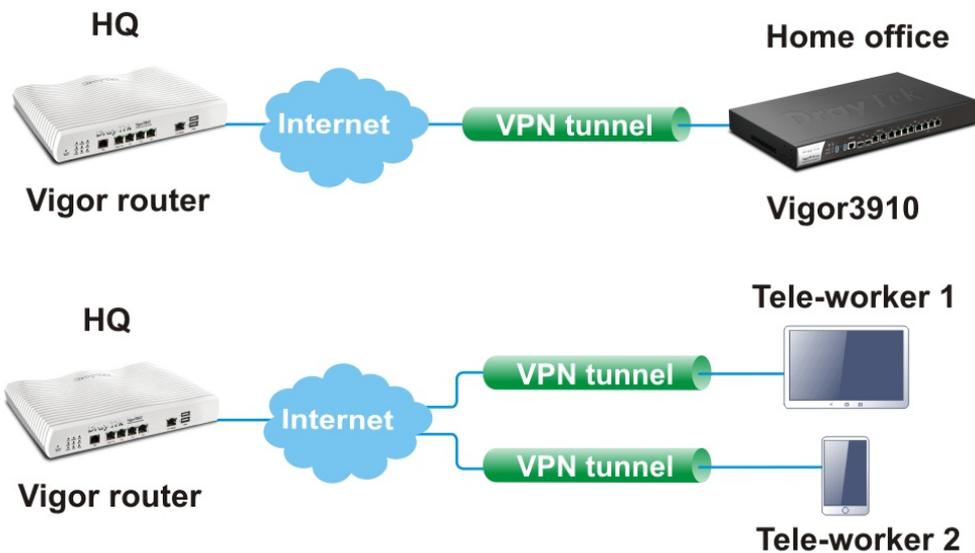
VPN and Remote Access >> Remote Access Control Setup

Remote Access Control Setup

☑ Enable PPTP VPN Service
☑ Enable IPsec VPN Service
☑ Enable L2TP VPN Service
☑ Enable SSL VPN Service
☑ Enable OpenVPN Service

Note:
To allow VPN pass-through to a separate VPN server on the LAN, disable any services above that use the same protocol and ensure that NAT Open Ports or Port Redirection is also configured.

OK   Clear   Cancel

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

III-1-2 PPP General Setup

This submenu only applies to PPP-related VPN connections, such as PPTP, L2TP, L2TP over IPsec.

Available settings are explained as follows:

Item	Description
Dial-In PPP Authentication	**PAP Only** - elect this option to force the router to authenticate dial-in users with the PAP protocol.
	PAP/CHAP/MS-CHAP/MS-CHAPv2 - Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication.
Dial-In PPP Encryption (MPPE)	**Optional MPPE** - This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit "no MPPE encrypted packets". Otherwise, the MPPE encryption scheme will be used to encrypt the data.
	● **Require MPPE (40/128bits) -** Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data.
	● **Maximum MPPE -** This option indicates that the router will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.
Mutual Authentication (PAP)	The Mutual Authentication function is mainly used to communicate with other routers or clients who need

	bi-directional authentication in order to provide stronger security, for example, Cisco routers. So you should enable this function when your peer router requires mutual authentication. You should further specify the **User Name** and **Password** of the mutual authentication peer.
	The length of the name/password is limited to 23/19 characters.
IP Address Assignment for Dial-In Users	Enter a start IP address for the dial-in PPP connection. You should choose an IP address from the local private network. For example, if the local private network is 192.168.1.0/255.255.255.0, you could choose 192.168.1.200 as the Start IP Address.
PPP Authentication Methods	Select the method(s) to be used for authentication in PPP connection.
While using Radius or LDAP Authentication	If PPP connection will be authenticated via RADIUS server or LDAP profiles, it is necessary to specify the LAN profile for the dial-in user to get IP from.

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

III-1-3 IPsec General Setup

In **IPsec General Setup**, there are two major parts of configuration.

There are two phases of IPsec.

● Phase 1: negotiation of IKE parameters including encryption, hash, Diffie-Hellman parameter values, and lifetime to protect the following IKE exchange, authentication of both peers using either a Pre-Shared Key or Digital Signature (x.509). The peer that starts the negotiation proposes all its policies to the remote peer and then remote peer tries to find a highest-priority match with its policies. Eventually to set up a secure tunnel for IKE Phase 2.

● Phase 2: negotiation IPsec security methods including Authentication Header (AH) or Encapsulating Security Payload (ESP) for the following IKE exchange and mutual examination of the secure tunnel establishment.

There are two encapsulation methods used in IPsec, **Transport** and **Tunnel**. The **Transport** mode will add the AH/ESP payload and use original IP header to encapsulate the data payload only. It can just apply to local packet, e.g., L2TP over IPsec. The **Tunnel** mode will not only add the AH/ESP payload but also use a new IP header (Tunneled IP header) to encapsulate the whole original IP packet.

Authentication Header (AH) provides data authentication and integrity for IP packets passed between VPN peers. This is achieved by a keyed one-way hash function to the packet to create a message digest. This digest will be put in the AH and transmitted along with packets. On the receiving side, the peer will perform the same one-way hash on the packet and compare the value with the one in the AH it receives.

Encapsulating Security Payload (ESP) is a security protocol that provides data confidentiality and protection with optional authentication and replay detection service.

VPN and Remote Access >> IPsec General Setup

VPN IKE/IPsec General Setup
(Dial-in settings for Remote Dial-In users and LAN-to-LAN VPN Client with Dynamic IP.)

IKE Authentication Method

Certificate	None ▼
Preferred Local ID	Alternative Subject Name ▼
General Pre-Shared Key	Max: 64 characters
Confirm General Pre-Shared Key	
XAuth User Pre-Shared Key	Max: 64 characters
Confirm XAuth User Pre-Shared Key	

IPsec Security Method

○ Basic   ○ Medium   ○ High
Encryption: AES/3DES/DES
HMAC: SHA256/SHA1/MD5
DH Group: G21/G20/G19/G14/G5/G2/G1
AH: ☑ Enable

[OK] [Cancel]

Available settings are explained as follows:

Item	Description
IKE Authentication Method	This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPsec-related VPN connections such as L2TP over IPsec and IPsec tunnel. There are two methods offered by Vigor router for you to authenticate the incoming data coming from remote dial-in user, **Certificate (X.509)** and **Pre-Shared Key**.
	Certificate – X.509 certificates can be used for IKE authentication. To set up certificates on the router, go to the Certificate Management section.
	Preferred Local ID - Specify the preferred local ID information (**Alternative Subject Name First** or **Subject Name First**) for IPsec authentication while the client is using the general setting (without a specific Peer IP or ID in the VPN profile).
	General Pre-Shared Key- Define the PSK key for general authentication.
	Confirm General Pre-Shared Key- Re-enter the characters to confirm the pre-shared key.
	XAuth User Pre-Shared Key - Define the PSK key for IPsec XAuth authentication.
	Confirm XAuth User Pre-Shared Key- Re-enter the characters to confirm the pre-shared key for IPsec XAuth authentication.
	Note: Any packets from the remote dial-in user which does not match the rule defined in **VPN and Remote Access>>Remote Dial-In User** will be applied with the method specified here.
IPsec Security Method	Available mthods include **Basic**, **Medium** and **High**. Each method offers different encryption, HMAC and DH Group.
	Basic - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.
	Medium - When this option is selected, the Authentication Header (AH) protocol can be used to provide authentication to IPsec traffic.
	High - When this option is selected, the Encapsulating Security Payload (ESP) protocol can be used to provide authentication and encryption to IPsec traffic. Three encryption standards are supported for ESP: DES, 3DES and AES, in ascending order of security.

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

III-1-4 IPsec Peer Identity

To use digital certificate for peer authentication in either LAN-to-LAN connection or Remote User Dial-In connection, here you may edit a table of peer certificate for selection. As shown below, the router provides 500 entries of digital certificates for peer dial-in users.

Available settings are explained as follows:

Item	Description
Set to Factory Default	Click it to clear all indexes.
Index	Click the number below Index to access into the setting page of IPsec Peer Identity.
Enable	Check the box to enable such profile.
Name	Display the profile name of that index.

Click each index to edit one peer digital certificate. There are three security levels of digital signature authentication: Fill each necessary field to authenticate the remote peer. The following explanation will guide you to fill all the necessary fields.

Available settings are explained as follows:

Item	Description
Enable this account	Check it to enable such account profile.
Profile Name	Type the name of the profile. The maximum length of the name you can set is 32 characters.
Accept Any Peer ID	Click to accept any peer regardless of its identity.
Accept Subject Alternative Name	Click to check one specific field of digital signature to accept the peer with matching value. The field can be **IP Address**, **Domain**, or **E-mail** address. The box under the Type will appear according to the type you select and ask you to fill in corresponding setting.
Accept Subject Name	Click to check the specific fields of digital signature to accept the peer with matching value. The field includes **Country (C)**, **State (ST)**, **Location (L)**, **Organization (O)**, **Organization Unit (OU)**, **Common Name (CN)**, and **Email (E)**.

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

III-1-5 OpenVPN

OpenVPN offers a convenient way for users to build VPN between local end and remote end.

With integrating of OpenVPN, Vigor router can help users to achieve more robust, reliable and secure private connections for business needs.

There are two advantages of OpenVPN:

- It can be operated on different systems such as Windows, Linux, and MacOS.

- Based on the standard protocol of SSL encryption, OpenVPN can provide you with a scalable client/server mode, permitting multi-client to connect to a single OpenVPN Server process over a single TCP or UDP port.

III-1-5-1 General Setup

Before establishing OpenVPN connection, general settings for OpenVPN service shall be configured first.

VPN and Remote Access >> OpenVPN

| General Setup | Client Config |

☑ Enable UDP
UDP Port   1194
☑ Enable TCP
TCP Port   1194
Cipher Algorithm   AES128 ▼
HMAC Algorithm   SHA1 ▼
Certificate Authentication ☐

Note: OpenVPN on vigor only support **TUN** device interface currently. So please setup corresponding configurations on the client side.

OK

Available settings are explained as follows:

Item	Description
Enable UDP	Check the box to enable UDP port setting for OpenVPN. **UDP Port** – Enter a number.
Enable TCP	Check the box to enable TCP port setting for OpenVPN. **TCP Port** – Enter a number.
Cipher Algorithm	Two encryptions are supported, AES128 and AES256.
HMAC Algorithm	The HMAC algorithm only supports SHA1/SHA256.
Certificate Authentication	If certificate authentication is required for OpenVPN, simply check the box to apply the trusted CA certificate and local certificate for OpenVPN tunnel. Certificate authentication can offer more secure VPN tunnel between the client and the router.

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

III-1-5-2 Client Config

The settings on this page can be downloaded as a file. Later, such file can be imported and applied to remote end's CPE (as VPN client). Then, a private connection via OpenVPN tunnel between the server and the client can be connected successfully.

Available settings are explained as follows:

Item	Description
Remote Server	Click **IP** and use the drop down list to specify an IP address of WAN for VPN connection. Or click **Domain** to enter a domain name for the remote server.
Transport Protocol	Simply choose UDP or TCP as protocol for building OpenVPN connection between the server and the remote client.
Fine Name	Enter a name for the configuration file.
CA cert	Enter the certificate authority (CA) file name obtained from 3rd party provider
Client cert	Each client in an OpenVPN connection must have its certificate and private key. Enter the certificate file name obtained from 3rd party provider
Client key	Enter the private key file name obtained from 3rd party provider
Export	The settings in this page can be saved as a file after clicking such button. Later, the downloaded file can be imported to the VPN client for building OpenVPN connection.

III-1-6 Remote Dial-in User

You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in via VPN connection. You may set parameters including specified connection peer ID, connection type (VPN connection - including PPTP, IPsec Tunnel, and L2TP by itself or over IPsec) and corresponding security methods, etc.

The router provides 500 access accounts for dial-in users. Besides, you can extend the user accounts to the RADIUS server through the built-in RADIUS client function. The following figure shows the summary table.

Available settings are explained as follows:

Item	Description
Set to Factory Default	Click to clear all indexes.
View	**All** – Click it to display the all of the user accounts.
	Online – Click it to display the online user accounts.
	Offline – Click it to display the offline user accounts.
Index	Click the number below Index to access into the setting page of Remote Dial-in User.

Enable	Check the box to activate such profile.
User	Display the username for the specific dial-in user of the LAN-to-LAN profile. The symbol **???** represents that the profile is empty.
Status	Display the access state of the specific dial-in user.

Click each index to edit one remote user profile. **Each Dial-In Type requires you to fill the different corresponding fields on the right.** If the fields gray out, it means you may leave it untouched. The following explanation will guide you to fill all the necessary fields.

Available settings are explained as follows:

Item	Description
User account and Authentication	**Enable this account** - Select to enable this profile to be used by remote dial-in users. **Idle Timeout** - Allowed idle time before the router disconnects the VPN connection. Default timeout value is 300 seconds.
Allowed Dial-In Type	Select all VPN protocols allowed for this profile. For L2TP, specify how IPsec should be applied. Options are **None** – IPsec cannot be used with L2TP connections. ● **Nice to Have** – IPsec is preferred but not mandatory for L2TP connections.

	● **Must** – IPsec is required when establish L2TP connections. **Specify Remote Node** - The IP address of the remote VPN client (Remote Client IP) or the Peer ID (used in IKE aggressive mode) can be optionally specified. The router will reject the connection if either of these values are entered in the profile but the remote client does not pass the value, or passes the wrong value. **Netbios Naming Packet -** Specifies whether to allow NetBIOS naming packets to traverse through the VPN tunnel. ● **Pass** - Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. ● **Block** – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel. **Multicast via VPN** - Specifies whether to allow multicast packets to traverse through the VPN tunnel. ● **Pass** - Click this button to let multicast packets pass through the router. ● **Block** – This is default setting. Click this button to let multicast packets be blocked by the router.
Subnet	The VPN client will receive an IP address from the DHCP pool or IP address range specified in IP Address Assignment for Dial-In Users for the selected LAN subnet. **Assign Static IP Address** – Alternatively, a static IP address can be set by selecting the Assign Static IP Address checkbox. **User Name** - Used for PPTP, L2TP or SSL Tunnel dial-in type. The length of the name is limited to 23 characters. **Password** - Used for PPTP, L2TP or SSL Tunnel dial-in type. The length of the password is limited to 19 characters. **Enable Mobile One-Time Passwords (mOTP) -** Select to enable one-time passwords (Mobile-OTP). Enter the PIN Code and Secret. DrayTek's SmartVPN client has built-in support for mOTP. Third-party mOTP clients can be used to generate passwords when using other VPN clients. For more information on mOTP, visit Mobile-OTP's homepage. ● **PIN Code** - Enter the code for authentication (e.g, 1234). ● **Secret** – Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).
IKE Authentication Method	**Pre-Shared Key** - This checkbox is available when Remote Client IP or Peer ID is specified. Check the checkbox and click IKE Pre-shared Key to enter an IKE PSK (1~63 characters) that will be used only for this profile. **Digital Signature (X.509) –** To enable authentication using X.509 Peer IDs, check the checkbox then select an X.509 profile. X.509 profiles can be configured in **VPN and Remote Access >> IPsec Peer Identity**.
IPsec Security Method	Select all the IPsec protocols that are allowed to be used for this profile. **Medium-Authentication Header (AH)** means data will be authenticated, but not be encrypted. By default, this option

is invoked. You can uncheck it to disable it.

High (ESP) - High-Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

Local ID (Optional)- Specify a local ID to be used when establishing a LAN-to-LAN VPN connection using IKE aggressive mode.

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

III-1-7 LAN to LAN

Here you can manage LAN-to-LAN connections by maintaining a table of connection profiles. You may set parameters including specified connection direction (dial-in or dial-out), connection peer ID, connection type (VPN connection - including PPTP, IPsec Tunnel, and L2TP by itself or over IPsec) and corresponding security methods, etc.

The following figure shows the summary table according to the item (All/Trunk/Online/Offline) selected for **View**.

Available settings are explained as follows:

Item	Description
Set to Factory Default	Click to clear all indexes.
View	**All –** Shows all LAN-to-LAN VPN profiles. **Trunk –** Shows all Trunk profiles (see VPN and Remote Access >> VPN TRUNK Management).
Index	Click the index number of the profile to view or edit its settings.
Enable	Check to enable the LAN-to-LAN VPN profile.
Name	Display the name of the LAN-to-LAN profile. The symbol **???** represents that the profile is empty.
Remote Network	Display the name of the remote network.
Status	Shows the status of the profile. Online – LAN-to-LAN VPN is connected. Offline – LAN-to-LAN VPN is disconnected. --- – Profile is disabled.
Pass Routing LAN to VPN	Check the box to allow the packets from the Routing LAN to pass over the VPN tunnel. Default setting is "Disable".
Pass Packets to NAT when VPN disconnects	If enabled, the Vigor router will send the packets to the default gateway once the VPN disconnects. Default setting is "Enable".
Backup	Click **Backup** to save the configuration.
Restore	Click **Select** to choose a configuration file. Then click **Restore** to apply the file.

To edit each profile:

1. Click each index to edit each profile and you will get the following page. Each LAN-to-LAN profile includes 5 subgroups. If the fields gray out, it means you may leave it untouched. The following explanations will guide you to fill all the necessary fields.

Available settings are explained as follows:

Item	Description
Common Settings	**Profile Name** – Specify a name for the profile of the LAN-to-LAN connection. **Enable this profile** - Check here to activate this profile. **VPN Dial-Out Through** - Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only. ● **WANx First**- While connecting, the router will use WANx as the first channel for VPN connection. If WANx fails, the router will use another WAN interface instead. ● **WANx Only** - While connecting, the router will use WANx as the only channel for VPN connection. ● **WAN1 Only: Only establish VPN if WAN2 down** - If WAN2 failed, the router will use WAN1 for VPN connection. ● **WAN2 Only: Only establish VPN if WAN1 down** - If WAN1 failed, the router will use WAN2 for VPN connection. **Netbios Naming Packet** ● **Pass** – click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel

while connecting.

● **Block** – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.

Multicast via VPN - Some programs might send multicast packets via VPN connection.

● **Pass** – Click this button to let multicast packets pass through the router.

● **Block** – This is default setting. Click this button to let multicast packets be blocked by the router.

Call Direction - Specify the allowed call direction of this LAN-to-LAN profile.

● **Both**:-initiator/responder

● **Dial-Out**- initiator only

● **Dial-In**- responder only.

Tunnel Mode - At present, a tunnel (GRE tunnel) without encryption is offered to fit the requiarement of specific client.

Always On-Check to enable router always keep VPN connection.

Idle Timeout: The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.

Enable PING to keep alive - This function is to help the router to determine the status of IPsec VPN connection, especially useful in the case of abnormal VPN IPsec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address.

Enable PING to keep alive is used to handle abnormal IPsec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial. Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer disconnects without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection).

PING to the IP - Enter the IP address of the remote host that located at the other-end of the VPN tunnel.

Dial-Out Settings	**Type of Server I am calling - PPTP -** Build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server.
	IPsec Tunnel - Build an IPsec VPN connection to the server through Internet.
	L2TP with IPsec Policy - Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below:
	● **None:** Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec

policy can be viewed as one pure L2TP connection.

- **Nice to Have**: Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN connection becomes one pure L2TP connection.

- **Must**: Specify the IPsec policy to be definitely applied on the L2TP connection.

User Name - This field is applicable when you select, PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 49 characters.

Password - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 15 characters.

PPP Authentication - This field is applicable when you select, PPTP or L2TP with or without IPSec policy above. PAP/CHAP/MS-CHAP/MS-CHAPv2 is the most common selection due to compatibility.

VJ compression - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally set to **On** to improve bandwidth utilization.

IKE Authentication Method - This group of fields is applicable for IPsec Tunnels and L2TP with IPsec Policy.

- **Pre-Shared Key** - Input 1-63 characters as pre-shared key.

- **Digital Signature (X.509)** - Select one predefined Profiles set in the **VPN and Remote Access >>IPsec Peer Identity**.

  Peer ID - Select one of the predefined Profiles set in **VPN and Remote Access >>IPsec Peer Identity**.

  Local ID – Specify a local ID (**Alternative Subject Name First** or **Subject Name First**) to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.

- **Local Certificate –** Select one of the profiles set in **Certificate Management>>Local Certificate**.

IPsec Security Method - This group of fields is a must for IPsec Tunnels and L2TP with IPsec Policy.

- **Medium AH (Authentication Header)** means data will be authenticated, but not be encrypted. By default, this option is active.

- **High (ESP-Encapsulating Security Payload)-** means payload (data) will be encrypted and authenticated. Select from below:

- **DES without Authentication** -Use DES encryption algorithm and not apply any authentication scheme.

- **DES with Authentication-**Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.

- **3DES without Authentication-**Use triple DES encryption algorithm and not apply any authentication scheme.

- **3DES with Authentication-**Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.

- **AES without Authentication-**Use AES encryption algorithm and not apply any authentication scheme.

● **AES with Authentication**-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.

Advanced - Specify mode, proposal and key life of each IKE phase, Gateway, etc.

The window of advance setup is shown as below:

IKE phase 1 mode -Select from **Main** mode and **Aggressive** mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPsec session. However, the **Aggressive** mode is faster. The default value in Vigor router is Main mode.

● **IKE phase 1 proposal**-To propose the local available authentication schemes and encryption algorithms to the VPN peers, and get its feedback to find a match. Two combinations are available for Aggressive mode and nine for **Main** mode. We suggest you select the combination that covers the most schemes.

● **IKE phase 2 proposal**-To propose the local available algorithms to the VPN peers, and get its feedback to find a match. Three combinations are available for both modes. We suggest you select the combination that covers the most algorithms.

● **IKE phase 1 key lifetime**-For security reason, the lifetime of key should be defined. The default value is 28800 seconds. You may specify a value in between 900 and 86400 seconds.

● **IKE phase 2 key lifetime**-For security reason, the lifetime of key should be defined. The default value is 3600 seconds.   You may specify a value in between 600 and 86400 seconds.

● **Perfect Forward Secret (PFS)**-The IKE Phase 1 key will be reused to avoid the computation complexity in phase 2. The default value is inactive this function.

    Local ID-In **Aggressive** mode, Local ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters.

Schedule Profile - Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications** >> **Schedule** setup. The default setting of this field is blank and the function will always work.

Available settings are explained as follows:

Item	Description
Dial-In Settings	**Allowed Dial-In Type -** Determine the dial-in connection with different types. ● **PPTP -** Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below. ● **IPsec Tunnel-** Allow the remote dial-in user to trigger an IPsec VPN connection through Internet. ● **L2TP with IPsec Policy -** Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below: ■ **None -** Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection. ■ **Nice to Have -** Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. ■ **Must -** Specify the IPsec policy to be definitely applied on the L2TP connection. ● **SSL Tunnel-** Allow the remote dial-in user to trigger an SSL VPN connection through Internet. **Specify Remote VPN Gateway -** You can specify the IP address of the remote dial-in user or peer ID (should be the same with the ID setting in dial-in type) by checking the box.

	Also, you should further specify the corresponding security methods on the right side.
	If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings.
	User Name - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 11 characters.
	Password - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 11 characters.
	VJ Compression - VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select PPTP or L2TP with or without IPsec policy above.
	IKE Authentication Method - This group of fields is applicable for IPsec Tunnels and L2TP with IPsec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPsec tunnel either with or without specify the IP address of the remote node.
	● **Pre-Shared Key** - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key.
	● **Digital Signature (X.509)** –Check the box of Digital Signature to invoke this function and select one predefined Profiles set in the **VPN and Remote Access >>IPsec Peer Identity**.
	■ **Local ID** – Specify which one will be inspected first.
	■ **Alternative Subject Name First** – The alternative subject name (configured in **Certificate Management>>Local Certificate**) will be inspected first.
	■ **Subject Name First** – The subject name (configured in **Certificate Management>>Local Certificate**) will be inspected first.
	IPsec Security Method - This group of fields is a must for IPsec Tunnels and L2TP with IPsec Policy when you specify the remote node.
	● **Medium-** Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.
	● **High-** Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
GRE over IPsec Settings	**Enable IPsec Dial-Out function GRE over IPsec:** Check this box to verify data and transmit data in encryption with GRE over IPsec packet after configuring IPsec Dial-Out setting. Both ends must match for each other by setting same virtual IP address for communication.
	Logical Traffic: Such technique comes from RFC2890. Define logical traffic for data transmission between both sides of VPN tunnel by using the characteristic of GRE. Even hacker can decipher IPsec encryption, he/she still cannot ask LAN site to do data transmission with any information. Such

	function can ensure the data transmitted on VPN tunnel is really sent out from both sides. This is an optional function. However, if one side wants to use it, the peer must enable it, too.
	My GRE IP: Type the virtual IP for router itself for verified by peer.
	Peer GRE IP: Type the virtual IP of peer host for verified by router.
TCP/IP Network Settings	**My WAN IP –**This field is only applicable when you select PPTP or L2TP with or without IPsec policy above. The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.
	Remote Gateway IP - This field is only applicable when you select PPTP or L2TP with or without IPsec policy above. The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.
	Remote Network IP/ Remote Network Mask - Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPsec, this is the destination clients IDs of phase 2 quick mode.
	Local Network IP / Local Network Mask - Display the local network IP and mask for TCP / IP configuration. You can modify the settings if required.
	More - Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Masks through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.
	192.168.1.1/doc/l2lMRt.htm **Profile Index :1** Network IP Netmask 255.255.255.255 / 32 ▼ Remote Network Add Delete Edit ☐ Create Phase2 SA for each subnet.(IPsec) OK Close
	RIP Direction - The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable.
	From first subnet to remote network, you have to do - If the remote network only allows you to dial in with single IP,
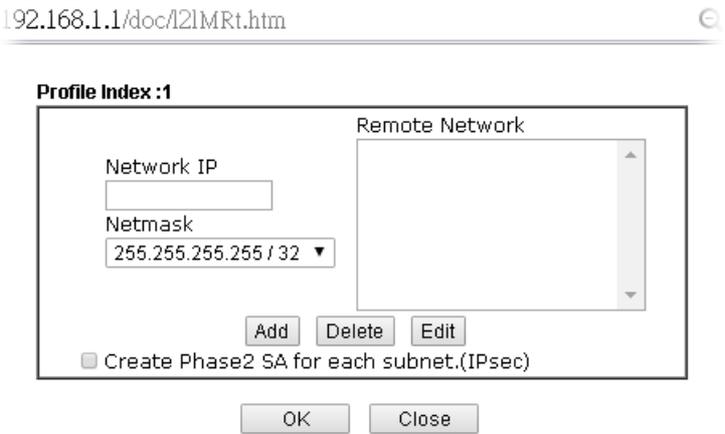
	please choose **NAT**, otherwise choose **Route**.
	Change default route to this VPN tunnel - Check this box to change the default route with this VPN tunnel.
IPSec VPN with the Same subnet	For both ends (e.g., different sections in a company) are within the same subnet, there is a function which allows you to build Virtual IP mapping between two ends. Thus, when VPN connection established, the router will change the IP address according to the settings configured here and block sessions which are not coming from the IP address defined in the Virtual IP Mapping list.
	After checking the box of **IPSec VPN with the Same subnet**, the options under **TCP/IP Network Settings** will be changed as shown below:
	Remote Network IP/ Remote Network Mask - Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPSec, this is the destination clients IDs of phase 2 quick mode.
	Translated Local Network – This function is enabled in default. Use the drop down list to specify a LAN port as the transferred direction. Then specify an IP address. Click **Advanced** to configure detailed settings if required.
	Advanced – Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.

Translated Type – There are two types for you to choose.
- **Whole Subnet**
- **Specific IP Address**

Virtual IP Mapping – A pop up dialog will appear for you to specify the local IP address and the mapping virtual IP address.
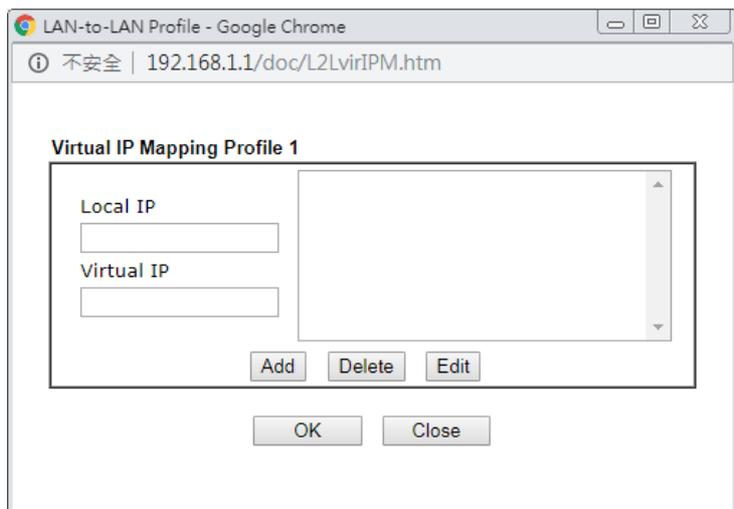
2. After finishing all the settings here, please click **OK** to save the configuration.

III-1-8 VPN Trunk Management

VPN trunk includes four features - VPN Backup, VPN load balance, GRE over IPsec, and Binding tunnel policy.

Features of VPN TRUNK – VPN Backup Mechanism

VPN TRUNK Management is a backup mechanism which can set multiple VPN tunnels as backup tunnel. It can assure the network connection not to be cut off due to network environment blocked by any reason.

● VPN TRUNK-VPN Backup mechanism can judge abnormal situation for the environment of VPN server and correct it to complete the backup of VPN Tunnel in real-time.

● VPN TRUNK-VPN Backup mechanism is compliant with all WAN modes (single/multi)

● Dial-out connection types contain IPsec, PPTP, L2TP, L2TP over IPsec and ISDN (depends on hardware specification)

● The web page is simple to understand and easy to configure

● Fully compliant with VPN Server LAN Site Single/Multi Network

● Mail Alert support, please refer to **System Maintenance >> SysLog / Mail Alert** for detailed configuration

● Syslog support, please refer to **System Maintenance >> SysLog / Mail Alert** for detailed configuration

● Specific ERD (Environment Recovery Detection) mechanism which can be operated by using Telnet command

VPN TRUNK-VPN Backup mechanism profile will be activated when initial connection of single VPN tunnel is off-line. Before setting VPN TRUNK -VPN Backup mechanism backup profile, please configure at least two sets of LAN-to-LAN profiles (with fully configured dial-out settings) first, otherwise you will not have selections for grouping Member1 and Member2.

Features of VPN TRUNK – VPN Load Balance Mechanism

VPN Load Balance Mechanism can set multiple VPN tunnels for using as traffic load balance tunnel. It can assist users to do effective load sharing for multiple VPN tunnels according to real line bandwidth. Moreover, it offers three types of algorithms for load balancing and binding tunnel policy mechanism to let the administrator manage the network more flexibly.

● Three types of load sharing algorithm offered, Round Robin, Weighted Round Robin and Fastest

● Binding Tunnel Policy mechanism allows users to encrypt the data in transmission or specified service function in transmission and define specified VPN Tunnel for having effective bandwidth management

● Dial-out connection types contain IPsec, PPTP, L2TP, L2TP over IPsec and GRE over IPsec

● The web page is simple to understand and easy to configure

● The TCP Session transmitted by using VPN TRUNK-VPN Load Balance mechanism will not be lost due to one of VPN Tunnels disconnected. Users do not need to reconnect with setting TCP/UDP Service Port again. The VPN Load Balance function can keep the transmission for internal data on tunnel stably

VPN and Remote Access >> VPN TRUNK Management

Backup Profile List | **Set to Factory Default** |

Note: [Active:NO] The LAN-to-LAN Profile is disabled or under Dial-In(Call Direction) at present.

```
No. Status Name          Member1(Active)Type        Member2(Active)Type
```

[Advanced] [▼]

Load Balance Profile List | **Set to Factory Default** |

Note: [Active:NO] The LAN-to-LAN Profile is disabled or under Dial-In(Call Direction) at present.

```
No. Status Name          Member1(Active)Type        Member2(Active)Type
```

[Advanced] [▼]

General Setup

Status	⊙ Enable ○ Disable
Profile Name	[_____]
Member1	Please select a LAN-to-LAN Dial-Out profile. ▼
Member2	Please select a LAN-to-LAN Dial-Out profile. ▼
Active Mode	⊙ Backup ○ Load Balance

[Add] [Update] [Delete]

Available settings are explained as follows:

Item	Description
Backup Profile List	**Set to Factory Default** - Click to clear all VPN TRUNK-VPN Backup mechanism profile.
	No – The order of VPN TRUNK-VPN Backup mechanism profile.
	Status - "v" means such profile is enabled; "x" means such profile is disabled.
	Name - Display the name of VPN TRUNK-VPN Backup mechanism profile.
	Member1 - Display the dial-out profile selected from the Member1 drop down list below.
	Active - "Yes" means normal condition. "No" means the state might be disabled or that profile currently is set with Dial-in mode (for call direction) in LAN-to-LAN.
	Type - Display the connection type for that profile, such as IPsec, PPTP, L2TP, L2TP over IPsec (NICE), L2TP over IPsec(MUST) and so on.
	Member2 - Display the dial-out profile selected from the Member2 drop down list below.
	Advanced – This button is available only when LAN to LAN profile (or more) is created.
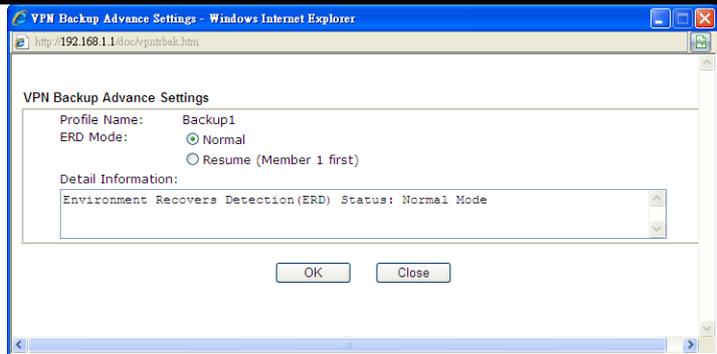
Detailed information for this dialog, see later section - **Advanced Load Balance and Backup**.

Load Balance Profile List	**Set to Factory Default -** Click to clear all VPN TRUNK-VPN Load Balance mechanism profile.
	No - The order of VPN TRUNK-VPN Load Balance mechanism profile.
	Status - "v" means such profile is enabled; "x" means such profile is disabled.
	Name - Display the name of VPN TRUNK-VPN Load Balance mechanism profile.
	Member1 - Display the dial-out profile selected from the Member1 drop down list below.
	Active - "Yes" means normal condition. "No" means the state might be disabled or that profile currently is set with Dial-in mode (for call direction) in LAN-to-LAN.
	Type - Display the connection type for that profile, such as IPsec, PPTP, L2TP, L2TP over IPsec (NICE), L2TP over IPsec(MUST) and so on.
	Member2 - Display the dial-out profile selected from the Member2 drop down list below.
	Advanced – This button is only available when there is one or more profiles created in this page.
	Detailed information for this dialog, see later section - **Advanced Load Balance and Backup**.

General Setup	**Status**- After choosing one of the profile listed above, please click **Enable** to activate this profile. If you click **Disable**, the selected or current used VPN TRUNK-Backup/Load Balance mechanism profile will not have any effect for VPN tunnel.
	Profile Name- Type a name for VPN TRUNK profile. Each profile can group two VPN connections set in LAN-to-LAN. The saved VPN profiles in LAN-to-LAN will be shown on Member1 and Member2 fields. The length of the name is limited to 11 characters.
	Member 1/Member2 - Display the selection for LAN-to-LAN dial-out profiles (configured in **VPN and Remote Access >> LAN-to-LAN**) for you to choose for grouping under certain VPN TRUNK-VPN Backup/Load Balance mechanism profile.
	● **No** - Index number of LAN-to-LAN dial-out profile.
	● **Name** - Profile name of LAN-to-LAN dial-out profile.
	● **Connection Type** - Connection type of LAN-to-LAN dial-out profile.
	● **VPN ServerIP (Private Network)** - VPN Server IP of LAN-to-LAN dial-out profiles.
	Active Mode - Display available mode for you to choose. Choose **Backup** or **Load Balance** for your router.
	Add - Add and save new profile to the backup profile list. The corresponding members (LAN-to-LAN profiles) grouped in such new VPN TRUNK – VPN Backup mechanism profile will be locked. The profiles in LAN-to-LAN will be displayed in red. VPN TRUNK – VPN Load Balance mechanism profile will be locked. The profiles in LAN-to-LAN will be displayed in blue.
	Update - Click this button to save the changes to the **Status** (Enable or Disable), profile name, member1 or member2.
	Delete - Click this button to delete the selected VPN TRUNK profile. The corresponding members (LAN-to-LAN profiles) grouped in the deleted VPN TRUNK profile will be released and that profiles in LAN-to-LAN will be displayed in black.

Time for activating VPN TRUNK – VPN Backup mechanism profile

VPN TRUNK – VPN Backup mechanism will be activated automatically after the initial connection of single VPN Tunnel off-line. The content in Member1/2 within VPN TRUNK – VPN Backup mechanism backup profile is similar to dial-out profile configured in LAN-to-LAN web page. VPN TRUNK – VPN Backup mechanism backup profile will process and handle everything unless it is off-line once it is activated.

Time for activating VPN TRUNK – VPN Load Balance mechanism profile

After finishing the connection for one tunnel, the other tunnel will dial out automatically within two seconds. Therefore, you can choose any one of members under VPN Load Balance for dialing out.

Time for activating VPN TRUNK –Dial-out when VPN Load Balance Disconnected

For there is one Tunnel created and connected successfully, to keep the load balance effect between two tunnels, auto-dial will be executed within two seconds.

To close two tunnels of load balance after connecting, please click **Disable** for **Status** in **General Setup** field.

How can you set a VPN TRUNK-VPN Backup/Load Balance mechanism profile?

1. First of all, go to **VPN and Remote Access>>LAN-to-LAN**. Set two or more LAN-to-LAN profiles first that will be used for Member1 and Member2. If you do not set enough LAN-to-LAN profiles, you cannot operate VPN TRUNK – VPN Backup /Load Balance mechanism profile management well.

2. Access into **VPN and Remote Access>>VPN TRUNK Management**.

3. Set one group of VPN TRUNK – VPN Backup/Load Balance mechanism backup profile by choosing **Enable** radio button; type a name for such profile (e.g., 071023); choose one of the LAN-to-LAN profiles from Member1 drop down list; choose one of the LAN-to-LAN profiles from Member2 drop down list; and click **Add** at last.

4. Take a look for LAN-to-LAN profiles. Index 1 is chosen as Member1; index 2 is chosen as Member2. For such reason, LAN-to-LAN profiles of 1 and 2 will be expressed in red to indicate that they are fixed. If you delete the VPN TRUNK – VPN Backup/Load Balance mechanism profile, the selected LAN-to-LAN profiles will be released and expressed in black.

How can you set a GRE over IPsec profile?

1. Please go to LAN to LAN to set a profile with IPsec.

2. If the router will be used as the VPN Server (i.e., with virtual address 192.168.50.200). Please type 192.168.50.200 in the field of My GRE IP. Type IP address (192.168.50.100) of the client in the field of Peer GRE IP. See the following graphic for an example.

High(ESP) ☑ DES ☑ 3DES ☑ AES

4. Gre over IPsec Settings

☐ Enable IPsec Dial-Out function GRE over IPsec
☐ Logical Traffic   My GRE IP 192.168.50.200   Peer GRE IP 192.168.50.100

5. TCP/IP Network Settings

My WAN IP	0.0.0.0	RIP Direction	Disable ▼
Remote Gateway IP	192.168.1.1	From first subnet to remote network, you have to do	
Remote Network IP	192.168.1.0		Route ▼
Remote Network Mask	255.255.255.0		
Local Network IP	192.168.25.1	☐ Change default route to this VPN tunnel (Only single WAN supports this)	
Local Network Mask	255.255.255.0		

More

3. Later, on peer side (as VPN Client): please type 192.168.50.100 in the field of My GRE IP and type IP address of the server (192.168.50.200) in the field of Peer GRE IP.

High(ESP) ☑ DES ☑ 3DES ☑ AES

4. Gre over IPsec Settings

☑ Enable IPsec Dial-Out function GRE over IPsec
☐ Logical Traffic   My GRE IP 192.168.50.100   Peer GRE IP 192.168.50.200

5. TCP/IP Network Settings

My WAN IP	0.0.0.0	RIP Direction	Disable ▼
Remote Gateway IP	192.168.25.1	From first subnet to remote network, you have to do	
Remote Network IP	192.168.25.0		Route ▼
Remote Network Mask	255.255.255.0		
Local Network IP	192.168.1.1	☐ Change default route to this VPN tunnel (Only single WAN supports this)	
Local Network Mask	255.255.255.0		

More

Advanced Load Balance and Backup

After setting profiles for load balance, you can choose any one of them and click Advance for more detailed configuration. The windows for advanced load balance and backup are different. Refer to the following explanation:

Advanced Load Balance

Available settings are explained as follows:

Item	Description
Profile Name	List the load balance profile name.
Load Balance Algorithm	**Round Robin** – Based on packet base, both tunnels will send the packet alternatively. Such method can reach the balance of packet transmission with fixed rate.
	Weighted Round Robin – Such method can reach the balance of packet transmission with flexible rate. It can be divided into Auto Weighted and According to Speed Ratio. **Auto Weighted** can detect the device speed (10Mbps/100Mbps) and switch with fixed value ratio (3:7) for packet transmission. If the transmission rate for packets on both sides of the tunnels is the same, the value of Auto Weighted should be 50:50. **According to Speed Ratio** allows user to adjust suitable rate manually. There are 100 groups of rate ratio for Member1:Member2 (range from 1:99 to 99:1).
VPN Load Balance Policy	Below shows the algorithm for Load Balance.
	Edit – Click this radio button for assign a blank table for configuring Binding Tunnel.
	Insert after – Click this radio button to adding a new binding

	tunnel table.
	Tunnel Bind Table Index- 128 Binding tunnel tables are provided by this device. Specify the number of the tunnel for such Load Balance profile.
	Active – In-active/Delete can delete this binding tunnel table. Active can activate this binding tunnel table.
	Binding Dial Out Index – Specify connection type for transmission by choosing the index (LAN to LAN Profile Index) for such binding tunnel table.
	Scr IP Start /End– Specify source IP addresses as starting point and ending point.
	Dest IP Start/End – Specify destination IP addresses as starting point and ending point.
	Dest Port Start /End– Specify destination service port as starting point and ending point.
	Protocol – **Any** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here, such binding tunnel table can be established for TCP Service Port/UDP Service Port/ICMP/IGMP specified here.
	TCP means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and TCP Service Port also fits the number here, such binding tunnel table can be established. **UDP** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and UDP Service Port also fits the number here, such binding tunnel table can be established. **TCP/UPD** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and TCP/UDP Service Port also fits the number here, such binding tunnel table can be established. **ICMP** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and ICMP Service Port also fits the number here, such binding tunnel table can be established. **IGMP** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and IGMP Service Port also fits the number here, such binding tunnel table can be established. **Other** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here with different TCP Service Port/UDP Service Port/ICMP/IGMP, such binding tunnel table can be established.
Detail Information	This field will display detailed information for Binding Tunnel Policy. Below shows a successful binding tunnel policy for load balance:

To configure a successful binding tunnel, you have to:

Type Binding Src IP range (Start and End) and Binding Des IP range (Start and End). Choose TCP/UDP, IGMP/ICMP or Other as Binding Protocol.

Advanced Backup
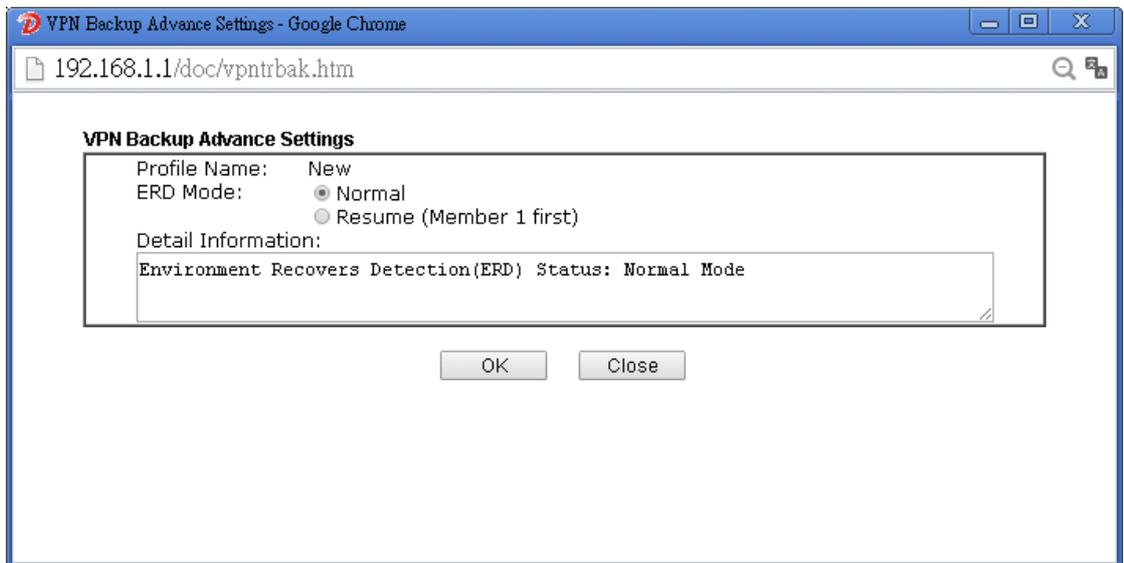
Available settings are explained as follows:

Item	Description
Profile Name	List the backup profile name.
ERD Mode	ERD means "Environment Recovers Detection". **Normal** – choose this mode to make all dial-out VPN TRUNK backup profiles being activated alternatively. **Resume** – when VPN connection breaks down or disconnects,

Vigor3910 Series User's Guide

	Member 1 will be the top priority for the system to do VPN connection.
Detail Information	This field will display detailed information for Environment Recovers Detection.

III-1-9 Connection Management

You can find the summary table of all VPN connections. You may disconnect any VPN connection by clicking **Drop** button. You may also aggressively Dial-out by using Dial-out Tool and clicking **Dial** button.

Available settings are explained as follows:

Item	Description
Dial-out Tool	**General Mode -** This filed displays the profile configured in LAN-to-LAN (with Index number and VPN Server IP address). The VPN connection built by General Mode does not support VPN backup function. **Backup Mode -** This filed displays the profile name saved in VPN TRUNK Management (with Index number and VPN Server IP address). The VPN connection built by Backup Mode supports VPN backup function. **Dial -** Click this button to execute dial out function. **Refresh Seconds -** Choose the time for refresh the dial
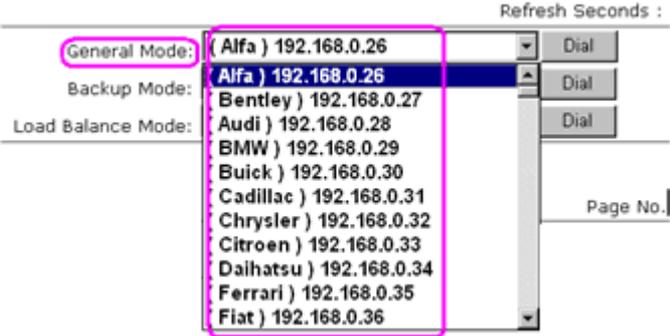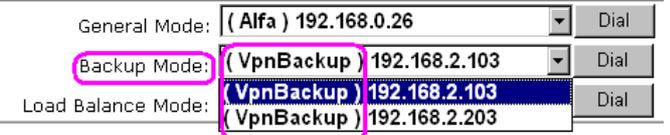
| | information among 5, 10, and 30. |
| | **Refresh -** Click this button to refresh the whole connection status. |

Application Notes

A-1 How to Build a LAN-to-LAN VPN Between Remote Office and Headquarter via IPsec Tunnel (Main Mode)
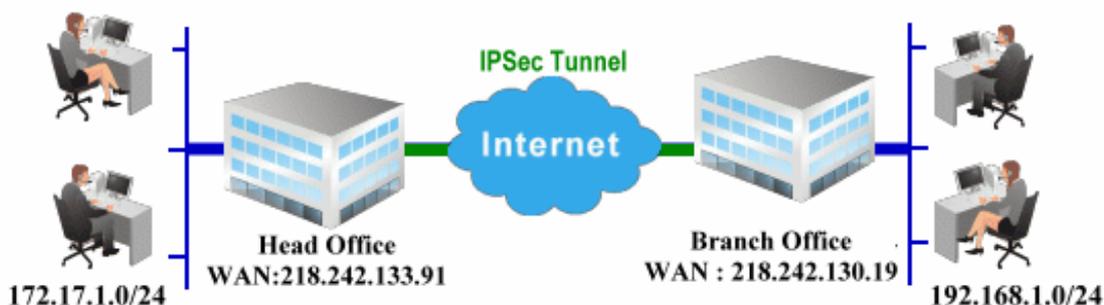
Configuration on Vigor Router for Head Office

1. Log into the web user interface of Vigor router.

2. Open **VPN and Remote Access>>LAN to LAN** to create a LAN-to-LAN profile. The following settings are for a permanent VPN connection.

3. Click any index number to open the configuration page. Type a name which is easy for identification for such profile (in this case, type *VPN Server*), and check the box of **Enable This Profile**. For Vigor router will be set as a **server**, the call direction shall be set as **Dial-in** and set 0 as **Idle Timeout**.

4. Now navigate to the next section, **Dial-In Settings** to check PPTP, IPsec Tunnel and L2TP boxes. Check the box of **Specify Remote...** and type the **Peer VPN Server IP** (e.g., 218.242.130.19 in this case). Press the **IKE Pre-Shared Key** button to set the **PSK**; and select **Medium (AH)** or **High (ESP)** as the security method.

5. Continue to navigate to the **TCP/IP Network Settings** for setting the LAN IP for remote side.

6. Click **OK** to save the settings.

7. Open **VPN and Remote Access>>Connection Management** to check the dial-in connection status (from branch office).

Configuration on Vigor Router for Branch Office

1. Log into the web user interface of Vigor router.

2. Open **VPN and Remote Access>>LAN to LAN** to create a LAN-to-LAN profile. The following settings are for a permanent VPN connection.

3. Click any index number to open the configuration page. Type a name which is easy for identification for such profile (in this case, type *VPN Client*), and check the box of **Enable This Profile**. For such Vigor router will be set as a **client**, the call direction shall be set as **Dial-out**. Check the box of **Always on** for a permanent VPN connection.

4. Now navigate to the next section, **Dial-Out Settings** to select the **IPsec Tunnel** service and type the remote server IP/host name (e.g., 218.242.133.91, in this case). Press the **IKE Pre-Shared Key** button to set the **PSK**; and select **Medium (AH)** or **High (ESP)** as the security method.

5. Continue to navigate to the **TCP/IP Network Settings** for setting the LAN IP for the remote side.

6. Click **OK** to save the settings.

7. Open **VPN and Remote Access>>Connection Management** to check the dial-in connection status (from head office).

III-2 SSL VPN

SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that encrypts traffic using SSL, which is the same technology used on secured websites. Because of SSL's prominence as an encryption protocol on the Internet, most networks have few restrictions on SSL traffic, and as a result SSL VPN is more likely to work when other VPN technologies experience difficulties due to obstacles such as firewalls and Network Address Translation (NAT).

In short,

● It is not necessary for users to preinstall VPN client software for executing SSL VPN connection.

● There are less restrictions for the data encrypted through SSL VPN in comparing with traditional VPN.

Web User Interface
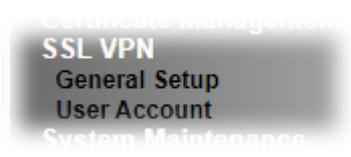
III-2-1 General Setup

The general settings of the SSL VPN Server and SSL Tunnel are entered on this page.

Available settings are explained as follows:

Item	Description
Bind to WAN	Select the WAN interfaces to accept inbound SSL VPN connections.
Port	The port to be used for SSL VPN server. This is separate from the management port which is configured in **System Maintenance>>Management**. The default setting is 443.
Server Certificate	When the client does not set any certificate, default certificate will be used for HTTPS and SSL VPN server. Specify the certificate to be used for SSL connections. Select a certificate from imported or generated certificates on the router, or choose **Self-signed** to use the router's built-in default certificate. The selected certificate can be used in SSL VPN server and HTTPS Web Proxy.

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

III-2-2 User Account

With SSL VPN, Vigor3910 Series let teleworkers have convenient and simple remote access to central site VPN. The teleworkers do not need to install any VPN software manually. From regular web browser, you can establish VPN connection back to your main office even in a guest network or web cafe. The SSL technology is the same as the encryption that you use for secure web sites such as your online bank. The SSL VPN can be operated in either full tunnel mode or proxy mode. Now, Vigor3910 Series allows up to 16 simultaneous incoming users.

SSL VPN authentication and permissions management are implemented through user accounts. SSL VPN user accounts are shared with the remote dial-in user accounts used by other VPN protocols such as PPTP and L2TP, and hence SSL VPN's User Account setup page **SSL VPN >> User Account** is identical to **VPN and Remote Access >> Remote Dial-in user**.

SSL VPN >> Remote Dial-in User

Remote Access User Accounts: | Set to Factory Default |

View: ● All ○ Online ○ Offline   [   ] [Search]

Index	Enable	User	Status	Index	Enable	User	Status
1.	☑	testtest123888	LAN1-DHCP	17.	☐	???	---
2.	☐	???	---	18.	☐	???	---
3.	☐	???	---	19.	☐	???	---
4.	☐	???	---	20.	☐	???	---
5.	☐	???	---	21.	☐	???	---
6.	☐	???	---	22.	☐	???	---
7.	☐	???	---	23.	☐	???	---
8.	☐	???	---	24.	☐	???	---
9.	☐	???	---	25.	☐	???	---
10.	☐	???	---	26.	☐	???	---
11.	☐	???	---	27.	☐	???	---
12.	☐	???	---	28.	☐	???	---
13.	☐	???	---	29.	☐	???	---
14.	☐	???	---	30.	☐	???	---
15.	☐	???	---	31.	☐	???	---
16.	☐	???	---	32.	☐	???	---

<< 1-32 | 33-64 | 65-96 | 97-128 | 129-160 | 161-192 | 193-224 | 225-256 | 257-288 | 289-320 | 321-352 | 353-384 | 385-416 | 417-448 | 449-480 | 481-500 >>   Next >>

Note:
User Accounts need to be added into User Group to enable SSL Portal Login.

[OK]   [Cancel]

Backup setting to file:
[Backup]

Restore From File: [選擇檔案] 未選擇任何檔案
[Restore]

ℹ

Info	SSL VPN can work only with Smart VPN Client developed by DrayTek. After configuring SSL VPN profile, download the utility of Smart VPN Client to build SSL VPN connection.

Click each index to edit one remote user profile.

SSL VPN >> Remote Dial-in User

Index No. 1

User account and Authentication
☑ Enable this account
Idle Timeout   300   second(s)

Allowed Dial-In Type
☑ PPTP
☑ IPsec Tunnel
　☑ IKEv1/IKEv2 ☑ IKEv2 EAP ☑ IPsec XAuth
☑ L2TP with IPsec Policy [None ▼]
☑ SSL Tunnel
☑ OpenVPN Tunnel

☐ Specify Remote Node
Remote Client IP
[　　　　　　]
or Peer ID [　　　　　　]
Netbios Naming Packet   ◉ Pass ○ Block
Multicast via VPN   ○ Pass ◉ Block
　(for some IGMP,IP-Camera,DHCP Relay..etc.)

Subnet
[LAN 1 ▼]
☐ Assign Static IP Address
0.0.0.0

Username   testtest123888
Password   •••
☐ Enable Mobile One-Time Passwords(mOTP)
　PIN Code [　　　　　　]
　Secret [　　　　　　]

IKE Authentication Method
☑ Pre-Shared Key
[IKE Pre-Shared Key]   [Max: 64 characters]
☐ Digital Signature(X.509)
[None ▼]

IPsec Security Method
☑ Medium(AH)
High(ESP)   ☑ DES ☑ 3DES ☑ AES
Local ID (optional) [　　　　　　]

Note:
1. Username can not contain characters ' " and \ .
2. OpenVPN tunnel does not support mOTP.

[OK] [Clear] [Cancel]

Available settings are explained as follows:

Item	Description
User account and Authentication	**Enable this account** - Check the box to enable this function.
	Idle Timeout- If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.
	User Name - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the name/password is limited to 23 characters.
	Password - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the name/password is limited to 19 characters.
	Enable Mobile One-Time Passwords (mOTP) - Check this box to make the authentication with mOTP function.
	● **PIN Code** – Type the code for authentication (e.g, 1234).
	● **Secret** – Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).
Allowed Dial-In Type	Select the VPN protocols that this user is allowed to use.
	PPTP - Allow the remote dial-in user to establish VPN connections with the PPTP protocol. You should set the User

Item	Description
	Name and Password of remote dial-in user below.
	IPSec Tunnel - Allow the remote dial-in user to establish IPsec tunnels.
	L2TP with IPSec Policy - Allow the remote dial-in user to establish L2TP VPN connections. You can select to use L2TP alone or with IPSec. Select one of the following options:
	● **None -** Do not apply the IPSec policy. L2TP connections are not encrypted.
	● **Nice to Have -** Attempt to establish an IPsec secure channel first, before starting an L2TP session. If an IPsec secure channel cannot be established with the remote client, fall back to an L2TP connection without encryption.
	● **Must -** Require that an IPsec secure channel be established before starting an L2TP connection. Disconnect if an IPsec secure channel cannot be established.
	SSL Tunnel - Select to allow the remote dial-in user to initiate SSL VPN tunnels.
	OpenVPN Tunnel - Select to allow the remote dial-in user to initiate OpenVPN tunnels.
	Specify Remote Node - Select this option to specify the remote IP address, ISDN number or peer ID (used in IKE aggressive mode) used to authenticate the remote dial-in user. If this option is not selected, the authentication and security methods specified in the **general settings** will be used instead.
	Netbios Naming Packet
	● **Pass** – Select this to allow Netbios name inquiries between the hosts located on both sides of VPN Tunnel.
	● **Block** – Select this to block Netbios name inquiries between remote and local hosts.
	Multicast via VPN - Some programs might send multicast packets via VPN connection.
	● **Pass** –Select this to allow multicast packets to pass through VPN connections.
	● **Block** –Select this to block multicast packets from passing through the VPN connections. This is the default setting.
Subnet	Select a subnet for this VPN profile.
	Assign Static IP Address –If you would like to assign a static IP address to this user, enter it here.
IKE Authentication Method	All fields in this section, except for Digital Signature (X.509), are applicable to IPsec Tunnels and L2TP connections with IPsec Policy when you specify the IP address of the remote node (Remote Client IP in Specify Remote Node above).
	Digital Signature (X.509) can be used with IPSec tunnels regardless of the IP address of the remote node is specified or not.
	Pre-Shared Key - Select this checkbox to enable Pre-shared Key function and enter a string of up to 63 characters as the pre-shared key.
	Digital Signature (X.509) – Select this checkbox to enable X.509 Digital Signature and choose a predefined profile that

Item	Description
	has been set in **VPN and Remote Access >> IPSec Peer Identity**.
IPSec Security Method	When the remote node is specified, all fields in this section are required for IPsec Tunnels and L2TP connections with IPsec Policy. Select any combination of Medium, DES, 3DES and AES security methods as desired.
	Medium (AH, Authentication Header) - Data will be authenticated, but not be encrypted. By default, this option is enabled. You can uncheck it to disable it.
	High (ESP, Encapsulating Security Payload) - Payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
	Local ID - Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.

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

III-3 Certificate Management

A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Here Vigor router support digital certificates conforming to standard X.509.

Any entity wants to utilize digital certificates should first request a certificate issued by a CA server. It should also retrieve certificates of other trusted CA servers so it can authenticate the peer with certificates issued by those trusted CA servers.

Here you can manage generate and manage the local digital certificates, and set trusted CA certificates. Remember to adjust the time of Vigor router before using the certificate so that you can get the correct valid period of certificate.

Web User Interface

III-3-1 Local Certificate

Available settings are explained as follows:

Item	Description
Generate	Click this button to open **Generate Certificate Request** window. Type in all the information that the window requests. Then click **Generate** again.
Import	Click this button to import a saved file as the certification information.
Refresh	Click this button to refresh the information listed below.
View	Click this button to view the detailed settings for certificate request.
Delete	Click this button to delete selected name with certification information.

GENERATE

Click this button to open **Generate Certificate Signing Request** window. Type in all the information that the window request such as certifcate name (used for identifying different certificate), subject alternative name type and relational settings for subject name. Then click **GENERATE** again.

Certificate Management >> Local Certificate

Generate Certificate Signing Request

Certificate Name	

Subject Alternative Name

Type	IP Address ▼
IP	

Subject Name

Country (C)	
State (ST)	
Location (L)	
Organization (O)	
Organization Unit (OU)	
Common Name (CN)	
Email (E)	

Key Type	RSA ▼
Key Size	1024 Bit ▼
Algorithm	SHA-256 ▼

Generate

ⓘ

Info	Please be noted that "Common Name" must be configured with rotuer's WAN IP or domain name.

After clicking **GENERATE**, the generated information will be displayed on the window below:

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify	
server	/C=TW/ST=Hsinchu/L=Hsinchu/O...	Requesting	View	Delete
---	---	---	View	Delete
---	---	---	View	Delete

GENERATE   IMPORT   REFRESH

IMPORT

Vigor router allows you to generate a certificate request and submit it the CA server, then import it as "Local Certificate". If you have already gotten a certificate from a third party, you may import it directly. The supported types are PKCS12 Certificate and Certificate with a private key.

Click this button to import a saved file as the certification information. There are three types of local certificate supported by Vigor router.

Available settings are explained as follows:

Item	Description
Upload Local Certificate	It allows users to import the certificate which is generated by Vigor router and signed by CA server. If you have done well in certificate generation, the Status of the certificate will be shown as "**OK**".
Upload PKCS12 Certificate	It allows users to import the certificate whose extensions are usually .pfx or .p12. And these certificates usually need passwords. **Note:** PKCS12 is a standard for storing private keys and certificates securely. It is used in (among other things) Netscape and Microsoft Internet Explorer with their import and export options.
Upload Certificate and Private Key	It is useful when users have separated certificates and private keys. And the password is needed if the private key is encrypted.

REFRESH

Click this button to refresh the information listed below.

View

Click this button to view the detailed settings for certificate request.

Info	You have to copy the certificate request information from above window. Next, access your CA server and enter the page of certificate request, copy the information into it and submit a request. A new certificate will be issued to you by the CA server. You can save it.

Delete

Click this button to remove the selected certificate.

III-3-2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate. In addition, you can build a RootCA certificate if required.

When the local client and remote client are required to make certificate authentication (e.g., IPsec X.509) for data passing through SSL tunnel and avoiding the attack of MITM, a trusted root certificate authority (Root CA) will be used to authenticate the digital certificates offered by both ends.

However, the procedure of applying digital certificate from a trusted root certificate authority is complicated and time-consuming. Therefore, Vigor router offers a mechanism which allows you to generate root CA to save time and provide convenience for general user. Later, such root CA generated by DrayTek server can perform the issuing of local certificate.

Info	Root CA can be deleted but not edited. If you want to modify the settings for a Root CA, please delete the one and create another one by clicking Create Root CA.

Certificate Management >> Trusted CA Certificate

X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify
Root CA	---	---	Create
Trusted CA-1	---	---	View Delete
Trusted CA-2	---	---	View Delete
Trusted CA-3	---	---	View Delete

Note:
1. Please setup the "System Maintenance >> **Time and Date**" correctly before you try to generate a RootCA!!
2. The Time Zone MUST be setup correctly!!

IMPORT REFRESH

Creating a RootCA

Click Create Root CA to open the following page. Type in all the information that the window request such as certifcate name (used for identifying different certificate), subject alternative name type and relational settings for subject name. Then click **GENERATE** again.

Importing a Trusted CA

To import a pre-saved trusted CA certificate, please click **IMPORT** to open the following window. Use **Browse**... to find out the saved text file. Then click **Import**. The one you imported will be listed on the Trusted CA Certificate window.

For viewing each trusted CA certificate, click **View** to open the certificate detail information window. If you want to delete a CA certificate, choose the one and click **Delete** to remove all the certificate information.
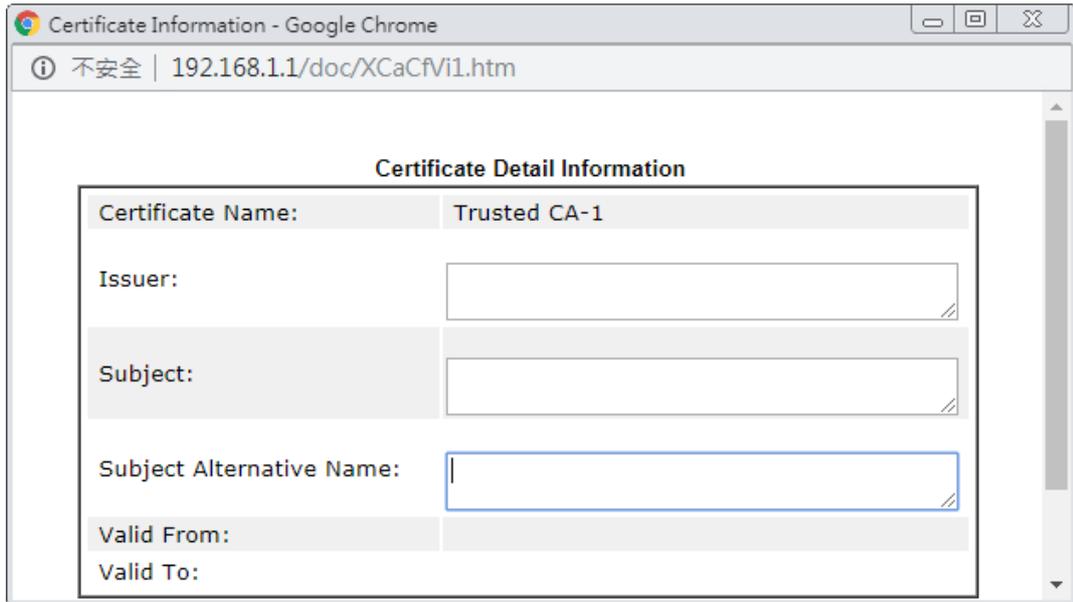
III-3-3 Certificate Backup

Local certificate and Trusted CA certificate for this router can be saved within one file. Please click **Backup** on the following screen to save them. If you want to set encryption password for these certificates, please type characters in both fields of **Encrypt password** and **Confirm password**.

Also, you can use **Restore** to retrieve these two settings to the router whenever you want.

III-3-4 Self-Signed Certificate

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

The self-signed certificate will be applied in SSL VPN, HTTPS, and so on. In addition, it can be created for free by using a wide variety of tools.

Certificate Management >> Self-Signed Certificate

Self-Signed Certificate Information

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 :	Oct 7 15:39:44 2019 GMT
Valid To :	Oct 6 15:39:44 2049 GMT
PEM Format Content :	

```
-----BEGIN CERTIFICATE-----
MIIDijCCAnKgAwIBAgIJAP03qa0NuWcyMA0GCSqGSIb3DQEBCwUAMHgxCzAJBgNV
BAYTAlRXMRAwDgYDVQQIDAdIc2luQ2h1MQ4wDAYDVQQHDAVIdUtvdTEWMBQGA1UE
CgwNRHJheVRlayBDb3JwLjEYMBYGA1UECwwPRHJheVRlayBTdXBwb3J0MRUwEwYD
VQQDDAxWaWdvciBSb3V0ZXIwHhcNMTkxMDA3MTUzOTQ0WhcNNDkxMDA2MTUzOTQ0
WjB4MQswCQYDVQQGEwJUVzEQMA4GA1UECAwHSHNpbkNodTEOMAwGA1UEBwwFSHVL
b3UxFjAUBgNVBAoMDURyYXlUZWsgQ29ycC4xGDAWBgNVBAsMD0RyYXlUZWsgU3Vw
cG9ydDEVMBMGA1UEAwwMVmlnb3IgUm91dGVyMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAyUYWNkKV4D/no6dEd6w2eMfA/FEuVVnjT7cUsocUGxyO/7gi
ryD1HRIqbs7yItE/d+KWC176pKs1KM89GpBIgwQJ0KQx+DG5v7FIVSxcYgIUMff9
H7uIZggqAbeTxhYYViYwyI5p/2v/+FcwtcgEdEzHMkcFD4y1UndGYVr7eIJfCxkD
MBg/aUAoEoX67zZm64ZiRbECiEptRL+TK4gCuQzmqkF/LaupCmUUpNTdT0sU6Kd0
CwrL9NNWG0ZMjTpicpCEp2l0X+7CLa5C9IB9HjjPbNfRdeN6BR/0t1IDw8tYWbPv
5oWbhsTxdy+Pbh8o4p+qW0ZVJSF/rJtenaA9OwIDAQABoxcwFTATBgNVHSUEDDAK
BggrBgEFBQcDATANBgkqhkiG9w0BAQsFAAOCAQEAh29rKu/7T1UtOAYrlOlYZ528
GcHRTPZrQeAeKCp+w6Fz2lBuuyGHpxcneI67y1NFiwTXWlrRm0uqR3D1Nz5uiJmo
Y85HueZgXha3H+X9LJ9tfULMcVEfjtZcB6obPrP4Phc67Lt5fYP2EuAID2jWh3sP
jvKh2io1/ryjCpEAVE3gcrMSsUUOjcFd/bbTjH7zq476QUp7CB5lgGAwhdhkenhD
d4YH/33G06gUVMvuFdcWxWcfgg9ylMKNICTjuuvFGMTue4AzvDuoqrpBIa4JQ0Zw
5RAtuEf5s8FeEIG423f4mm/zCZvy6Xkrr8CpW3tn7Cbay+V9NyfHrU/qnhWFJg==
-----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]

Part IV Security

Firewall

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

CSM

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

IV-1 Firewall

While the broadband users demand more bandwidth for multimedia, interactive applications, or distance learning, security has been always the most concerned. The firewall of the Vigor router helps to protect your local network against attack from unauthorized outsiders. It also restricts users in the local network from accessing the Internet. Furthermore, it can filter out specific packets that trigger the router to build an unwanted outgoing connection.

Firewall Facilities

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

● User-configurable IP filter (Call Filter/ Data Filter).

● Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data

● Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

IP Filters

Depending on whether there is an existing Internet connection, or in other words "the WAN link status is up or down", the IP filter architecture categorizes traffic into two: **Call Filter** and **Data Filter**.

● **Call Filter -** When there is no existing Internet connection, **Call Filter** is applied to all traffic, all of which should be outgoing. It will check packets according to the filter rules. If legal, the packet will pass. Then the router shall **"initiate a call"** to build the Internet connection and send the packet to Internet.

● **Data Filter** - When there is an existing Internet connection, **Data Filter** is applied to incoming and outgoing traffic. It will check packets according to the filter rules. If legal, the packet will pass the router.

The following illustrations are flow charts explaining how router will treat incoming traffic and outgoing traffic respectively.
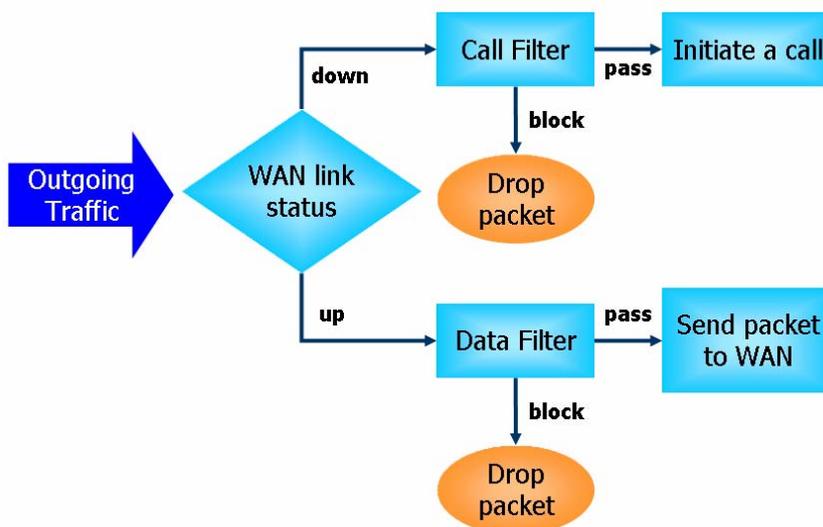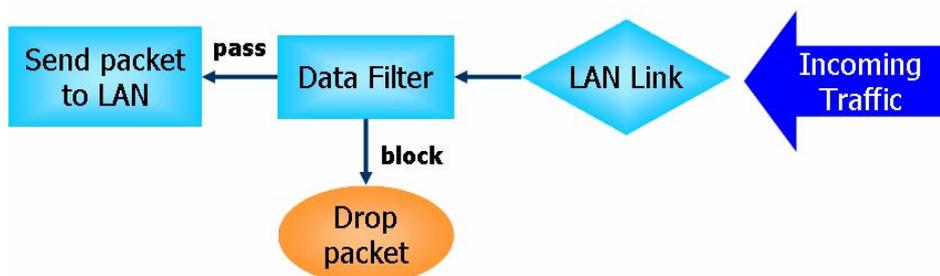
Stateful Packet Inspection (SPI)

Stateful inspection is a firewall architecture that works at the network layer. Unlike legacy static packet filtering, which examines a packet based on the information in its header, stateful inspection builds up a state machine to track each connection traversing all interfaces of the firewall and makes sure they are valid. The stateful firewall of Vigor router not only examines the header information also monitors the state of the connection.

Denial of Service (DoS) Defense

The **DoS Defense** functionality helps you to detect and mitigate the DoS attack. The attacks are usually categorized into two types, the flooding-type attacks and the vulnerability attacks. The flooding-type attacks will attempt to exhaust all your system's resource while the vulnerability attacks will try to paralyze the system by offending the vulnerabilities of the protocol or operation system.

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

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

The below shows the attack types that DoS/DDoS defense function can detect:

1. SYN flood attack
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. Unassigned Numbers

Web User Interface

Below shows the menu items for Firewall.
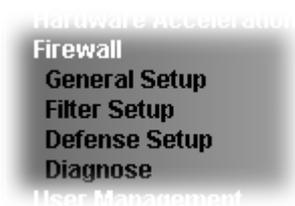
IV-1-1 General Setup

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

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

General Setup Page

Such page allows you to enable / disable Call Filter and Data Filter, determine general rule for filtering the incoming and outgoing data.

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.
Allow pass inbound gragmented large...	Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor router will reject these fragmented packets to prevent attack unless you enable "**Allow pass inbound gragmented large...**". By checking this box, you can play these kinds of on-line games. If security concern is in higher priority, you cannot enable "**Allow pass inbound gragmented large...**".
Enable Strict Security Firewall	For the sake of security, the router will execute strict security checking for data transmission. Such feature is enabled in default. All the packets, while transmitting through Vigor router, will be filtered by firewall. If the firewall system (e.g., content filter server) does not make any response (pass or block) for these packets, then the router's firewall will block the packets directly.
Block routing 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 router.

Firewall >> General Setup

General Setup

| General Setup | Default Rule |

Actions for default rule:

Application	Action/Profile	Syslog
Filter	Pass ▼	☐
Sessions Control	0 / 150000	☐
Quality of Service	None ▼	☐
User Management	None ▼	☐
APP Enforcement	None ▼	☐
URL Content Filter	None ▼	☐
Web Content Filter	None ▼	☐
DNS Filter	None ▼	☐

| Advance Setting | Edit |

OK   Cancel

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.
Quality of Service	Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later.
User Management	Such item is available only when **Rule-Based** is selected in **User Management>>General Setup**. The general firewall rule will be applied to the user/user group/all users specified here. **Note:** When there is no user profile or group profile existed, **Create New User** or **Create New Group** item will appear for you to click to create a new one.
APP Enforcement	Select an **APP Enforcement** profile for global IM/P2P application blocking. If there is no profile for you to select, please choose **[Create New]** from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the **APP Enforcement** profile selected here. For detailed information, refer to the section of **APP Enforcement** profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by

	checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
URL Content Filter	Select one of the **URL Content Filter** profile settings (created in **CSM>> URL Content Filter**) for applying with this router. Please set at least one profile for choosing in **CSM>> URL Content Filter** web page first. Or choose **[Create New]** from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for **URL Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
Web Content Filter	Select one of the **Web Content Filter** profile settings (created in **CSM>> Web Content Filter**) for applying with this router. Please set at least one profile for anti-virus in **CSM>> Web Content Filter** web page first. Or choose **[Create New]** from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for **Web Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
DNS Filter	Select one of the DNS Filter profile settings (created in CSM>>DNS Filter) for applying with this router. Please set at least one profile in **CSM>> Web Content Filter** web page first. Or click the DNS Filter link in this page to create a new profile.
Advance Setting	Click **Edit** to open the following window. However, it is **strongly recommended** to use the default settings here. **Firewall >> General Setup** Advance Setting Codepage ANSI(1252)-Latin I Window size: 65535 Session timeout: 1440 Minute OK Close **Codepage** - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtain correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage. If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.

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

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

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

IV-1-2 Filter Setup

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

Firewall >> Filter Setup

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

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

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1
Comments : Default Call Filter

Rule	Enable	Comments	Direction	Src IP	Dst IP	Service Type	Action	CSM	Move Up	Move Down
1	☑	Block NetBios	LAN/RT/VPN -> WAN	Any	Any	TCP/UDP, Port: from 137~139 to any	Block Immediately			Down
2	☐		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
3	☐		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
4	☐		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
5	☐		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
6	☐		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
7	☐		LAN/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	

Filter Set 1 2 3 4 5 6 7 8 9 10 11 12   Next Filter Set None ▼

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

OK   Clear   Cancel

Available settings are explained as follows:

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

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

To use Wizard Mode, simple do the following steps:

1. Click the **Wizard Mode** radio button.

2. Click **Index 1**. The setting page will appear as follows:

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

Filter Set 1 Rule 1

Firewall Rule applies to packets that meet the following criteria

Comments:	Block NetBios
Direction:	LAN/RT/VPN -> WAN
Source IP:	Any Address
Start IP Address	0.0.0.0
End IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Destination IP:	Any Address
Start IP Address	0.0.0.0
End IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Protocol:	TCP/UDP
Source Port	= 137 ~ 139
Destination Port	= 1 ~ 65535

Back   Next   Finish   Cancel

Available settings are explained as follows:

Item	Description
Comments	Enter filter set comments/description. Maximum length is 14- character long.
Direction	Set the direction of packet flow. It is for **Data Filter** only. For the **Call Filter**, this setting is not available since **Call Filter** is only applied to outgoing traffic. LAN/RT/VPN -> WAN LAN/RT/VPN -> WAN WAN -> LAN/RT/VPN LAN/RT/VPN -> LAN/RT/VPN **Note:** RT means routing domain for 2nd subnet or other LAN.
Source/Destination IP	To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and type them in this dialog.
Protocol	Specify the protocol(s) which this filter rule will apply to.
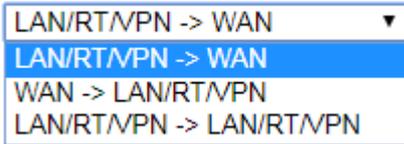
Vigor3910 Series User's Guide

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

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

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

Filter Set 1 Rule 1

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

○ Pass Immediately
   APP Enforcement: None ▾
   URL Content Filter: None ▾
   Web Content Filter: 1-Default ▾
   DNS Filter   None ▾
○ Block Immediately

[Back] [Next] [Finish] [Cancel]

Available settings are explained as follows:

Item	Description
Pass Immediately	Packets matching the rule will be passed immediately.
	APP Enforcement - Select an **APP Enforcement** profile for global IM/P2P application blocking. If there is no profile for you to select, please choose **[Create New]** from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the **APP Enforcement** profile selected here. For detailed information, refer to the section of **APP Enforcement** profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
	URL Content Filter - Select one of the **URL Content Filter** profile settings (created in **CSM>> URL Content Filter**) for applying with this router. Please set at least one profile for choosing in **CSM>> URL Content Filter** web page first. Or choose **[Create New]** from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for **URL Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
	Web Content Filter - Select one of the **Web Content Filter** profile settings (created in **CSM>> Web Content Filter**) for applying with this router. Please set at least one profile for anti-virus in **CSM>> Web Content Filter** web page first. Or choose **[Create New]** from the drop down list in this page

	to create a new profile. For troubleshooting needs, you can specify to record information for **Web Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
	DNS Filter - Select one of the DNS Filter profile settings (created in CSM>>DNS Filter) for applying with this router. Please set at least one profile in **CSM>> Web Content Filter** web page first. Or click the DNS Filter link from the drop down list in this page to create a new profile.
Block Immediately	Packets matching the rule will be dropped immediately.

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

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

Filter Set 1 Rule 1 Configuration Summary

Comments :	Block NetBios

Direction

    LAN/RT/VPN -> WAN

Criteria

Source IP	Any
Destination IP	Any
Protocol	TCP/UDP, Port: from 137 ~ 139 to any

More options

    Pass Immediately

APP Enforcement :	None
URL Content Filter :	None
Web Content Filter :	1 - Default
DNS Filter :	None

[Back]   [Next]   [Finish]   [Cancel]

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

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

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

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 1

☑ Enable	
Comments	Block NetBios
Schedule Profile	None ▼, None ▼, None ▼, None ▼
	☐ Clear sessions when schedule is ON
Direction	LAN/RT/VPN -> WAN ▼ [Advanced]
Source IP/Country	Any [Edit]
Destination IP/Country	Any [Edit]
Service Type	TCP/UDP, Port: from 137~139 to any [Edit]
Fragments	Don't Care ▼

Application	Action/Profile	Syslog
Filter	Block Immediately ▼	☐
Branch to Other Filter Set	None ▼	
Sessions Control	0 / 150000	☐
MAC Bind IP	Non-Strict ▼	☐
Quality of Service	None ▼	☐
User Management	None ▼	☐
APP Enforcement	None ▼	☐
URL Content Filter	None ▼	☐
Web Content Filter	None ▼	☐
DNS Filter	None ▼	☐
Advance Setting	[Edit]	

[OK] [Clear] [Cancel]

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable the filter rule.
Comments	Enter filter set comments/description. Maximum length is 14- character long.
Schedule Profile	Set PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications** >> **Schedule** setup. The default setting of this field is blank and the function will always work.
Clear sessions when schedule is 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 IP / Country **Destination IP / Country**	Click **Edit** to access into the following dialog to choose the source/destination IP or IP ranges.
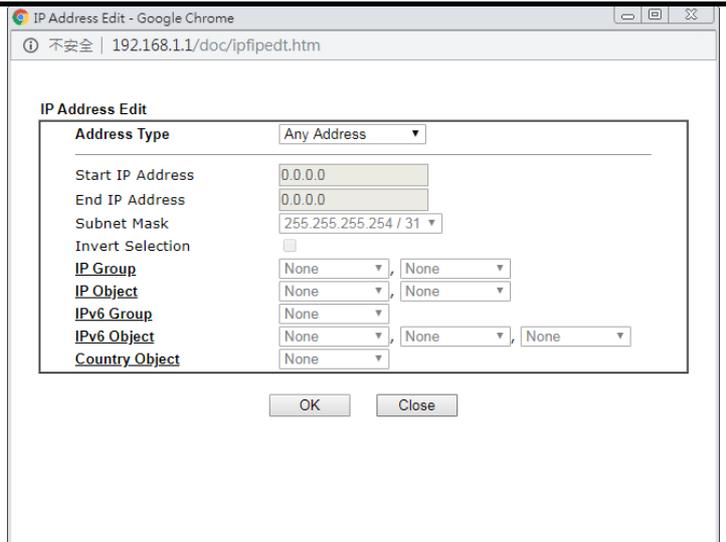
To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address/Group and Objects/Country Object** as the Address Type and type them in this dialog. For example, if you want to use the IP range from defined groups or objects, please choose **Group and Objects** as the Address Type.
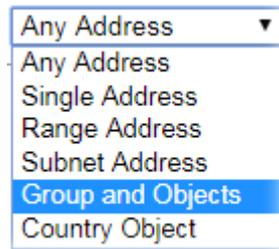
From the **IP Group** drop down list, choose the one that you want to apply. Or use the **IP Object** drop down list to choose the object that you want.

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
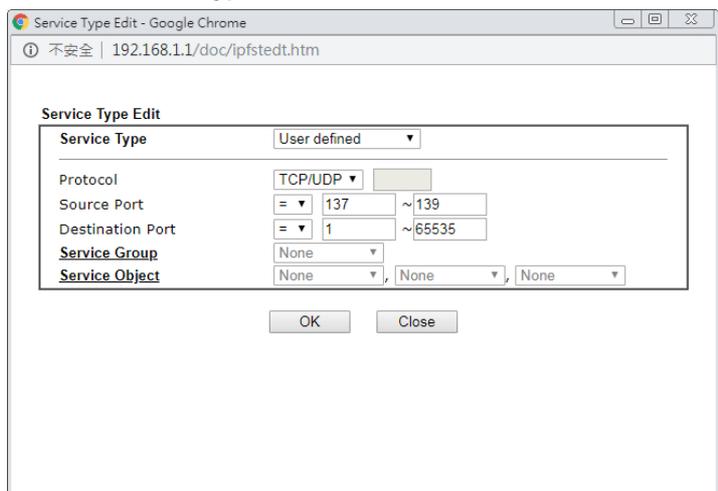
Vigor3910 Series User's Guide

	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 router will apply the specified filter rule for ever and will not return to previous filter rule any more.
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.
MAC Bind IP	**Strict** – Make the MAC address and IP address settings configured in **IP Object** for **Source IP** and **Destination IP** are bound for applying such filter rule.
	No-Strict - no limitation.
Quality of Service	Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later.
User Management	Such item is available only when **Rule-Based** is selected in User **Management>>General Setup**. The general firewall

	rule will be applied to the user/user group/all users specified here.
	Note: When there is no user profile or group profile existed, **Create New User** or **Create New Group** item will appear for you to click to create a new one.
APP Enforcement	Select an **APP Enforcement** profile for global IM/P2P application blocking. If there is no profile for you to select, please choose **[Create New]** from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the **APP Enforcement** profile selected here. For detailed information, refer to the section of **APP Enforcement** profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
URL Content Filter	Select one of the **URL Content Filter** profile settings (created in **CSM>> URL Content Filter**) for applying with this router. Please set at least one profile for choosing in **CSM>> URL Content Filter** web page first. Or choose **[Create New]** from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for **URL Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
Web Content Filter	Select one of the **Web Content Filter** profile settings (created in **CSM>> Web Content Filter**) for applying with this router. Please set at least one profile for anti-virus in **CSM>> Web Content Filter** web page first. Or choose **[Create New]** from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for **Web Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
DNS Filter	Select one of the DNS Filter profile settings (created in **CSM>>DNS Filter**) for applying with this router. Please set at least one profile in **CSM>> Web Content Filter** web page first. Or click the DNS Filter link from the drop down list in this page to create a new profile.
Advance Setting	Click **Edit** to open the following window. However, it is **strongly recommended** to use the default settings here.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 1

Advance Setting

Codepage	ANSI(1252)-Latin I ▼
Window size:	65535
Session timeout:	60 Minute
DrayTek Banner:	☑

Strict Security Checking

☐ APP Enforcement

[OK]   [Close]

Codepage - This function is used to compare the characters among different languages. Choose correct codepage can

help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage.

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

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

Session timeout–Setting timeout for sessions can make the best utilization of network resources. However, Queue timeout is configured for TCP protocol only; session timeout is configured for the data flow which matched with the firewall rule.

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

Strict Security Checking - All the packets, while transmitting through Vigor router, will be filtered by firewall settings configured by Vigor router. When the resource is inadequate, the packets will be blocked if Strict Security Checking is enabled. If Strict Security Checking is not enabled, then the packets will pass through the router.

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

IV-1-3 Defense Setup

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

IV-1-3-1 DoS Defense

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

Firewall >> Defense Setup

DoS Defense	Spoofing Defense

DoS defense

☐ Enable DoS Defense [Select All] [White/Black List Option]   Log: [Enable ▾]

  ☐ Enable SYN flood defense   Threshold 2000 packets / sec
                                       Timeout   10 sec

  ☐ Enable UDP flood defense   Threshold 2000 packets / sec
                                         Timeout   10 sec

  ☐ Enable ICMP flood defense   Threshold 250 packets / sec
                                         Timeout   10 sec

  ☐ Enable Port Scan detection   Threshold 2000 packets / sec
  ☐ Block IP options   ☐ Block TCP flag scan
  ☐ Block Land   ☐ Block Tear Drop
  ☐ Block Smurf   ☐ Block Ping of Death
  ☐ Block trace route   ☐ Block ICMP fragment
  ☐ Block SYN fragment   ☐ Block Unassigned Numbers
  ☐ Block Fraggle Attack

[OK] [Clear All] [Cancel]

Available settings are explained as follows:

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

Enable UDP flood defense	Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent UDP packets for a period defined in Timeout.
	The default setting for threshold and timeout are 2000 packets per second and 10 seconds, respectively. That means, when 2000 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.
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 router will discard the ICMP echo requests coming from the Internet.
	The default setting for threshold and timeout are 250 packets per second and 10 seconds, respectively. That means, when 250 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.
Enable PortScan detection	Port Scan attacks the Vigor router by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the port-scanning Threshold rate, the Vigor router will send out a warning.
	By default, the Vigor router sets the threshold as 2000 packets per second. That means, when 2000 packets per second received, they will be regarded as "attack event".
Block IP options	Check the box to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messages…etc. An eavesdropper outside might learn the details of your private networks.
Block Land	Check the box to enforce the Vigor router to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.
Block Smurf	Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.
Block trace route	Check the box to enforce the Vigor router not to forward any trace route packets.
Block SYN fragment	Check the box to activate the Block SYN fragment function. The Vigor router will drop any packets having SYN flag and more fragment bit set.
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 router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.
Block Ping of Death	Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.
Block ICMP Fragment	Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.
Block Unassigned Numbers	Check the box to activate the Block Unknown Protocol function. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and reject this kind of packets.
Warning Messages	We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client. All the warning messages related to **DoS Defense** will be sent to user and user can review it through Syslog daemon. Look for the keyword **DoS** in the message, followed by a name to indicate what kind of attacks is detected. System Maintenance >> SysLog / Mail Alert Setup **SysLog / Mail Alert Setup** **SysLog Access Setup** ☑ Enable Syslog Save to: ☑ Syslog Server ☐ USB Disk **Router Name** [ ] Server IP Address [ ] Destination Port [514] Mail Syslog ☐ Enable Enable syslog message: ☑ Firewall Log ☑ User Access Log ☑ WAN Log ☑ Router/DSL information **AlertLog Setup** ☐ Enable AlertLog Port [514] **Mail Alert Setup** ☑ Enable [Send a test e-mail] SMTP Server [ ] SMTP Port [25] Mail To [ ] Return-Path [ ] ☐ Authentication User Name [ ] Password [ ] Enable E-Mail Alert: ☑ DoS Attack ☑ IM-P2P ☑ VPN LOG Note: 1. Mail Syslog cannot be activated unless USB Disk is ticked for "Syslog Save to". 2. Mail Syslog feature sends a Syslog file when its size reaches 1M Bytes. [OK] [Clear]
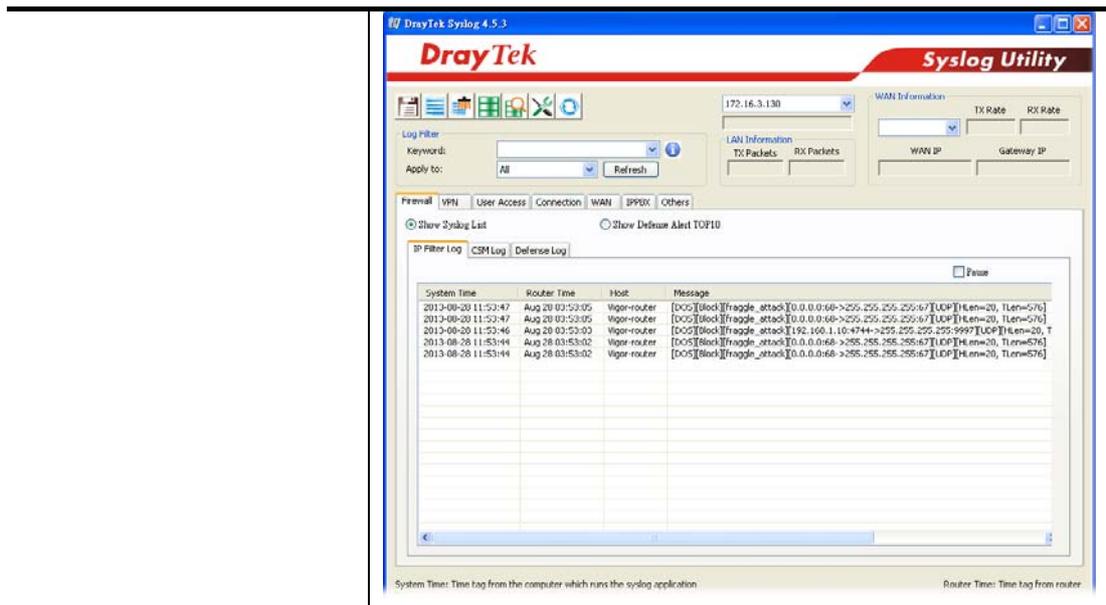
IV-1-3-2 Spoofing Defense

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

IV-1-4 Diagnose

The purpose of this function is to test when the router receiving incoming packet, which firewall rule will be applied to that packet. The test result, including firewall rule profile, IP address translation in packet transmission, state of the firewall fuctions and etc., also will be shown on this page.

Info	The result obtained by using Diagnose is offered for RD debug. It will be different according to actual state such as netework connection, LAN/WAN settings and so on.

Available settings are explained as follows:

Item	Description
Mode	To have a firewall rule test, specify the service type (ICMP, UDP, TCP) of the packet and type of the IP address (IPv4/IPv6).
Direction	Set the way (from WAN or from LAN) that Vigor router receives the first packet for test. Different way means the firewall will process the connection initiated from LAN or from WAN.
Test View	This is a dynamic display page. According to the direction specified, test view will display the figure to guide you typing IP address, port number, and MAC address. Later, after clicking the Analyze button, the information for the firewall rule profile and address translation will be shown on this page.
Src IP	Type the IPv4/IPv6 address of the packet's source.
Src Port	Type the port number of the packet's source.
Src MAC	Type the MAC address of the packet's source.
Dst IP	Type the IPv4/IPv6 address of the packet's destination.
Dst Port	Type the port number of the packet's destination.
Packet & Payload	In firewall diagnose, two packets belong to one connection. In general, two packets are enough for Vigor router to perform this test. **Enable** – Check the box to send out the test packet. **Direction** – The first packet of the firewall test will follow the direction specified above. However, the direction for the second packet might be different. Simply choose the direction (from Computer A to B or from the B to A) for the second packet. **Protocol** – It displays the mode selected above and the sate. If required, click the mode link to configure advanced setting. The common service type (Customize, Ping, Trace

	Route / Customize, DNS, Trace Route / Customize, Http(GET) related to that mode (ICMP / UDP / TCP) will be shown on the following dialog box.
	● **Type** - Choose Customize, Ping, Trace Route / Customize, DNS, Trace Route / Customize, Http (GET).
	● **Payload** - It is available when Customzie is selected. Simply type 16 HEX characters which represent certain packet (e.g., DNS packet) if you want to set the data transfered with protocol (ICMP/UDP/TCP) which is different to Type setting.
Analyze	Execute the test and analyze the result.
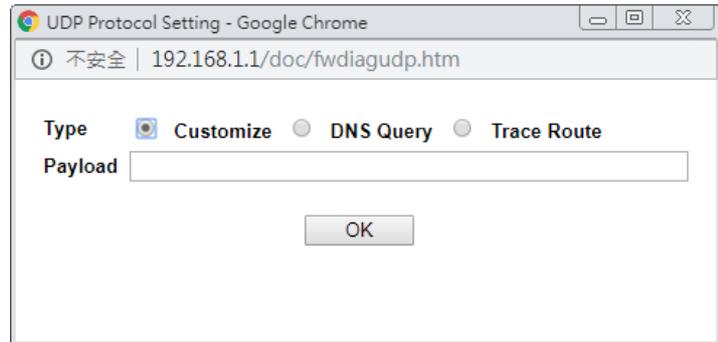
The following figure shows the test result after clicking **Analyze**. Processing state for the fuctions (MAC Filter, QoS, User management, etc.,) related to the firewall will be displayed by green or red LED.

Application Notes

A-1 How to Configure Certain Computers Accessing to Internet

We can specify certain computers (e.g., 192.168.1.10 ~ 192.168.1.20) accessing to Internet through Vigor router. Others (e.g., 192.168.1.31 and 192.168.1.32) outside the range can get the source from LAN only.
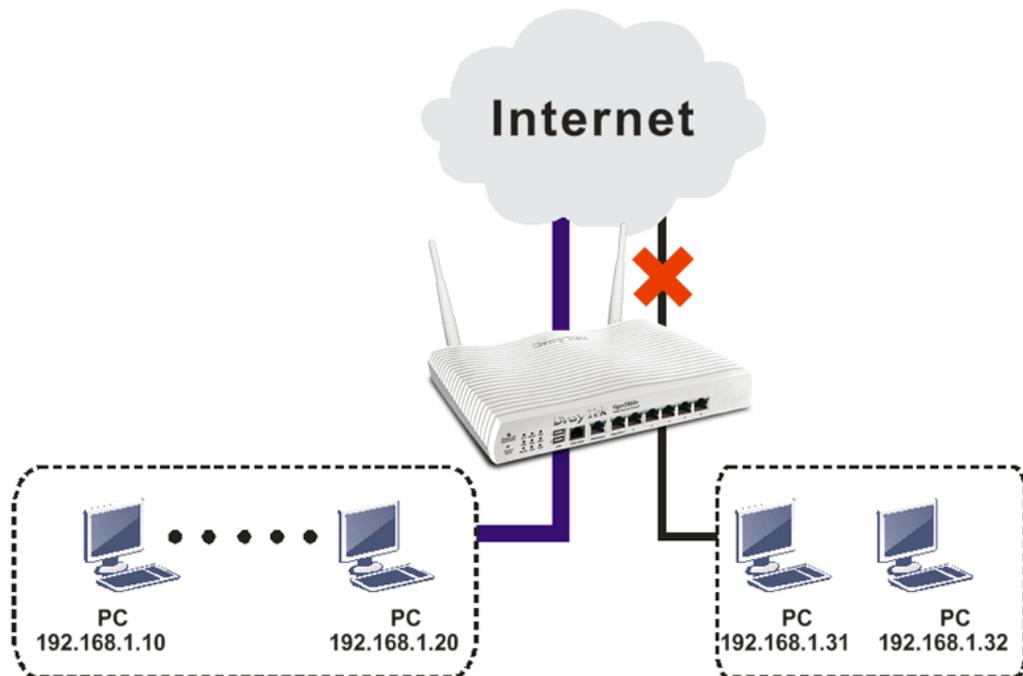
The way we can use is to set two rules under **Firewall**. For **Rule 1** of **Set 2** under **Firewall>>Filter Setup** is used as the default setting, we have to create a new rule starting from Filter Rule 2 of Set 2.

1. Access into the web user interface of Vigor router.

2. Open **Firewall>>Filter Setup**. Click the **Set 2** link and choose the **Filter Rule 2** button.

3. Check **Enable** to enable the filter rule. Type the comments (e.g., **block_all**). Choose **Block If No Further Match** for the **Filter** setting. Then, click **OK**.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 2

☑ Enable

Comments	block_all
Schedule Profile	None ▼ , None ▼ , None ▼ , None ▼
	☐ Clear sessions when schedule is ON

Direction	LAN/RT/VPN -> WAN ▼ [Advanced]
Source IP/Country	Any [Edit]
Destination IP/Country	Any [Edit]
Service Type	Any [Edit]
Fragments	Don't Care ▼

Application	Action/Profile	Syslog
Filter	Block If No Further Match ▼	☐
Branch to Other Filter Set	None ▼	

ℹ️

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

4. Next, set another rule. Just open **Firewall>>Filter Setup**. Click the **Set 2** link and choose the **Filter Rule 3** button.

5. Check **Enable** to enable the filter rule. Type the comments (e.g., **open_ip**). Click the **Edit** button for **Source IP**.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 3

☑ Enable

Comments	open_ip
Schedule Profile	None ▼ , None ▼ , None ▼ , None ▼
	☐ Clear sessions when schedule is ON

Direction	LAN/RT/VPN -> WAN ▼ [Advanced]
Source IP/Country	Any [Edit]
Destination IP/Country	Any [Edit]
Service Type	Any [Edit]
Fragments	Don't Care ▼

6. A dialog box will be popped up. Choose **Range Address** as **Address Type** by using the drop down list. Type 192.168.1.10 in the field of **Start IP**, and type 192.168.1.20 in the field of **End IP**. Then, click **OK** to save the settings. The computers within the range can access into the Internet.
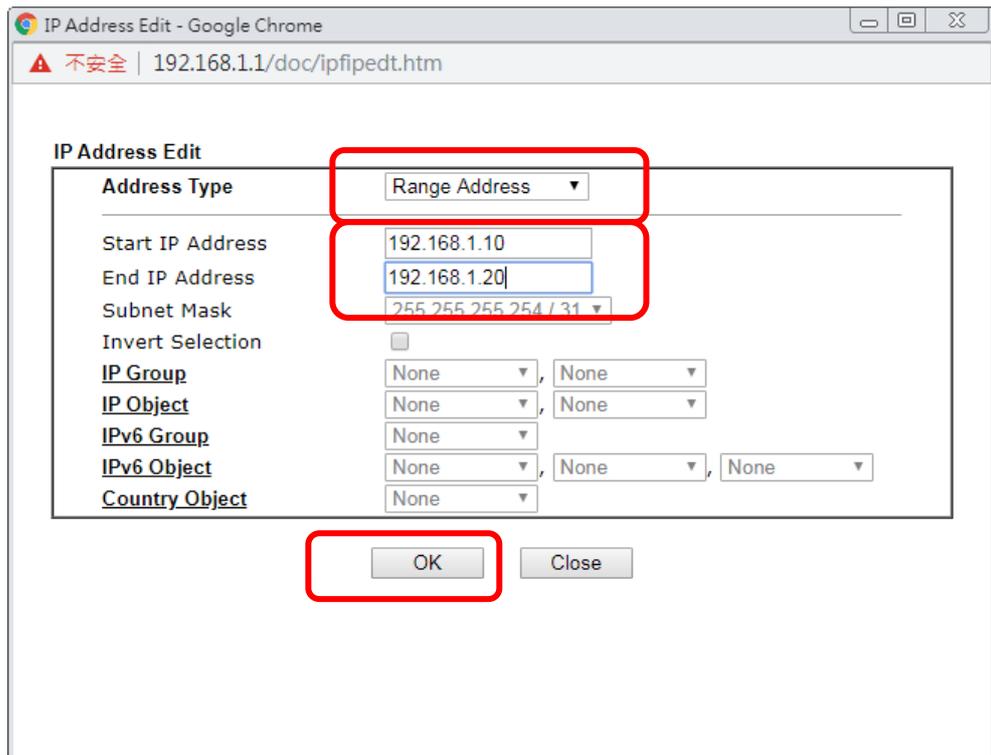
7. Now, check the content of **Source IP** is correct or not. The action for **Filter** shall be set with **Pass Immediately.** Then, click **OK** to save the settings.
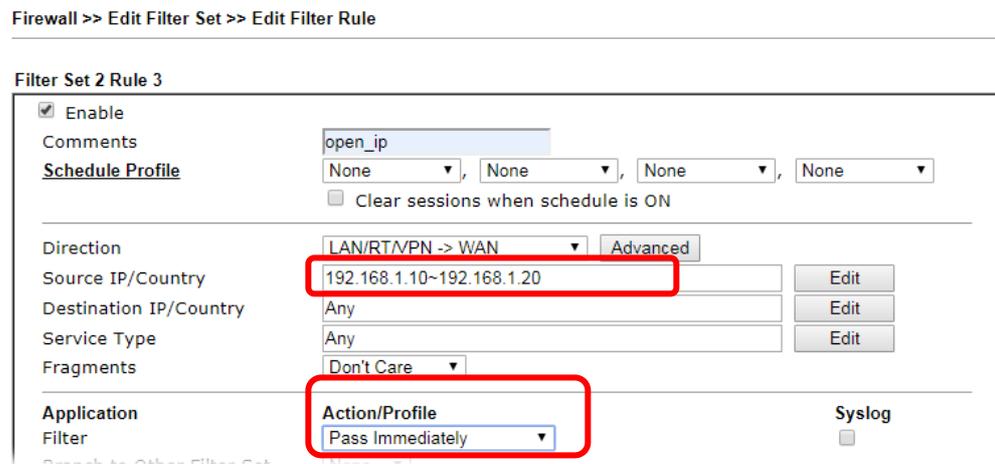
8. Both filter rules have been created. Click **OK**.
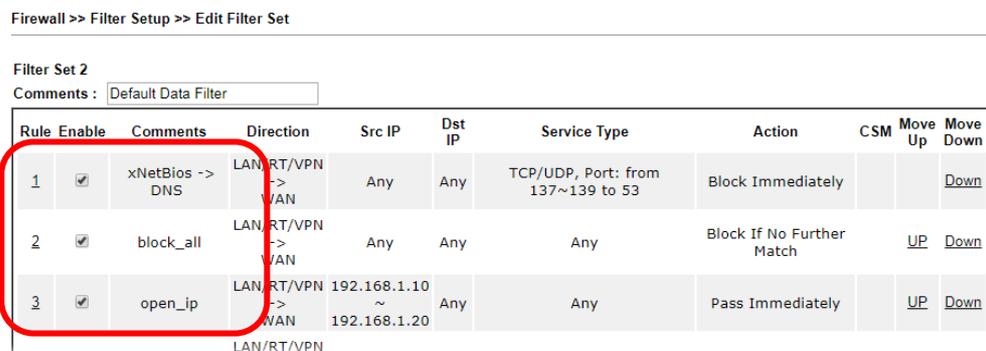
Now, all the settings are configured well. Only the computers with the IP addresses within 192.168.1.10 ~ 192.168.1.20 can access to Internet.

IV-2 CSM (Central Security Management)

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

APP Enforcement Filter

As the popularity of all kinds of instant messenger application arises, communication cannot become much easier. Nevertheless, while some industry may leverage this as a great tool to connect with their customers, some industry may take reserved attitude in order to reduce employee misusage during office hour or prevent unknown security leak. It is similar situation for corporation towards peer-to-peer applications since file-sharing can be convenient but insecure at the same time. To address these needs, we provide CSM functionality.

URL Content Filter

To provide an appropriate cyberspace to users, Vigor router equips with **URL Content Filter** not only to limit illegal traffic from/to the inappropriate web sites but also prohibit other web feature where malicious code may conceal.

Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines to teenagers. At office, **URL Content Filter** can also provide a job-related only environment hence to increase the employee work efficiency. How can URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.

On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from websites, you may risk bringing threat to your system. For example, an ActiveX control object is usually used for providing interactive web feature. If malicious code hides inside, it may occupy user's system.

Web Content Filter

We all know that the content on the Internet just like other types of media may be inappropriate sometimes. As a responsible parent or employer, you should protect those in your trust against the hazards. With Web filtering service of the Vigor router, you can protect your business from common primary threats, such as productivity, legal liability, network and security threats. For parents, you can protect your children from viewing adult websites or chat rooms.

Once you have activated your Web Filtering service in Vigor router and chosen the categories of website you wish to restrict, each URL address requested (e.g.www.bbc.co.uk) will be checked against our server database. This database is updated as frequent as daily by a global team of Internet researchers. The server will look up the URL and return a category to your router. Your Vigor router will then decide whether to allow access to this site according to the categories you have selected. Please note that this action will not introduce any delay in your Web surfing because each of multiple load balanced database servers can handle millions of requests for categorization.

Info	The priority of URL Content Filter is higher than Web Content Filter.

Web User Interface

IV-2-1 APP Enforcement Profile

You can define policy profiles for IM (Instant Messenger)/P2P (Peer to Peer)/Protocol/Misc application. This page allows you to set 32 profiles for different requirements. The APP Enforcement Profile will be applied in **Default Rule** of **Firewall>>General Setup** for filtering.

CSM >> APP Enforcement Profile

APP Enforcement Profile Table:　　　　　　　　　　　　　　　　| **Set to Factory Default** |

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

Available settings are explained as follows:

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

Click the number under Index column for settings in detail.

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
Select All	Click it to choose all of the items in this page.
Clear All	Uncheck all the selected boxes.
Enable	Check the box to select the APP to be blocked by Vigor router.

The profiles configured here can be applied in the **Firewall>>General Setup** and **Firewall>>Filter Setup** pages as the standard for the host(s) to follow.

IV-2-2 URL Content Filter Profile

To provide an appropriate cyberspace to users, Vigor router equips with **URL Content Filter** not only to limit illegal traffic from/to the inappropriate web sites but also prohibit other web feature where malicious code may conceal.

Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines to teenagers. At office, **URL Content Filter** can also provide a job-related only environment hence to increase the employee work efficiency. How can URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.

On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from websites, you may risk bringing threat to your system. For example, an ActiveX control object is usually used for providing interactive web feature. If malicious code hides inside, it may occupy user's system.

For example, if you add key words such as "sex", Vigor router will limit web access to web sites or web pages such as "www.sex.com", "www.backdoor.net/images/sex/p_386.html". Or you may simply specify the full or partial URL such as "www.sex.com" or "sex.com".

Also the Vigor router will discard any request that tries to retrieve the malicious code.

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

Each item is explained as follows:

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

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

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

CSM >> URL Content Filter Profile

Profile Index: 1

Profile Name:	[ ]
Priority:	Either : URL Access Control First ▾ **Log:** Block ▾

1.URL Access Control

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

Action: Group/Object Selections

Pass ▾   [   ]   Edit

☐ Exception List   [   ]   Edit

2.Web Feature

☐ Enable Web Feature Restriction

Action:

Pass ▾   **File Extension Profile:** None ▾   ☐ Cookie   ☐ Proxy   ☐ Upload

OK   Clear   Cancel

Available settings are explained as follows:

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

	Either : URL Access Control First ▼ Both : Pass Both : Block Either : URL Access Control First Either : Web Feature First
Log	**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. Block ▼ Pass Block All from IP a
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 router 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. **Exception List** – Specify the object profile(s) as the exception list which will be processed in an opposite manner to the action selected above. **Group/Object Selections** – The Vigor router provides several frames for users to define keywords and each frame supports multiple keywords. The keyword could be a noun, a partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or semicolon. In addition, the maximal length of each frame is 32-character long. After specifying keywords, the Vigor router will decline the connection request to the website whose URL string matched to any user-defined keyword. It should be noticed that the more simplified the blocking keyword list is, the more efficiently the Vigor router performs.

Vigor3910 Series User's Guide

	Object/Group Edit **Keyword Object** — None ▼ or Keyword Object — None ▼ or Keyword Object — None ▼ or Keyword Object — None ▼ or Keyword Object — None ▼ or Keyword Object — None ▼ or Keyword Object — None ▼ or Keyword Object — None ▼ or **Keyword Group** — None ▼ or Keyword Group — None ▼ or Keyword Group — None ▼ or Keyword Group — None ▼ or Keyword Group — None ▼ or Keyword Group — None ▼ or Keyword Group — None ▼ or Keyword Group — None ▼ OK Close
Web Feature	**Enable Web Feature Restriction -** Check this box to make the keyword being blocked or passed. **Action -** This setting is available only when **Either: URL Access Control First** or **Either: Web Feature First** is selected. ● **Pass -** Allow accessing into the corresponding webpage with the keywords listed on the box below. ● **Block -** Restrict accessing into the corresponding webpage with the keywords listed on the box below. If the web pages do not match with the specified feature set here, it will be processed with reverse action. **Cookie -** Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy. **Proxy -** Check the box to reject any proxy transmission. To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages. **Upload –** Check the box to block the file upload by way of web page. **File Extension Profile –** Choose one of the profiles that you configured in **Object Setting>> File Extension Objects** previously for passing or blocking the file downloading. File Extension Profile: None ▼ None 1-image

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

IV-2-3 Web Content Filter Profile

There are three ways to activate WCF on vigor router, using **Service Activation Wizard**, by means of **CSM>>Web Content Filter Profile** or via **System Maintenance>>Activation**.

Service Activation Wizard allows you to use trial version of WCF directly without accessing into the server (*MyVigor*) located on http://myvigor.draytek.com.

However, if you use the **Web Content Filter Profile** page to activate WCF feature, it is necessary for you to access into the server (*MyVigor*) located on http://myvigor.draytek.com. Therefore, you need to register an account on http://myvigor.draytek.com for using corresponding service. Please refer to section of creating MyVigor account.

WCF adopts the mechanism developed and offered by certain service provider (e.g., DrayTek). No matter activating WCF feature or getting a new license for web content filter, you have to click **Activate** to satisfy your request. Be aware that service provider matching with Vigor router currently offers a period of time for trial version for users to experiment. If you want to purchase a formal edition, simply contact with the channel partner or your dealer.

Click **CSM** and click **Web Content Filter Profile** to open the profile setting page. The default setting for Setup Query Server /Setup Test Server is **auto-selected**. You can choose another server for your necessity by clicking **Find more** to open http://myvigor.draytek.com for searching another qualified and suitable one.

Info 1	Web Content Filter (WCF) is not a built-in service of Vigor router but a service powered by Commtouch. If you want to use such service (trial or formal edition), you have to perform the procedure of activation first. For the service of formal edition, please contact with your dealer/distributor for detailed information.
Info 2	Commtouch is merged by Cyren, and GlobalView services will be continued to deliver powerful cloud-based information security solutions! Refer to: http://www.prnewswire.com/news-releases/commtouch-is-now-cyren-239 025151.html

Available settings are explained as follows:

Item	Description
Activate	Click it to access into MyVigor for activating WCF service.
Setup Query Server	It is recommended for you to use the default setting, auto-selected. You need to specify a server for categorize searching when you type URL in browser based on the web content filter profile.
Setup Test Server	It is recommended for you to use the default setting, auto-selected.
Find more	Click it to open http://myvigor.draytek.com for searching another qualified and suitable server.
Cache	**None** – the router will check the URL that the user wants to access via WCF precisely, however, the processing rate is normal. Such item can provide the most accurate URL matching. **L1** – the router will check the URL that the user wants to access via WCF. If the URL has been accessed previously, it will be stored in the router to be accessed quickly if required. Such item can provide accurate URL matching with faster rate. **L2** – the router will check the URL that the user wants to access via WCF. If the data has been accessed previously, the IP addresses of source and destination IDs will be memorized for a short time (about 1 second) in the router. When the user tries to access the same destination ID, the router will check it by comparing the record stored. If it matches, the page will be retrieved quickly. Such item can provide URL

	matching with the fastest rate.
	L1+L2 Cache - the router will check the URL with fast processing rate combining the feature of L1 and L2.
Set to Factory Default	Click this link to retrieve the factory settings.
Default Message	You can type the message manually for your necessity or click this button to get the default message which will be displayed on the field of **Administration Message**.

Eight profiles are provided here as Web content filters. Simply click the index number under Profile to open the following web page.

The items listed in Categories will be changed according to the different service providers. If you have and activate another web content filter license, the items will be changed simultaneously. All of the configuration made for web content filter will be deleted automatically. Therefore, please backup your data before you change the web content filter license.

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.
Log	**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.
Black/White List	**Enable** – Activate white/black list function for such profile. **Group/Object Selections** – Click **Edit** to choose the group or object profile as the content of white/black list.
	Pass - **allow** accessing into the corresponding webpage with the characters listed on **Group/Object Selections**. If the web pages do not match with the specified feature set here, they

	will be processed with the categories listed on the box below.
	Block - **restrict** accessing into the corresponding webpage with the characters listed on **Group/Object Selections**. If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below.
Action	**Pass** - allow accessing into the corresponding webpage with the categories listed on the box below.
	Block - restrict accessing into the corresponding webpage with the categories 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.

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

IV-2-4 DNS Filter Profile

The DNS Filter monitors DNS queries on UDP port 53 and will pass the DNS query information to the WCF to help with categorizing HTTPS URL's.

DNS can be specified in **LAN>>General Setup** by using the server (e.g., 168.95.1.1) on router or external DNS server (e.g., 8.8.8.8). If the router server is used, **DNS Filter General Setting** will be applied to DNS query from clients on LAN. However, if the external DNS server is used, **DNS Filter Profile** will be applied to DNS query coming from clients on LAN.

Info	For DNS filter must use the WCF service profile to filter the packets, therefore WCF license must be activated first. Otherwise, DNS filter does not have any effect on packets.

CSM >> DNS Filter

DNS Filter Profile Table | Set to Factory Default|

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

Note:
To make DNS Filter profile effective, please go to **Firewall >> Filter Setup** page to create a firewall rule and select the desired profile.

DNS Filter Local Setting

DNS Filter	☐ Enable
Web Content Filter	None ▼
URL Content Filter	None ▼
Syslog	None ▼
Black/White List	☐ Enable Blacklist ▼
Address Type	Any Address ▼
Start IP Address	0.0.0.0
End IP Address	0.0.0.0
Subnet Mask	0.0.0.0
IP Group	None ▼
or IP Group	None ▼
or **IP Object**	None ▼
or IP Object	None ▼

Administration Message   (Max 255 characters)   [Default Message]

```
<body><center><br><br><br><p>The requested Web page <br> from %SIP% <br>to %URL% <br>that is
categorized with %CL% <br>has been blocked by %RNAME% DNS Filter.<p>Please contact your
system administrator for further information.</center></body>
```

Legend:
%SIP%   - Source IP ,   %URL%   - URL
%CL%   - Category ,   %RNAME%   - Router Name

[OK] [Cancel]

Available settings are explained as follows:

Item	Description
DNS Filter Profile Table	It displays a list of different DNS filter profiles (with

	specified WCF and UCF).
	Click the profile link to open the following page. Then, type the name of the profile and specify WCF/UCF based on your requirement.
DNS Filter Local Setting	**DNS Filter Local Setting** will be applied to DNS query from clients on LAN when router's DNS server is used.
	DNS Filter - Check Enable to enable such feature.
	Web Content Filter- Set the filtering conditions.
	URL Content Filter - Set the filtering conditions.
	Syslog - The filtering result can be recorded according to the setting selected for Syslog.
	● **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.
	Black/White List – Specify IP address, subnet mask, IP object, or IP group as a black list or white list for DNS packets passing through or blocked by Vigor router.
Administration Message	When DNS packets are blocked by DNS filter, a web page containing the description listed on Administration Message will be shown on the screen.
	Type the words or sentences which will be displayed when a web page is blocked by Vigor router. You can type the message manually for your necessity or click **Default Message** button to get the default text displayed on the field of **Administration Message**.

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

Application Notes

A-1 How to Create an Account for MyVigor

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

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

Create an Account via Vigor Router

1. Click **CSM>> Web Content Filter Profile**. The following page will appear.

    Or

    Click **System Maintenance>>Activation** to open the following page.

2. Click the **Activate** link. A login page for MyVigor web site will pop up automatically.

3. Click the link of **Create an account now**.

4. The system will ask if you are 16 years old or over.

    ■ If yes, click **I am 16 or over**.
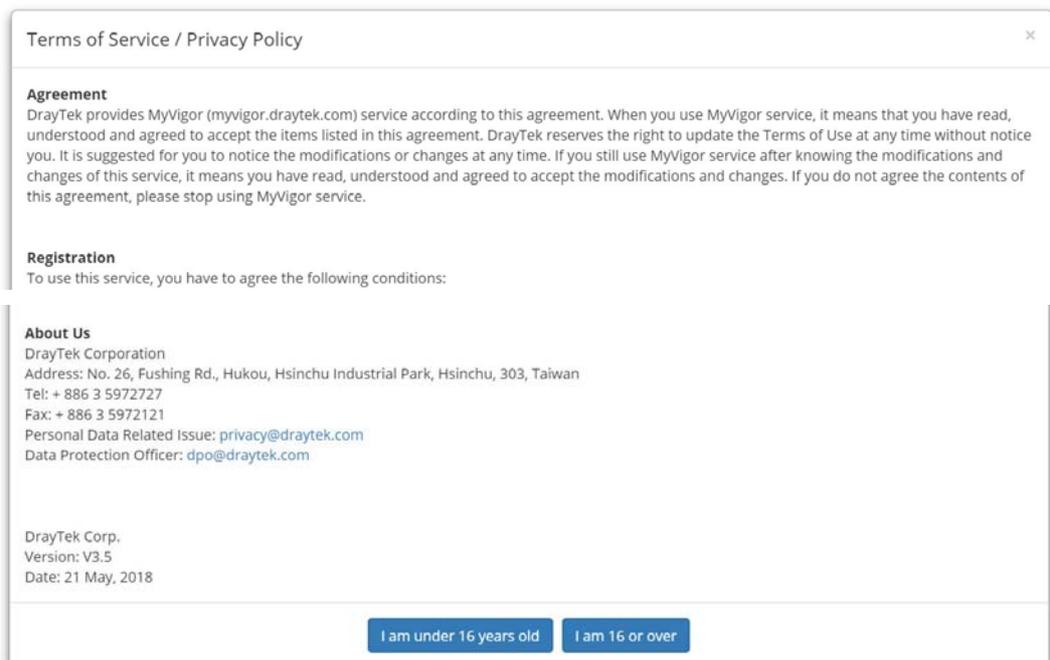
■ If not, click **I am under 16 years old** to get the following page. Then, click **I and my legal guardian agree**.

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

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

7. Choose proper selection for your computer and click **Continue**.
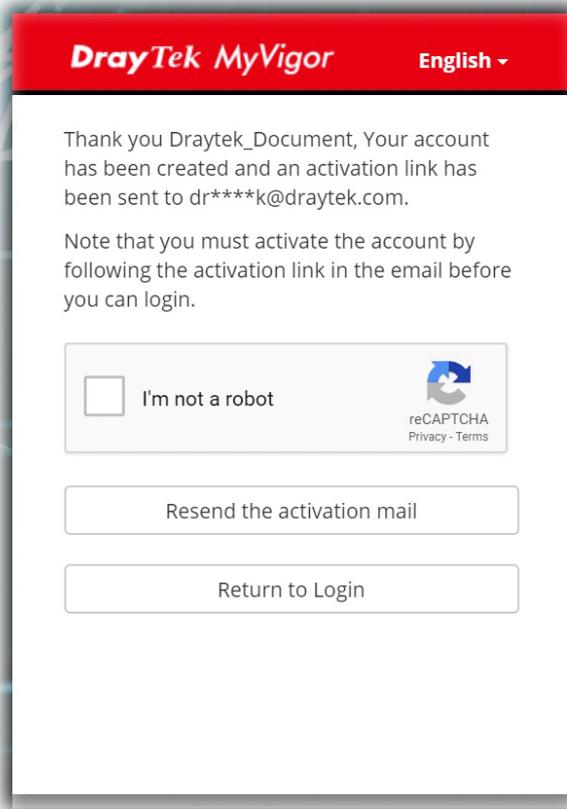
8. Now you have created an account successfully.

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

10. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.
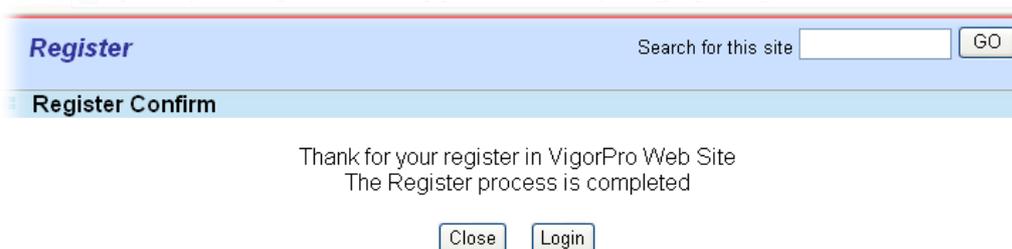
11. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**.
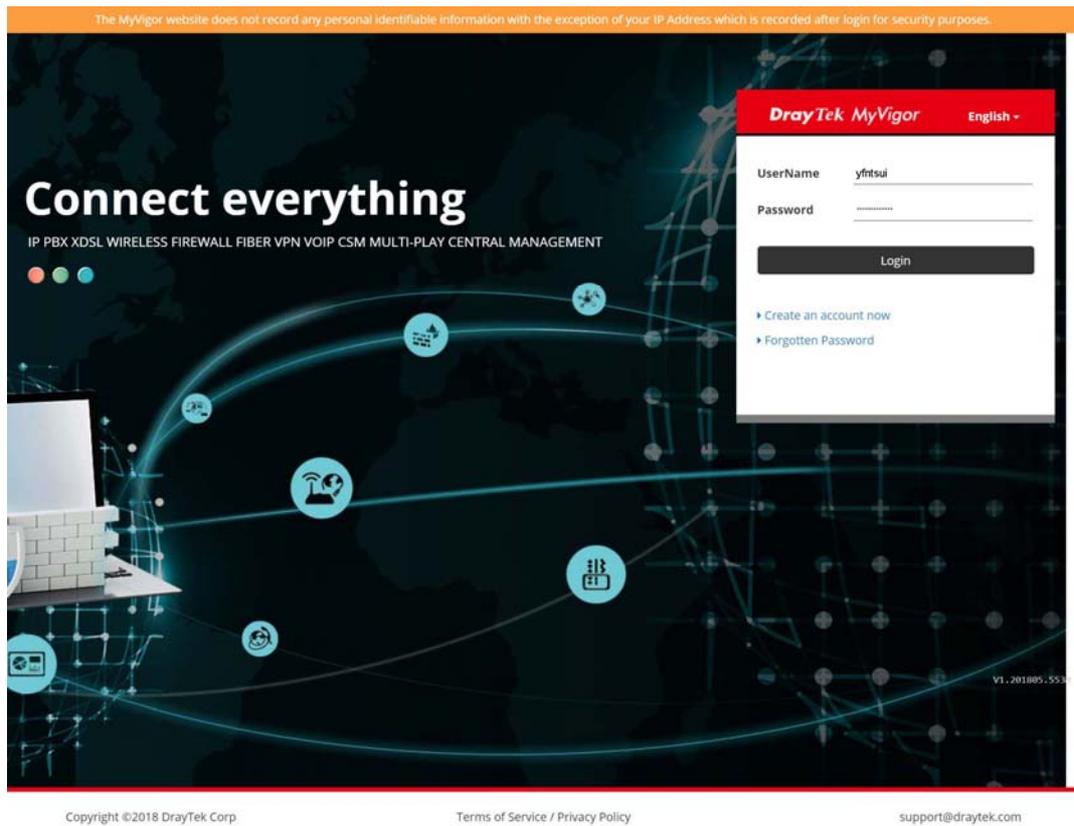
12. Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

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

There are two ways to block the facebook service, Web Content Filter and URL Content Filter.

Web Content Filter,

Benefits: Easily and quickly implement the category/website that you want to block.

Note: License is required.

URL Content Filter,

Benefits: Free, flexible for customize webpage.

Note: Manual setting (e.g., one keyword for one website.)

I. Via Web Content Filter

1. Make sure the Web Content Filter license is valid.

2. Open **CSM** >> **Web Content Filter Profile** to create a WCF profile. Check **Social Networking** with **Action**, **Block**.

3. Select this profile in **Firewall**>>**General Setup**>>**Default Rule**.

4. Next time when someone accesses facebook via this router, the web page would be blocked and the following message would be displayed instead.

The requested Web page
from 192.168.2.114
to www.facebook.com/
that is categorized with [Social Networking]
has been blocked by Web Content Filter.

Please contact your system administrator for further information.

[Powered by DrayTek]

II. Via URL Content Filter

A. Block the web page containing the word of "Facebook"

1. Open **Object Settings**>>**Keyword Object**. Click an index number to open the setting page.

2. In the field of **Contents**, please type *facebook*. Configure the settings as the following figure.

Objects Setting >> Keyword Object Setup

Profile Index : 1

| Name | Facebook |
| Contents | facebook |

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

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

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

OK   Clear   Cancel

3. Open **CSM>>URL Content Filter Profile**. Click an index number to open the setting page.

4. Configure the settings as the following figure.

CSM >> URL Content Filter Profile

Profile Index: 1

| Profile Name: | Facebook |
| Priority: | Either : URL Access Control First ▼   **Log:**   All ▼ |

1.URL Access Control

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

Action: Group/Object Selections

Pass ▼   Facebook   Edit

☐ Exception List   Edit

2.Web Feature

☐ Enable Web Feature Restriction

Action:

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

OK   Clear   Cancel

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

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

B. Disallow users to play games on Facebook

1. Open **Object Settings**>>**Keyword Object**. Click an index number to open the setting page.

2. In the field of **Contents**, please type *apps.facebook*. Configure the settings as the following figure.

Vigor3910 Series User's Guide

3. Open **CSM>>URL Content Filter Profile**. Click an index number to open the setting page.

4. Configure the settings as the following figure.

5. When you finished the above steps, please open **Firewall>>General Setup**.

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

A-3 How to use APP Enforcement to block application like Facebook, YouTube or TeamViewer?

APP Enforcement helps network administrator to block applications on LAN network. Draytek routers provide a few categories to set up the profiles e.g., IM, P2P, Protocol, Stream, Remote control.

This section is going to demonstrate how to use APP Enforcement to block Facebook, Skype, YouTube and TeamViewer.
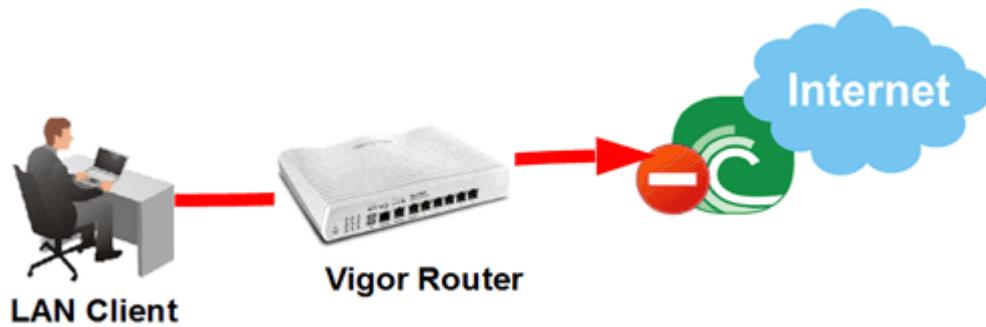
1. Create an APP Enforcement Profile: Click on an Index number to create a new profile at CSM >> **APP Enforcement Profile**.

CSM >> APP Enforcement Profile

APP Enforcement Profile Table: | Set to Factory Default |

Profile	Name	Profile	Name
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	

2. Set up the details in the profile.

(a) Enter Profile Name.

(b) Choose the Facebook in Instant Message.

(c) Choose Skype in VoIP.

(d) Choose YouTube in Stream.

(e) Choose TeamViewer in Remote control.

(f) Click **OK** to save.

3. Apply the APP Enforcement Profile to a Firewall Filter Rule. Go to **Firewall** >> **Filter Setup**, and click an available set.

4. Click on a Filter Rule index to set up a filter.

5. Set up the details in the profile.

(a) Enable the Filter Rule.

(b) Put the comments of this rule.

(c) Select the Direction as **LAN/DMZ/RT/VPN -> WAN**.

(d) Edit the **Source IP** which should be blocked from the APP.

(e) Select Filter as **Pass Immediately**.

(f) Select APP Enforcement as the profile we created in Step 2.

(g) You may also check the **Syslog** if needed.

(h) Click **OK** to save.

6. With the above configuration, LAN clients cannot be able to use the APP and website.

This site can't provide a secure connection

www.facebook.com sent an invalid response.

Try running Windows Network Diagnostics.

ERR_SSL_PROTOCOL_ERROR

This page is left blank.

Part V Management

System Maintenance

There are several items offered for the Vigor router system setup: System Status, TR-069, Administrator Password, User Password, Login Page Greeting, Configuration Backup, Configuration Export, Syslog /Mail Alert, Time and Date, SNMP, Management, Self-Signed Certificate, Reboot System, Firmware Upgrade, Activation, Internal Service User List and Dashboard Control.

Bandwidth Management

It is used to control the bandwith of data transmission through configuration of Sessions Limit, Bandwidth Limit, and Quality of Servie (QoS).

User Management

It is a security feature which disallows any IP traffic (except DHCP-related packets) from a particular host until that host has correctly supplied a valid username and password.

V-1 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: System Status, TR-069, Administrator Password, User Password, Login Page Greeting, Configuration Backup, Syslog /Mail Alert, Time and Date, Management, Panel Control, Reboot System, Firmware Upgrade, Activation, Internal Service User List and Dashboard Control.

Below shows the menu items for System Maintenance.
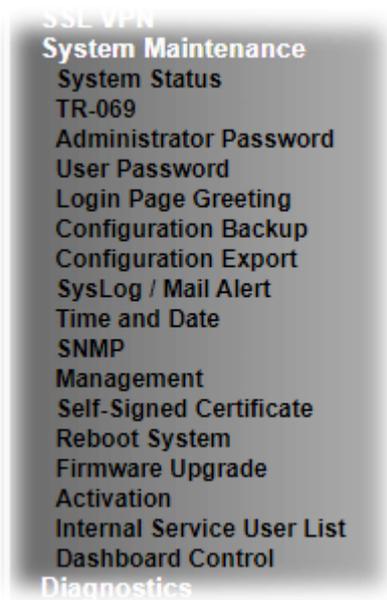
Web User Interface

V-1-1 System Status

The System Status displays basic network information of Vigor router including LAN and WAN interface status. Also available is the current firmware version and firmware related information.

System Status

Model Name   : Vigor3910
Firmware Version   : 3.9.1.2
Build Date/Time   : Dec 4 2019 14:21:52

LAN	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-1D-AA-4B-3E-80	192.168.1.1	255.255.255.0	Yes	8.8.8.8
IP Routed Subnet	00-1D-AA-4B-3E-80	192.168.0.1	255.255.255.0	Yes	8.8.8.8

WAN	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Disconnected	00-1D-AA-4B-3E-81	DHCP Client	---	---
WAN3	Disconnected	00-1D-AA-4B-3E-83	DHCP Client	---	---
WAN5	Disconnected	00-1D-AA-4B-3E-85	DHCP Client	---	---
WAN6	Disconnected	00-1D-AA-4B-3E-86	DHCP Client	---	---
WAN7	Disconnected	00-1D-AA-4B-3E-87	DHCP Client	---	---
WAN8	Disconnected	00-1D-AA-4B-3E-88	DHCP Client	---	---

IPv6	Address		Scope	Internet Access Mode
LAN	FE80::21D:AAFF:FE4B:3E80/64		Link	---

User Mode is OFF now.

Available settings are explained as follows:

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

	MAC Address
	- Displays the MAC address of the WAN Interface.
	Connection
	- Displays the connection type of the WAN interface..
	IP Address
	- Displays the IP address of the WAN interface.
	Default Gateway
	- Displays the assigned IP address of the default gateway.
IPv6	**Address -** Displays the IPv6 address for LAN.
	Scope - Displays the scope of IPv6 address. For example, **IPv6 Link Local** is non-routable and can only be used for local connections.
	Internet Access Mode – Displays the connection mode of the WAN interface.

V-1-2 TR-069

This device supports the TR-069 standard for remote management of customer-premises equipment (CPE) through an Auto Configuration Server, such as VigorACS.

V-1-2-1 ACS and CPE Settings

Available settings are explained as follows:

Item	Description
TR-069	Enables or disables TR-069 functionality.
ACS Server On	Choose the interface for connecting the router to the Auto Configuration Server.
ACS Server	This section specifies the settings of the ACS Server. **URL** – Enter the URL for connecting to the ACS. Please refer

	to the Auto Configuration Server user's manual for detailed information. ● **Wizard** – Click it to enter the IP address of VigorACS server, port number and the handler. ● **Acquire URL form DHCP option 43** – Select to acquire the ACS URL from DHCP option 43. **Username/Password** – Enter the credentials required to connect to the ACS server. ● **Test With Inform** – Click to send an inform message using the selected Event Code to test if the CPE is able to communicate with the VigorACS server. ● **Event Code** - Select an event for the inform test. **Last Inform Response Time** –Displays the time of the most recent Inform Response message received from the VigorACS.
CPE Client	This section specifies the settings of the CPE Client. **Protocol** – Select Https if the connection is encrypted; otherwise select Http. **Port** – In the event of port conflicts, change the port number of the CPE. **Username** and **Password** – Enter the username and password that the VigorACS will use to connect to the CPE.
Periodic Inform Settings	**Enable** – The default setting is Enable, which means the CPE Client will periodically connect to the ACS Server to update its connection parameters at intervals specified in the Interval Time field. ● **Time Interval** - Please set interval time or schedule time for the router to send notification to CPE. **Disable** - Select **Disable** to turn off periodic notifications.
STUN Settings	STUN allows the ACS Server to connect to the CPE Client even when the client is behind a network address translator (NAT). **Disable** - The default setting is Disable. **Enable** - Please Enter the relational settings listed below: ● **Server Address** – Enter the IP address of the STUN server. ● **Server STUN Port** – Enter the port number of the STUN server. ● **Minimum Keep Alive Period** – If STUN is enabled, the CPE must periodically transmit binding requests to the server for the purpose of maintaining the binding with the Gateway. Enter the minimum interval between keep-alive messages that the CPE client sends to the ACS server. The default setting is 60 seconds. ● **Maximum Keep Alive Period** – If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding with the Gateway. Enter the maximum interval between keep-alive messages that the CPE client sends to the ACS server. A value of -1 indicates that no maximum period is specified.
Apply Settings to APs	This feature is able to apply TR-069 settings (including STUN and ACS server settings) to all of APs managed by Vigor2865 at the same time.

	Disable – TR-069 and Related settings will not be applied to VigorAPs. **Enable** – TR-069 settings will be applied to VigorAPs after clicking **OK**. The VigorAP password must be specified. ● **AP Password** – Enter the password of the VigorAP that you want to apply Vigor router's TR-069 settings. **Specify STUN Settings for APs** – After clicking the **Enable** radio button for Apply Settings to APs, if you want to apply specific STUN settings (i.e., different from the Vigor2865 STUN settings) to VigorAPs to meet specific requirements, check this box and enter the server IP address, server port, and minimum and maxmum keep alive periods respectively.
Bandwidth Utilisation Notification Settings	This feature allows the ACS Server to be notified when bandwidth usage has been exceeded on the router. **Enable / Disable** – Select to enable or disable the featur. ● **Time Period** – Select the frequency of the notifications (15 mins, 30 mins, 1hour, 3 hours, or 6 hours). ● **WAN** – Select the WAN interfaces to be monitored and reported. ● **Threshold Level** – Sets the utilization percentages (of the preset Tx and Rx Line Speeds) when Medium or High Usage notifications should be sent. ● **Line Speed** – Enter the Tx and Rx bandwidths of the WAN interface.

Select **OK** to save changes on the page, or **Clear** to reset all settings to factory defaults.

V-1-2-2 Reporting Configuration

Information related to the router's health are divided into several categories and listed in this field. After checking the item(s), Vigor router will arrange and send corresponding data to VigorACS as a reference for the system administrator.

Available settings are explained as follows:

Item	Description
Health Parameters	Check the one that Vigor router will send the status information to VigorACS. **Threshold** (for VoIP R-Factor) - Once the quality of VoIP is lower than warning limit value or critical limit value, the router will send the result to VigorACS.
CPE Notification Settings	**Enable** - Check the box to select the notification item(s). Vigor router will send the utilization status to VigorACS.

Click **OK** to save changes on the page.

V-1-2-3 Export Parameters

Click **Export** to save the TR-069 parameter settings as an ".xml".

System Maintenance >> TR-069 Setting

ACS and CPE Settings	Reporting Configuration	Export Parameters

Export

Export tr069 parameters by xml.

Export

V-1-3 Administrator Password

This page allows you to set or change the administrator password.

Available settings are explained as follows:

Item	Description
Administrator Password	The administrator can login web user interface of Vigor router to modify all of the settings to fit the requirements. **Old Password** - Enter the current password. The factory default is "admin". **New Password** - Enter the new password. The maximum length of the password is 23 characters. **Confirm Password** – Enter the new password again for confirmation. **Enable 'admin' account login to Web UI from the Internet** – Select to allow the administrator to log in from the Internet. This option is enabled when Administrator Local User is enabled (see below). **Use only advanced authentication method for Admin "WAN" login** – Advanced authentication method can offer a **more secure** network connection. Select to require mOTP or 2-step authentication when logging in from the WAN. ● **Mobile one-Time Password (mOTP)** – Select to allow the use of mOTP passwords. Enter the PIN Code and Secret settings for getting one-time passwords. ● **2-Step Auth code via <u>SMS Profile</u> and/or <u>Mail Profile</u>** – Select the SMS and/or Mail profiles and the destination SMS number and/or email address for transmitting the password.
Administrator Local User	Usually, the system administrator has the highest privilege to modify the settings on the web user interface of the Vigor router. However, in some cases, it might be necessary to have other users in LAN to access into the web user interface of Vigor router. This feature allows you to add more administrators who can then log in to the web interface, with the same privileges as the administrator. **Enable Local User** – Check the box to allow other users to administer the router. ● **Use only advanced authentication method for Admin "WAN" login** – Advanced authentication method can offer a **more secure** network connection. In general, the above basic password setting will be used for authentication if such option is disabled. Simply check the box to enable the following settings. ● **Local User List** – Shows all the users that are set up to administer the router. ● **Specific User –** Create the new user account as the local user. Then specify the authentication method (dividing into Basic and Advanced) for the user account. ➢ **User Name** – Enter a user name. ● **Authentication method –** Select from **Basic** or **Advanced** authentication methods. **Basic** – Static passwords will be used to authenticate users. ➢ **Local Password** – Enter the password for the local user. **Advanced** - Mobile One-time Passwords (mOTP) or

	2-step authentication will be used to authenticate users.
	➢ **Mobile one-Time Password (mOTP)** – Select to allow the use of mOTP passwords. Enter the mOTP PIN Code and Secret that will be used to generate the one-time passwords.
	➢ **2-Step Authentication via SMS Profile and/or Mail Profile –** Select the SMS and/or Mail profiles and the destination SMS number and/or email address for transmitting the password.
	● **Add** – After entering the user name and password above, click this button to create a new local user. The new user will be shown on the Local User List immediately.
	● **Edit** – If you wish to change a user in the Local User List, select it, perform the necessary modifications, and click this button to update the user.
	● **Delete** - If you wish to delete a user in the Local User List, select it and click this button to remove it.
Administrator LDAP Setting	**Enable LDAP/AD login for admin users** – Select to allow authentication using an LDAP/Active Directory Server.
	LDAP Server Profiles Setup – Click to set up the LDAP/Active Directory server.

Click **OK** to save changes on the page, and you will be directed to the login screen. Please log in with the new password.

V-1-4 User Password

This page allows you to set new password for user operation.

Available settings are explained as follows:

Item	Description
Enable User Mode for simple web configuration	Check this box to enable User Mode for web user interface with the password typed here for simple web configuration.
	The simple web user interface settings differ from those on the full web user interface seen when logged in using the administrator password.
Password	Enter the password. The maximum length of the password is 31 characters.
Confirm Password	Enter the password again for verification.
Password Strength	Shows the security strength of the password specified above.
Set to Factory Default	Click to return to the factory default setting.

Click **OK** to save changes on the page, and you will be directed to the login screen. Please window will appear. Please log in with the new password.

Here are the steps involved in setting up the router for User Mode Access:

1. Navigate to **System Maintenance>>User Password** in the web user interface.

2. Check the box of **Enable User Mode for simple web configuration** to enable user mode operation. Enter a new password in the field of New Password and click **OK**.

System Maintenance >> User Password

☑ Enable User Mode for simple web configuration

User Password | **Set to Factory Default** |

Password	••••••••
Confirm Password	•••••••• (Max. 23 characters allowed)
Password Strength:	Weak	Medium	Strong

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

Note:

1. Password can contain a-z A-Z 0-9 , ; : . " < > * + = | ? @ # ^ ! ( )
2. Password can't be all asterisks(*). For example, '*' or '***' is illegal, but '123*' or '*45' is OK.

OK

3. The following screen will appear. Simply click **OK**.

System Maintenance >> User Password

Active Configuration

Password : *****

4. Log out the Vigor router web user interface by clicking the Logout button.

Logout
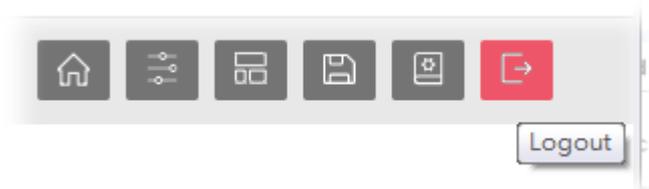
5. The following window will be shown. Enter the new user password in the Password field and click **Login**.

DrayTek

Vigor 3910

Username

Password

••••••••••

Login

6. The main screen with User Mode will be shown:
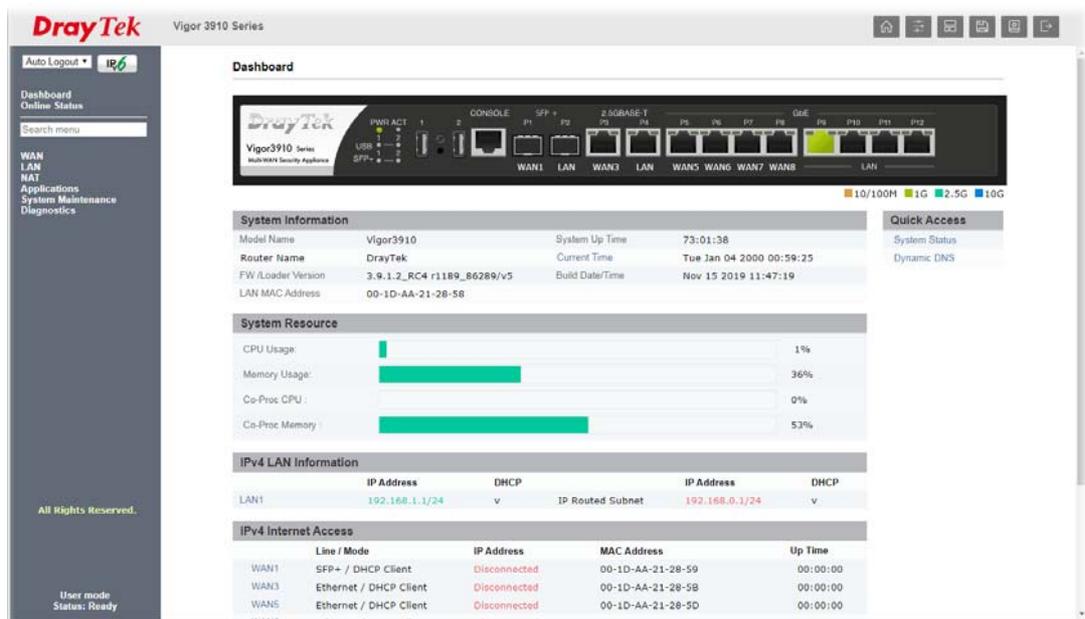
Only basic settings are available in User Mode. These are a subset of the Admin Mode settings.

Info	Setting in User Mode can be configured as same as in Admin Mode.

V-1-5 Login Page Greeting

When you want to access into the web user interface of Vigor router, the system will ask you to offer username and password first. At that moment, the background of the web page is blank and no heading will be displayed on the Login window. This page allows you to specify login URL and the heading on the Login window if you have such requirement.

This section allows you to customize the login page by adding a message and/or setting the page title.

System Maintenance >> Login Page Greeting

Login Page Greeting

☐ Enable

Login Page Title   Router Login   (31 char max.)

Welcome Message and Bulletin (Max 511 characters)   **Preview**| **Set to Factory Default** |

```
<h1><b><font color=red>Welcome Message</font></b></h1><p>This welcome
message is displayed in the Login page of the router. Replace this text
with your own message. </p><ol><li>The welcome message can be written in
HTML so lists such as this one can be created </li><li>Other markup tags
such as p, font or img can be used</li></ol>
```

Examples of Welcome Message and Bulletin:
```
<h1><b><font color=red>Welcome Message</font></b></h1>
<p>Message</p>
```

OK   Cancel

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable the login customization function.
Login Page Title	Enter a brief description (e.g., Welcome to DrayTek) which will be shown on the heading of the login dialog.
Welcome Message and Bulletin	Enter words or sentences here. It will be displayed for bulletin message. In addition, it can be displayed on the login dialog at the bottom. Note that do not enter URL redirect link here.
Preview	Click to preview the customized login window based on the settings entered on this page.
Set to Factory Default	Click to return to the factory default setting.

Below shows an example of a customized login page with the values entered in the **Login Page Title** and **Welcome Message and Bulletin** fields.

V-1-6 Configuration Backup

This function allows the backup and restoration of Vigor router settings.

Available settings are explained as follows:

Item	Description
Restore	**This file is encrypted with password** – Check the box and enter a password for encrypting the configuration file. Click the **Select File** button to specify a configuration file to be restored. **Restore** - Click to initiate restoration of configuration. If the backup file is encrypted, you will be asked to enter the password.
Backup	**Normal backup** - Click it to perform the configuration backup of this router. **Protect full file with password**- Select to encrypt the backup with a password. You will be prompted to enter the password as shown below: ● **Password** – Enter a new password for encrypting the configuration file. ● **Confirm Password** – Enter the new password again for confirmation. **Backup** - Click to initiate the backup process.

Backing up the Configuration

Follow the steps below to backup your configuration.

1. Go to **System Maintenance** >> **Configuration Backup**.

2. Click the **Backup** button. Depending on your browser, you may be prompted to select a location to save the file, or the file may be saved in the default download location of your browser.

   The configuration will download automatically to your computer as a file named **config.cfg**.

Info	Configuration Backup does not include certificates stored on the router. Please back up certificates separately by going to **Certificate Management** >> **Certificate Backup**.

Restoring the Configuration

1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be shown.

2. Click the **Choose File** button under **Backup** to bring up the open file dialog box to select the configuration file to be uploaded and restored.

3. Click the **Restore** button and wait for few seconds.

V-1-7 Configuration Export

Configuration for Vigor3910 can be exported as an user-readable text-based (.exp) file which can be applied to other Vigor router.

In addition, it is possible to import an ".exp" file from other DrayTek routers onto the Vigor3910.

Available settings are explained as follows:

Item	Description
Import	**This file is encrypted with password** – Check the box and enter a password for dencrypting the configuration file (if the.exp file is encrypted). Click the **Select File** button to specify an exp file. **Import** - Click to import a configuration file. If the file is encrypted, you will need to enter the password set on the above password field.
Export	**Do not encrypt** - The configuration file (.exp) will be output as an fully user-readable text-based file. **Encrypt password fields** - The configuration file (.exp) will be output as a user-readable text-based file except for password related fields (user passwords will be encrypted). **Protect full file with password** - The configuration file is protected by full encryption. The password will be needed when importing the "exp" file on Vigor router. **Export** - Click it to export the configuration of Vigor router as a file with the extension of "exp".

V-1-8 Syslog/Mail Alert

SysLog function is provided for users to monitor router.

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 router configured in **System Maintenance>>Management**. If there is no name here, simply lick the link to access into **System Maintenance>>Management** to set the router name. **Server IP / Hostname -** The IP address / hostname of the Syslog server. **Destination Port -** Assign a port for the Syslog protocol. **Mail Syslog –** Check the box to recode the mail event on Syslog. **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/SMTP Port -** The IP address/Port number 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.
	Username - Type the user name for authentication.
	Password - Type the password for authentication.
	Enable E-mail Alert - Check the box to send alert message to the e-mail box while the router detecting the item(s) you specify here.

Click **OK** to save these settings.

For viewing the Syslog, please do the following:

1. Just set your monitor PC's IP address in the field of Server IP Address

2. Install the Router Tools in the **Utility** within provided CD. After installation, click on the **Router Tools**>>**Syslog** from program menu.
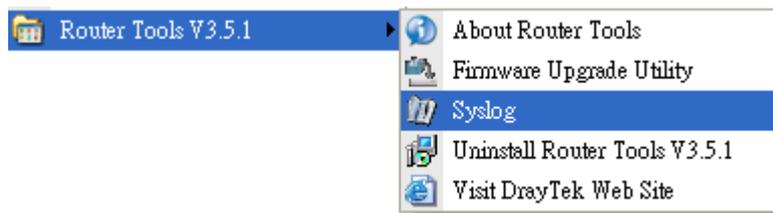
3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.
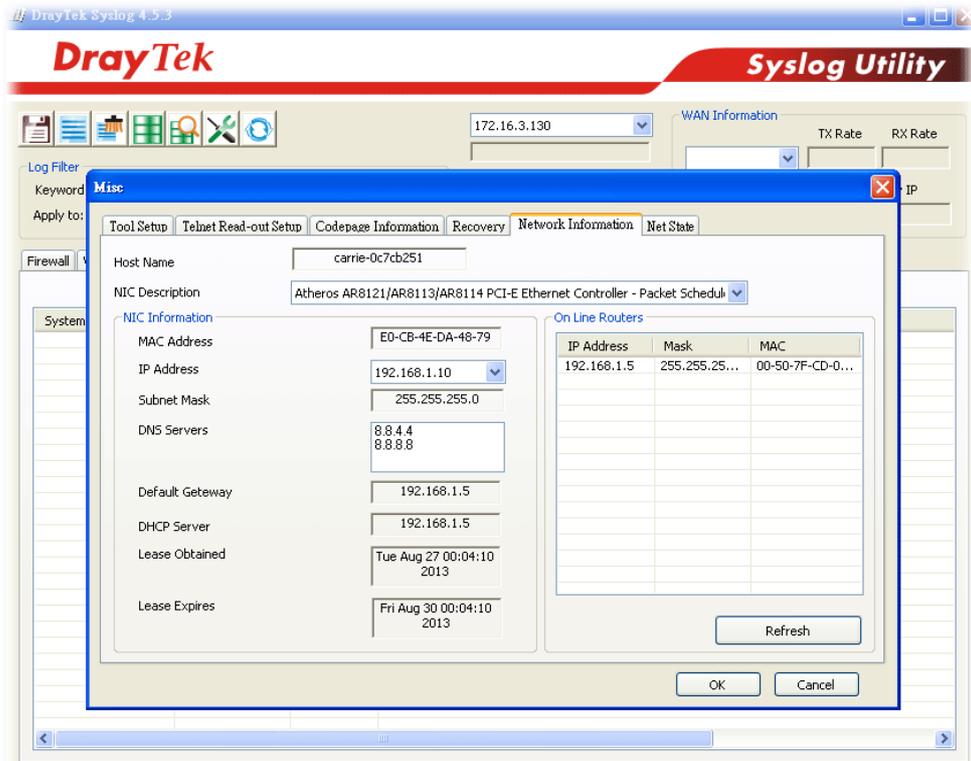
V-1-9 Time and Date

This section allows you to configure settings related to the system date and time.

Available settings are explained as follows:

Item	Description
Current System Time	Click **Inquire Time** to retrieve the current time from the time server.
Use Browser Time	Select this option to let the router set its system time using the time reported by the web browser.
Use Internet Time	Select this option to let the router set its system time by retrieving time information from the specified network time server using the Network Time Protocol (NTP).
Time Server	Enter the IP address / Host name of the time server.
Priority	Select **Auto** or **IPv6 First** as the priority.
Time Zone	Select the time zone where the router is located.
Enable Daylight Saving	Check the box to enable Daylight Saving Time (DST), if it is applicable to your location. **Advanced** - Click to enter a custom schedule to enable DST. Use the default time setting or set user defined time for your requirement. ● **Default** – uses the default DST schedule for the time

	zone.
	• **Customized: By Date** – Select this option if DST starts and ends on fixed dates.
	• **Customized: By Weekday** - Select this option if DST starts and ends on certain days of the week.
Automatically Update Interval	Select the time interval at which the router updates the system time.
Send NTP Request Through	Specify a WAN interface to send NTP request for time synchronization.

Select **OK** to save changes on the page, or **Cancel** to discard changes without saving.

V-1-10 SNMP

This section allows you to configure settings for SNMP and SNMPV3 services.

The SNMPv3 is **more secure than** SNMP through the use of encryption (supports AES and DES) and authentication (supports MD5 and SHA) for the management needs.

System Maintenance >> SNMP

SNMP Setup

☐ Enable SNMP Agent
    ☑ Enable SNMPV1 Agent
    ☑ Enable SNMPV2C Agent
Get Community   public
Set Community   private

Manager Host IP(IPv4)   Index   IP   Subnet Mask
    1
    2
    3

Manager Host IP(IPv6)   Index   IPv6 Address   / Prefix Length
    1   /0
    2   /0
    3   /0

Trap Community   public
Notification Host IP(IPv4)   Index   IP
    1
    2

Notification Host IP(IPv6)   Index   IPv6 Address
    1
    2

Trap Timeout   10
☐ Enable SNMPV3 Agent
USM User
Auth Algorithm   No Auth ▾
Auth Password
Privacy Algorithm   No Priv ▾
Privacy Password

Note:
SNMP service also shall be enabled for Internet access in **System Maintenance >> Management**.

[OK]   [Cancel]

Available settings are explained as follows:

Item	Description

Enable SNMP Agent	Check to enable **SNMP** function. Then, enable SNMPV1 agent/SNMPV2C agent.
Get Community	Enter the Get Community string. The default setting is **public**. Devices that send requests to retrieve information using get commands must pass the correct Get Community string.
	The maximum allowed length is 23 characters.
Set Community	Enter the Set Community string. The default setting is **private**. Devices that send requests to change settings using set commands must pass the correct Set Community string.
	The maximum length of the text is 23 characters.
Manager Host IP (IPv4)	Enter the IPv4 address of hosts that are allowed to issue SNMP commands. If this field is left blank, any IPv4 LAN host is allowed to issue SNMP commands.
Manager Host IP (IPv6)	Enter the IPv6 address of hosts that are allowed to issue SNMP commands. If this field is left blank, any IPv6 LAN host is allowed to issue SNMP commands.
Trap Community	Enter the Trap Community string. The default setting is **public**. Devices that send unsolicited messages to the SNMP console must pass the correct Trap Community string.
	The maximum length of the text is 23 characters.
Notification Host IP (IPv4)	Enter the IPv4 address of hosts that are allowed to send SNMP traps.
Notification Host IP (IPv6)	Enter the IPv6 address of hosts that are allowed to send SNMP traps.
Trap Timeout	The default setting is 10 seconds.
Enable SNMPV3 Agent	Check it to enable SNMPV3.
USM User	USM means user-based security mode.
	Enter the username to be used for authentication. The maximum allowed length is 23 characters.
Auth Algorithm	Choose one of the hashing methods to be used with the authentication algorithm. No Auth ▾ No Auth MD5 SHA
Auth Password	Enter a password for authentication. The maximum allowed length is 23 characters.
Privacy Algorithm	Choose one of the methods listed below as the privacy algorithm. Choose an encryption method as the privacy algorithm. No Priv ▾ No Priv DES AES
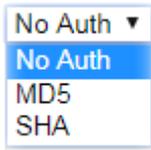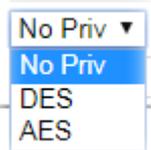
Privacy Password	Type a password for privacy. The maximum length of the text is limited to 23 characters.
	Enter a password for privacy. The maximum allowed length is 23 characters.

Select **OK** to save changes on the page, or **Cancel** to discard changes without saving.

V-1-11 Management

This page allows you to manage the settings for Internet/LAN Access Control, Access List from Internet, Management Port Setup, TLS/SSL Encryption Setup, CVM Access Control and Device Management.

The management pages for IPv4 and IPv6 protocols are different.

V-1-11-1 IPv4 Management Setup

Available settings are explained as follows:

Item	Description
Router Name	Enter the router name provided by ISP.
Default: Disable Auto-Logout	If enabled, the auto-logout function for the web user interface will be disabled. The web user interface session will not terminate until you manually click the Logout icon.

	Logout
Enable Validation Code in Internet/LAN Access	If enabled, Vigor router will require users to enter a validation code as shown in an image when they log in.
Internet Access Control	**Allow management from the Internet** – Select to allow system administrators to login from the Internet, and then select the specific services that are allowed to be remotely administered. **Domain name allowed** – If specified, only hosts belonging to that domain name are allowed to manage the router over the Internet. **Disable PING from the Internet -** Select to reject all PING packets from the Internet. For increased security, this setting is enabled by default.
Access List from the Internet	The ability of system administrators to log into the router can be restricted to up to 10 specific hosts or networks. **Apply Access List to PING** - When this option is checked and **Disable PING from the Internet** is unchecked, pings originating from the Internet will be accepted only if they are from one of the IP addresses and/or subnet masks specified below. This option has no effect if **Disable PING from the Internet** is checked, such that no pings from the Internet are accepted. **Index in IP Object** - Enter the index of a configured IP object. **IP / Mask** - Show the IP address and/or subnet mask of the selected IP object.
Management Port Setup	**User Define Ports -** Check to specify custom port numbers for the Telnet, HTTP, HTTPS, FTP, TR-069 and SSH servers. **Default Ports -** Check to use standard port numbers for the Telnet and HTTP servers.
Brute Force Protection	Any client trying to access into Internet via Vigor router will be asked for passing through user authentication. Such feature can prevent Vigor router from attacks when a hacker tries every possible combination of letters, numbers and symbols until find out the correct combination of password. **Enable brute force login protection** – Select to enable detection of brute force login attempts. **Maximum login failure** – Specify the maximum number of failed login attempts before further login is blocked. **Penalty period** – Set the lockout time after maximum number of login attempts has been exceeded. The user will be unable to attempt to log in until the specified time has passed. **Blocked IP List** – Display, in a new browser window, IP addresses that are currently blocked from logging into the router.
TLS/SSL Encryption Setup	**Enable SSL 3.0 and TLS 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. |

Select **OK** to save changes on the page.

V-1-11-2 IPv6 Management Setup

System Maintenance >> Management

| IPv4 Management Setup | IPv6 Management Setup | LAN Access Setup |

Management Access Control
☐ Allow management from the Internet
　☐ Telnet Server (Port : 23)
　☐ HTTP Server (Port : 80) ☐ Enforce HTTPS Access
　☐ HTTPS Server (Port : 443)
　☐ SSH Server (Port : 22)
　☐ SNMP Server (Port : 161)
☑ Disable PING from the Internet

Access List from the Internet
☐ Apply Access List to PING

List	index in IPv6 Object	IPv6 / Prefix
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Note:
Telnet / Http server port is the same as IPv4.

OK

Available settings are explained as follows:

Item	Description
Management Access Control	**Allow management from the Internet** – Select to allow system administrators to login from the Internet, and then select the specific services that are allowed to be remotely administered. **Disable PING from the Internet** - Select to reject all PING packets from the Internet. For increased security, this setting is enabled by default.
Access List from the Internet	The ability of system administrators to log into the router can be restricted to up to 10 specific hosts or networks. **Apply Access List to PING** - When this option is checked and **Disable PING from the Internet** is unchecked, pings originating from the Internet will be accepted only if they are from one of the IP addresses and/or subnet masks specified below. This option has no effect if **Disable PING**

from the Internet is checked, such that no pings from the Internet are accepted.

Index in IPv6 Object - Enter the index of a configured IP object.

IPv6 /Prefix - Show the IPv6 address and/or prefix of the selected IP object.

Select **OK** to save changes on the page.

V-1-11-3 LAN Access Control

Available settings are explained as follows:

Item	Description
Allow management from LAN	Enable the checkbox to allow system administrators to login from LAN interface. There are several servers provided by the system which allow you to manage the router from LAN interface. Check the box(es) to specify.
Apply To Subnet	Check the LAN interface for the administrator to use for accessing into web user interface of Vigor router. **Index in IP Object**- Type the index number of the IP object profile. Related IP address will appear automatically.

Select **OK** to save changes on the page.

Vigor3910 Series User's Guide

V-1-12 Self-Signed Certificate

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

The self-signed certificate 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 :	Aug 5 18:08:23 2019 GMT
Valid To :	Aug 4 18:08:23 2049 GMT
PEM Format Content :	(see below)

```
-----BEGIN CERTIFICATE-----
MIIDijCCAnKgAwIBAgIJALidtKDoJUDeMA0GCSqGSIb3DQEBCwUAMHgxCzAJBgNV
BAYTAlRXMRAwDgYDVQQIDAdIc2luQ2h1MQ4wDAYDVQQHDAVIdUtvdTEWMBQGA1UE
CgwNRHJheVRlayBDb3JwLjEYMBYGA1UECwwPRHJheVRlayBTdXBwb3J0MRUwEwYD
VQQDDAxWaWdvciBSb3V0ZXIwHhcNMTkwODA1MTgwODIzWhcNNDkwODA0MTgwODIz
WjB4MQswCQYDVQQGEwJUVzEQMA4GA1UECAwHSHNpbkNodTEOMAwGA1UEBwwFSHVL
b3UxFjAUBgNVBAoMDURyYXlUZWsgQ29ycC4xGDAWBgNVBAsMD0RyYXlUZWsgU3Vw
cG9ydDEVMBMGA1UEAwwMVmlnb3IgUm91dGVyMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAysXQKjz0rijEjlepRQ7nUgR6Qp1kGRgKlmdC22o572Y2z+m4
4oJDzMeDD2qGkFy4EKgTHaP5EZFwyirQLWs5VuzQDE/OcEd/I85sYlCiBCO/5zOb
wAVGSJ987Yq/tSP3wrzPOiU8kjAYjrpjoWE8Fb5PBiUS6ftOYpasTbEHLvm5lqlB
6ZbWIqBVeV1aTHFSCD9mhRHjowHmst++o9F/xi3TRN/CjQ9gq8sCDC9hSB3Qk2/a
+0rjk8bwIR2QNtt4Sa4n9LqpBKR5exBaQrDcBHpt0e/GvkC5UlrzqivduB3oMRDW
WZX8/l6e39LiVxoXCd3LwD5MLzPyhGugbzv2VwIDAQABoxcwFTATBgNVHSUEDDAK
BggrBgEFBQcDATANBgkqhkiG9w0BAQsFAAOCAQEAvnnEkxpA0AqbU+P9fwjABl+Q
/igED712nrG5A7n1s26amgCkCXNMgx8BoNsYxydvo75mkIhBxVxBoyWNic7YIW6n
6KbhNxZ932iWaDOGBPpxu0skPU1dxkDyJiWhhCPwv+rUq0HhyDHKoHa+Mn9yiSLf
NSwPPXj7f400cVZ3rz1aLzMw4NCsoWSZuFvdxh6YjuUhQ6vKr4bgM5UFmK02ZJDM
6tZQ8K+Kg/kRQ8QzRXRKH86hbHrbS3/EA6ZraBi2PmbLTvkt4jSlySXTAvUSFN0K
BHExOlkcNhQqci4WwyR/IAdarpP59drRg/riP7IJfe/ykeQLZaXgRhp+P6/42A==
-----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.

System Maintenance >> Regenerate Self-Signed Certificate

Regenerate Self-Signed Certificate

Certificate Name	self-signed

Subject Alternative Name

Type	IP Address ▼
IP	

Subject Name

Country (C)	
State (ST)	
Location (L)	
Organization (O)	
Organization Unit (OU)	
Common Name (CN)	
Email (E)	

Key Type	RSA ▼
Key Size	2048 Bit ▼

Generate

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

V-1-13 Reboot System

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

System Maintenance >> Reboot System

Reboot System

Do you want to reboot your router ?

◉ Using current configuration
○ Using factory default configuration

Reboot Now

Auto Reboot Time Schedule

Schedule Profile : None ▼ , None ▼ , None ▼ , None ▼

Note: Action and Idle Timeout settings will be ignored.

OK   Cancel

Available settings are explained as follows:

Item	Description
Reboot System	Select one of the following options, and press the **Reboot Now** button to reboot the router. **Using current configuration** – Select this option to reboot the router using the current configuration. **Using factory default configuration** – Select this option to reset the router's configuration to the factory defaults before rebooting.
Auto Reboot Time Schedule	**Schedule Profile** - Select up to 4 user-configured schedules to reboot the router on a scheduled basis.

Select **OK** to save changes on the page, or **Cancel** to discard changes without saving.

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

V-1-14 Firmware Upgrade

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

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

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

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

For the detailed information about firmware update, please go to Chapter 5.

V-1-15 Activation

There are three ways to activate WCF on vigor router, using Service Activation Wizard, by means of CSM>>Web Content Filter Profile or via System Maintenance>>Activation.

After you have finished the setting profiles for WCF (refer to **Web Content Filter Profile**), it is the time to activate the mechanism for your computer.

Click **System Maintenance**>>**Activation** to open the following page for accessing http://myvigor.draytek.com.

System Maintenance >> Activation	Activate via interface : auto-selected ▼

Web-Filter License
[Status: **Inactivated**]   **Activate**

Authentication Message

Note:
1. If you want to use email alert or syslog, please configure the <u>SysLog/Mail Alert Setup</u> page.
2. If you change the service provider, the configuration of the function will be reset.

OK   Cancel

Available settings are explained as follows:

Item	Description
Activate via Interface	Choose WAN interface used by such device for activating Web Content Filter.
Activate	The **Activate** link brings you accessing into www.vigorpro.com to finish the activation of the account and the router.
Authentication Message	As for authentication information of **web filter**, the process of authenticating will be displayed on this field for your reference.

V-1-16 Internal Service User List

User profiles (clients) defined and enabled in **User Management>>User Profile** will be displayed in this page.

Such page allows you to turn on or turn off security authentication service (offered by inernal RADIUS) for each user profile without accessing into the User Management configuration page.

System Maintenance >> Internal Service User List

User Name	☐ Radius	User Name	☐ Radius
No valid User Profile			

OK   Cancel

Note:
1. Only the user profiles which is enabled in User **Management >> User Profile** will be listed here.
2. If you enable RADIUS for a user profile here, it will use the default authentication methods; however, you may change its authentication methods via User **Management >> User Profile**.

Available settings are explained as follows:

Item	Description
User Name	Display the name of the existed user profile. To modify the detailed settings, simply click the user name link to access into the web page for modification.
Radius	Check the box to turn on the security authentication service offered by internal RADIUS server for the user profile.
	Uncheck the box to turn off ecurity authentication service offered by internal RADIUS server for the user profile.
	If you check the box next to such item, all of the user profiles listed in this page will be enabled with RADIUS service enabled vice versa.

Info   For the detailed setting (such as IP address, port number) configuration of internal RADIUS, refer to **Applications>>RADIUS/TACACS+**.

V-1-17 Dashboard Control

There are nine groups of setting information which can be displayed on Dashboard as a reference for administrator/user. Except for Front Panel and System Information, the settings information regarding to the groups listed on this page can be hidden if required.

System Maintenance >> Dashboard Control

☑ Front Panel
☑ System Information
☑ IPv4 LAN Information
☑ IPv4 Internet Access
☑ IPv6 Internet Access (shown when enabled)
☑ Interface
☑ Security
☑ System Resource
☑ Quick Access

[OK]   [Cancel]

V-2 Bandwidth Management

Sessions Limit

A PC with private IP address can access to the Internet via NAT router. The router will generate the records of NAT sessions for such connection. The P2P (Peer to Peer) applications (e.g., BitTorrent) always need many sessions for procession and also they will occupy over resources which might result in important accesses impacted. To solve the problem, you can use limit session to limit the session procession for specified Hosts.

Bandwidth Limit

The downstream or upstream from FTP, HTTP or some P2P applications will occupy large of bandwidth and affect the applications for other programs. Please use Limit Bandwidth to make the bandwidth usage more efficient.

Quality of Service (QoS)

Deploying QoS (Quality of Service) management to guarantee that all applications receive the service levels required and sufficient bandwidth to meet performance expectations is indeed one important aspect of modern enterprise network.

One reason for QoS is that numerous TCP-based applications tend to continually increase their transmission rate and consume all available bandwidth, which is called TCP slow start. If other applications are not protected by QoS, it will detract much from their performance in the overcrowded network. This is especially essential to those are low tolerant of loss, delay or jitter (delay variation).

Another reason is due to congestions at network intersections where speeds of interconnected circuits mismatch or traffic aggregates, packets will queue up and traffic can be throttled back to a lower speed. If there's no defined priority to specify which packets should be discarded (or in another term "dropped") from an overflowing queue, packets of sensitive applications mentioned above might be the ones to drop off. How this will affect application performance?

There are two components within Primary configuration of QoS deployment:

● Classification: Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.

● Scheduling: Based on classification of service level to assign packets to queues and associated service types

The basic QoS implementation in Vigor routers is to classify and schedule packets based on the service type information in the IP header. For instance, to ensure the connection with the headquarter, a teleworker may enforce an index of QoS Control to reserve bandwidth for HTTPS connection while using lots of application at the same time.

One more larger-scale implementation of QoS network is to apply DSCP (Differentiated Service Code Point) and IP Precedence disciplines at Layer 3. Compared with legacy IP Precedence that uses Type of Service (ToS) field in the IP header to define 8 service classes, DSCP is a successor creating 64 classes possible with backward IP Precedence compatibility. In a QoS-enabled network, or Differentiated Service (DiffServ or DS) framework, a DS domain owner should sign a Service License Agreement (SLA) with other DS domain owners to define the service level provided toward traffic from different domains. Then each DS node in these domains will perform the priority treatment. This is called per-hop-behavior (PHB). The definition of PHB includes Expedited Forwarding (EF), Assured Forwarding (AF), and Best Effort (BE). AF defines the four classes of delivery (or forwarding) classes and three levels of drop precedence in each class.

Vigor routers as edge routers of DS domain shall check the marked DSCP value in the IP header of bypassing traffic, to allocate certain amount of resource execute appropriate policing, classification or scheduling. The core routers in the backbone will do the same checking before executing treatments in order to ensure service-level consistency throughout the whole QoS-enabled network.
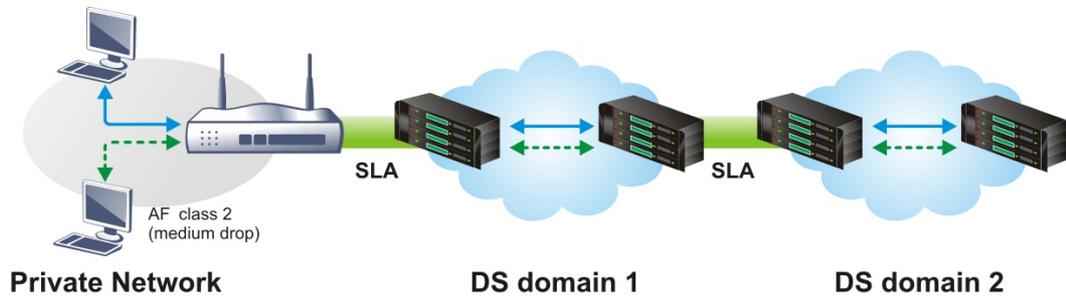
However, each node may take different attitude toward packets with high priority marking since it may bind with the business deal of SLA among different DS domain owners. It's not easy to achieve deterministic and consistent high-priority QoS traffic throughout the whole network with merely Vigor router's effort.

Web User Interface

Below shows the menu items for Bandwidth Management.

V-2-1 Sessions Limit

In the **Bandwidth Management** menu, click **Sessions Limit** to open the web page.

To activate the function of limit session, simply click **Enable** and set the default session limit.

Available settings are explained as follows:

Item	Description
Enable/Disable	**Enable** - Click this button to activate the function of limit session.
	Disable - Click this button to close the function of limit session.
	Default Max Sessions - Defines the default session number

	used for each computer in LAN.
Limitation List	Displays a list of specific limitations that you set on this web page.
Specific Limitation	**Start IP**- Defines the start IP address for limit session.
	End IP - Defines the end IP address for limit session.
	Maximum Sessions - Defines the available session number for each host in the specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index.
	Add - Adds the specific session limitation onto the list above.
	Edit - Allows you to edit the settings for the selected limitation.
	Delete - Remove the selected settings existing on the limitation list.
Administration Message	Type the words which will be displayed when reaches the maximum number of Internet sessions permitted.
	Default Message - Click this button to apply the default message offered by the router.
Time Schedule	**Schedule Profile** - You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application** >> **Schedule** web page and you can use the number that you have set in that web page.

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

V-2-2 Bandwidth Limit

In the **Bandwidth Management** menu, click **Bandwidth Limit** to open the web page.

To activate the function of limit bandwidth, simply click **Enable** and set the default upstream and downstream limit.

Available settings are explained as follows:

Item	Description
Enable / Disable	**Enable** - Click this button to activate the function of limit bandwidth. ● **IP Routed Subnet** – Check this box to apply the bandwidth limit to the second subnet specified in LAN>>General Setup. It is available for IPv4 settings only. **Disable** - Click this button to close the function of limit bandwidth.
Default Limit (Per User)	**TX Limit** - Define the default speed of the upstream for each computer in LAN. **RX Limit** - Define the default speed of the downstream for

	each computer in LAN.
Limitation List	Display a list of specific limitations that you set on this web page.
	Add Entry By − Specify an entry with an IP address (IP address range) and limit for data transmission.
	IP Range − All the IPs within the range defined will be restricted by bandwidth limit defined by TX Limit and RX Limit below.
	● **Start IP** - Define the start IP address for limit bandwidth.
	● **End IP** - Define the end IP address for limit bandwidth.
	IP Object − All the IPs specified by the selected IP object or IP group will be restricted by bandwith limit defined by TX Limit and RX Limit below.
	● **IP Group** − Specify an IP group by using the drop down list.
	● **IP Object** - Specify an IP object by using the drop down list.
	Each / Shared - Select **Each** to make each IP within the range of Start IP and End IP having the same speed defined in TX limit and RX limit fields; select **Shared** to make all the IPs within the range of Start IP and End IP share the speed defined in TX limit and RX limit fields.
	TX limit - Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
	RX limit - Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
	Add - Add the specific speed limitation onto the list above.
	Edit - Allow you to edit the settings for the selected limitation.
	Delete - Remove the selected settings existing on the limitation list.
Allow-Adjustment	**Allow user to use more bandwidth···** - Check this box to make the best utilization of available bandwidth.
Smart Bandwidth Limit	**Apply the below limit to users not in Limitation List…** - Check this box to apply the following limits to users not in Limitation List and apply to the user more than sessions defined.
	TX Limit - Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
	RX Limit - Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
Time Schedule	**Schedule Profile** - You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application >> Schedule** web page and you can use the number that you have set in that web page.

V-2-3 Quality of Service

In the **Bandwidth Management** menu, click **Quality of Service** to open the web page.

Available settings are explained as follows:

Item	Description
General Setup	**Index** – Display the WAN interface number link that you can edit.
	Enable – Check the box to enable the QoS function for WAN interface. If it is enabled, you can configure general QoS setting for each WAN interface.
	● **Direction** – Define which traffic the QoS Control settings will apply to.
	■ **IN**- apply to incoming traffic only.
	■ **OUT**-apply to outgoing traffic only.
	■ **BOTH**- apply to both incoming and outgoing traffic.
	● **Inbound/Outbound Bandwidth** – Set the connecting rate of data input/output for other WAN. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 1000kbps for this box. The default value is 10000kbps.
	● **Class 1 ~ 3 / Others** – Define the ratio of bandwidth to upstream speed and bandwidth to downstream speed. There are four queues allowed for QoS control. The first

Item	Description
	three (Class 1 to Class 3) class rules can be adjusted for your necessity. In which, the "Others" field is used for the packets which are not suitable for the three class rules. **Status** – Display the online statistics of WAN interface.
Class Rule	Set detailed settings for the selected Class. **Index** – Display the class number that you can edit. **Enable** - Display the status of this class rule. **QoS Class** - Display the QoS class level. **Local Address** - Display the local IP address for the rule. **Remote Address** - Display the remote IP address for the rule. **DSCP** - Display the levels of the data for processing with QoS control. **Service Type** – Display detailed settings for the service type. **Add** - Click it to create a class rule for QoS.
VoIP Prioritization	**Enable the First Priority for VoIP SIP/RTP** - When this feature is enabled, the VoIP SIP/UDP packets will be sent with highest priority. **SIP UDP Port** – Set a port number used for SIP.
Tag Outbound Traffic	**Add DSCP or Precedence Value for Class 1 to Class 3** - Check the box to add DSCP or Precedence value to Class 1 to Class 3.

You can configure general setup for the WAN/LTE interface, edit the Class Rule, and edit the Service Type for the Class Rule for your request. Click the link (WAN1 to WAN8) under Index to access into next page for the general setup of WAN interface. As to class rule, simply click the **Add** link to access into next page for configuration.

Online Statistics

Display an online statistics for quality of service for your reference. This feature is available only when the Quality of Service for WAN interface is enabled.
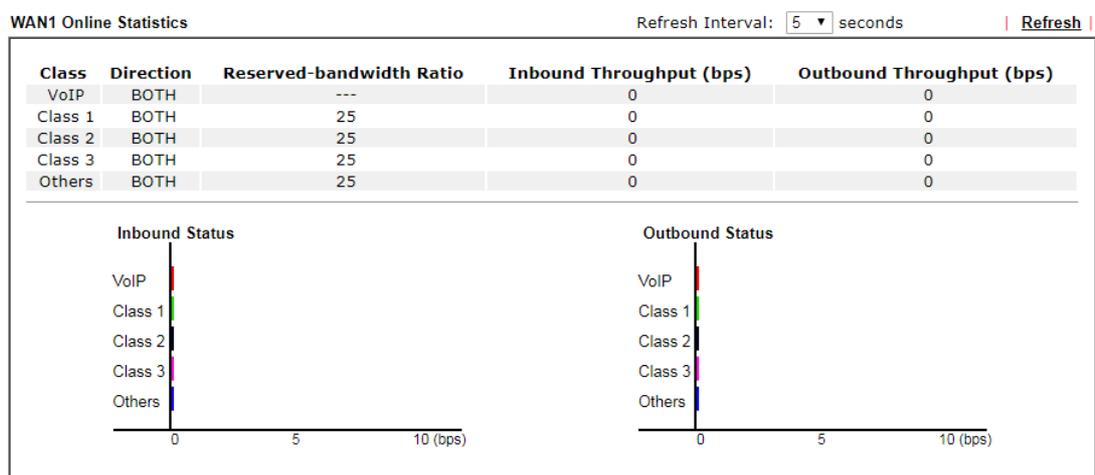
General Setup for WAN Interface

Click WAN interface number link to configure the limited bandwidth ratio for QoS of the WAN interface.

Bandwidth Management >> Quality of Service >> WAN1

☐ Enable UDP Bandwidth Control
      Limited_bandwidth Ratio 25 %
☐ Outbound TCP ACK Prioritize

[OK]   [Cancel]

Available settings are explained as follows:

Item	Description
Enable UDP Bandwidth Control	Set the limited bandwidth ratio. This is a protection of TCP application traffic since UDP application traffic such as streaming video will exhaust lots of bandwidth. **Limited_bandwidth Ratio -** The ratio typed here is reserved for limited bandwidth of UDP application.
Outbound TCP ACK Prioritize	The difference in bandwidth between download and upload are great in ADSL2+ environment. For the download speed might be impacted by the uploading TCP ACK, you can check this box to push ACK of upload faster to speed the network traffic.

Info   The rate of outbound/inbound must be smaller than the real bandwidth to ensure correct calculation of QoS. It is suggested to set the bandwidth value for inbound/outbound as 80% - 85% of physical network speed provided by ISP to maximize the QoS performance.

Edit the Class Rule for QoS

1. The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. To add, edit or delete the class rule, please click the **Add / Edit** link of that one.

2. For adding a new rule, click **Add** to open the following page.

Available settings are explained as follows:

Item	Description
Enable	Check this box to invoke these settings.
IP Version	Please specify which protocol (IPv4 or IPv6) will be used for this rule.

Local IP Address	Click the **Edit** button to set the local IP address (on LAN) for the rule.
Remote IP Address	Click the **Edit** button to set the remote IP address (on LAN/WAN) for the rule. **Address Type –** Determine the address type for the source address. For **Single Address**, you have to fill in Start IP address. For **Range Address**, you have to fill in Start IP address and End IP address. For **Subnet Address**, you have to fill in Start IP address and Subnet Mask.
DiffServ CodePoint	All the packets of data will be divided with different levels and will be processed according to the level type by the system. Please assign one of the levels of the data for processing with QoS control.
Service Type	It determines the service type of the data for processing with QoS control. It can also be edited. You can choose the predefined service type from the Service Type drop down list. Those types are predefined in factory. Simply choose the one that you want for using by current QoS.
QoS Class	Specify the QoS class (1, 2 or 3) for this rule.
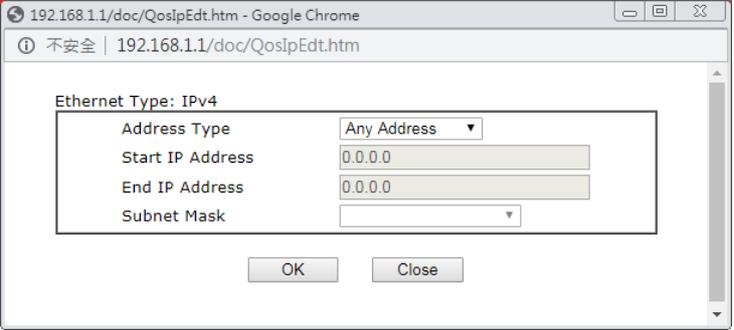
3. After finishing all the settings here, please click **OK** to save the configuration.

Bandwidth Management >> Quality of Service

General Setup | Set to Factory Default |

Index	Enable	Direction	Inbound/ Outbound Bandwidth				Class 1		Class 2		Class 3		Others		Status
WAN1	☐	BOTH ▾	100	Mbps ▾	/	100	Mbps ▾	25	%	25	%	25	%	25	%	**Status**
WAN3	☐	BOTH ▾	100	Mbps ▾	/	100	Mbps ▾	25	%	25	%	25	%	25	%	**Status**
WAN5	☐	BOTH ▾	100	Mbps ▾	/	100	Mbps ▾	25	%	25	%	25	%	25	%	**Status**
WAN6	☐	BOTH ▾	100	Mbps ▾	/	100	Mbps ▾	25	%	25	%	25	%	25	%	**Status**
WAN7	☐	BOTH ▾	100	Mbps ▾	/	100	Mbps ▾	25	%	25	%	25	%	25	%	**Status**
WAN8	☐	BOTH ▾	100	Mbps ▾	/	100	Mbps ▾	25	%	25	%	25	%	25	%	**Status**

Note:
QoS may not work properly if the bandwidth entered is not correct. Before enable QoS, you may run speed test (from e.g.,http://speedtest.net) or contact your ISP for the accurate bandwidth.

Class Rule

Index	Enable	Qos Class	Local Address	Remote Address	DSCP	Service Type
1	☑	Class 1	Any	Any	ANY	ANY
			Add			

Note:
The packets that don't match any class rules above will be classified into 'Others'

VoIP Prioritization

☑ **Enable the First Priority for VoIP SIP/RTP:**

SIP UDP Port: 5060 (Default:5060)

Tag Outbound Traffic

Class 1	☐ Add DSCP or Precedence Value	Default ▾
Class 2	☐ Add DSCP or Precedence Value	Default ▾
Class 3	☐ Add DSCP or Precedence Value	Default ▾

[OK] [Cancel]

By the way, you can set up to 20 rules for one Class. If you want to edit an existed rule, please select the radio button of that one and click **Edit** to open the rule edit page for modification.

Retag the Packets for Identification

Packets coming from LAN IP can be retagged through QoS setting. When the packets sent out through WAN interface, all of them will be tagged with certain header and that will be easily to be identified by server on ISP.

For example, in the following illustration, the VoIP packets in LAN go into Vigor router without any header. However, when they go forward to the Server on ISP through Vigor router, all of the packets are tagged with AF (configured in Bandwidth >>QoS>>Class) automatically.

.

V-3 User Management

User Management is a security feature which disallows any IP traffic (except DHCP-related packets) from a particular host until that host has correctly supplied a valid username and password. Instead of managing with IP address/MAC address, User Management function manages hosts with user account. Network administrator can give different firewall policies or rules for different hosts with different User Management accounts. This is more flexible and convenient for network management. Not only offering the basic checking for Internet access, User Management also provides additional firewall rules, e.g. CSM checking for protecting hosts.
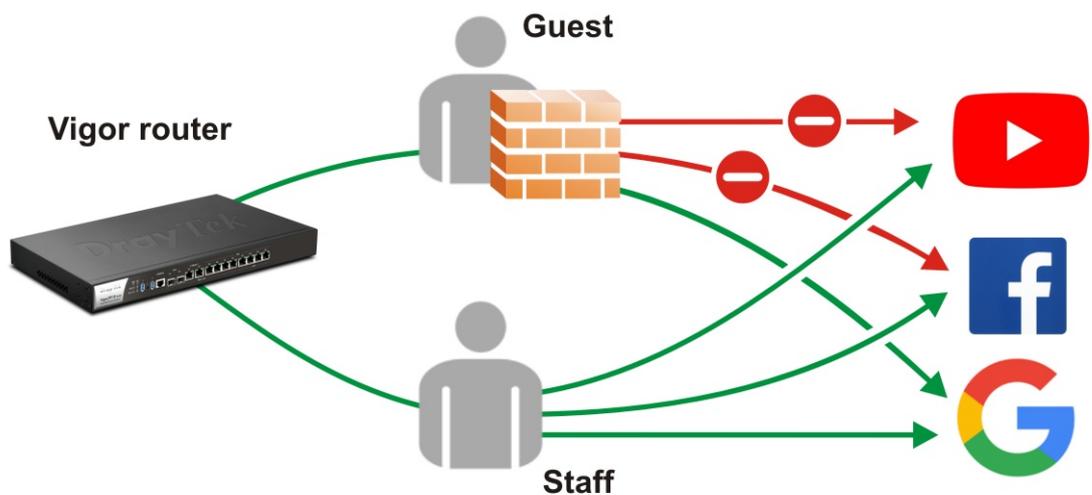
ℹ️ **Info**	Filter rules configured under Firewall usually are applied to the host (the one that the router installed) only. With user management, the rules can be applied to every user connected to the router with customized profiles.

Web User Interface

V-3-1 General Setup

General Setup can determine the standard (rule-based or user-based) for the users controlled by User Management. The mode (standard) selected here will influence the contents of the filter rule(s) applied to every user.

Available settings are explained as follows:

Item	Description
Mode Selection	There are two modes offered here for you to choose. Each mode will bring different filtering effect to the users involved. **User-Based** - If you choose such mode, the router will apply the filter rules configured in **User Management>>User**

	Profile to the users.
	Rule-Based –If you choose such mode, the router will apply the filter rules configured in **Firewall>>General Setup** and **Filter Rule** to the users.
Authentication page	**Web Authentication** - Choose the protocol for web authentication.
	Login Page Logo – A logo which can be used as an identification of enterprise can be uploaded and displayed on the login page. You can use the default one, blank page or upload other image files (the size no mare than 524 × 352 pixel) to have an image of enterprise or have the effect of advertisement.
	Login Page Greeting - Such link allows you to access into the setting page for login greeting. For detailed information, refer to **System Maintenance>>Login Page Greeting**.
	Display IP Address on tracking window - Check the box to display the IP address of the client on the tracking window.
Landing Page	Type the information to be displayed on the first web page when the LAN user accessing into Internet via such router.

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

V-3-2 User Profile

This page allows you to set customized profiles (up to 200) which will be applied for users controlled under **User Management**. Simply open **User Management>>User Profile**.

User Management >> User Profile

User Profile Table

| | Select All | Clear All | | | | Set to Factory Default | Search |

Profile	Enable	Name	Profile	Enable	Name
1.	☑	admin	17.	☐	
2.	☑	Dial-In User	18.	☐	
3.	☐		19.	☐	
4.	☐		20.	☐	
5.	☐		21.	☐	
6.	☐		22.	☐	
7.	☐		23.	☐	
8.	☐		24.	☐	
9.	☐		25.	☐	
10.	☐		26.	☐	
11.	☐		27.	☐	
12.	☐		28.	☐	
13.	☐		29.	☐	
14.	☐		30.	☐	
15.	☐		31.	☐	
16.	☐		32.	☐	

<< 1-32 | 33-64 | 65-96 | 97-128 | 129-160 | 161-192 | 193-200 >>   Next >>

Note:
1.admin: To change the administrator password,please go to System Maintenance >> Administrator Password.
2.Dial-In User Profile: Dial-In User Profile is reserved for VPN authentication.
3.During authentication,Router will check all the local user profiles first,and then the profiles in external servers.

[OK]   [Cancel]

To set the user profile, please click any index number link to open the following page. Notice that profile 1 (**admin**) and profile 2 (**Dial-In User**) are factory default settings. Profile 2 is reserved for future use.

User Management >>User Profile

Profile Index 3
Common Settings

☐ Enable this account

Username   [Max: 24 characters]   (Only support A-Z a-z 0-9 - . @)

Password   [Max: 24 characters]

Confirm Password [   ]

External Server Authentication   [None ▾]

Login Settings

Allow Authentication via   ☑ Web   ☑ Alert Tool   ☑ Telnet

Show Landing Page After Login   ☐

Idle Timeout   [10   ]   min. (0: Unlimited)

Auto Logout After   [0   ]   min. (0: Off)

Pop up Time-Tracking Window   ☑

Login Permission Schedule   [None ▾] , [None ▾] , [None ▾] , [None ▾]

Policy

Max. Login Devices   [0   ]   (0: Unlimited)

☐ Enable Time Quota   [0   ] min.   [-] [0   ] [+]

☐ Enable Data Quota   [0   ] [MB ▾]   [-] [0   ] [+]

☐ Reset Quota Automatically To   Time Limit [0   ] min.   Data Limit [0   ] MB
  When   ⦿ Login Permission Schedule Ends
                                  ○ Schedule [None ▾] Starts

PPPoE Login Settings

PPPoE MAC Bind   ○ Enable   ⦿ Disable

MAC Address   [00] : [00] : [00] : [00] : [00] : [00]

DHCP From   [LAN 1 ▾]

Static IP Address   [0.0.0.0   ]   (optional)

[OK]   [Refresh]   [Clear]   [Cancel]

Available settings are explained as follows:

Item	Description
Common Settings	**Enable this account** - Check this box to enable such user profile.
	Username - Type a name for such user profile (e.g., *LAN_User_Group_1, WLAN_User_Group_A, WLAN_User_Group_B*, etc). When a user tries to access Internet through this router, an authentication step must be performed first. The user has to type the User Name specified here to pass the authentication. When the user passes the authentication, he/she can access Internet via this router. However the accessing operation will be restricted with the conditions configured in this user profile.
	The maximum length of the name you can set is 24 characters.
	Password - Type a password for such profile (e.g., *lug123, wug123,wug456,* etc). When a user tries to access Internet through this router, an authentication step must be performed first. The user has to type the password specified here to pass the authentication. When the user passes the

	authentication, he/she can access Internet via this router with the limitation configured in this user profile.
	The maximum length of the password you can set is 24 characters.
	Confirm Password - Type the password again for confirmation.
	External Service Authentication - The router will authenticate the dial-in user by itself or by external service such as LDAP server or RADIUS server or TACACS+ server. If LDAP, Radius or TACACS+ is selected here, it is not necessary to configure the password setting above.
Login Settings	**Allow Authentication via**- Any user (from LAN side or WLAN side) tries to connect to Internet via Vigor router must be authenticated by the router first. There are three ways offered by the router for the user to choose for authentication.
	● **Web** – If it is selected, the user can type the URL of the router from any browser. Then, a login window will be popped up and ask the user to type the user name and password for authentication. If succeed, a **Welcome Message** (configured in **User Management >> General Setup)** will be displayed. After authentication, the destination URL (if requested by the user) will be guided automatically by the router.
	● **Alert Tool** – If it is selected, the user can open Alert Tool and type the user name and password for authentication. A window with remaining time of connection for such user will be displayed. Next, the user can access Internet through any browser on Windows. Note that Alert Tool can be downloaded from DrayTek web site.
	● **Telnet** – If it is selected, the user can use Telnet command to perform the authentication job.
	Show Landing Page After Login - When a user tries to access into the web user interface of Vigor router series with the user name and password specified in this profile, he/she will be lead into the web page configured in Landing Page field in **User Management>>General Setup**. Check this box to enable such function.
	Idle Timeout - If the user is idle over the limitation of the timer, the **network connection will be stopped for such user**. By default, the Idle Timeout is set to 10 minutes.
	Auto Logout After – Such account will be forced to logout after a certain time set here.
	Pop up Time-Tracking Window - If such function is enabled, a pop up window will be displayed on the screen with time remaining for connection if Idle Timeout is set. However, the system will update the time periodically to keep the connection always on. Thus, Idle Timeout will not interrupt the network connection.
	Login Permission Schedule - You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application >> Schedule** web page and you can use the number that you have set in that web page.

Policy	**Max Login Devices** - Such profile can be used by many users. You can set the limitation for the number of users accessing Internet with the conditions of such profile. The default setting is 0 which means no limitation in the number of users.
	Enable Time Quota - Time quota means the total connection time allowed by the router for the user with such profile. Check the box to enable the function of time quota. The first box displays the remaining time of the network connection. The second box allows to type the number of time (unit is minute) which is available for the user (using such profile) to access Internet.
	[+] – Click this box to set and increase the time quota for such profile.
	[-] – Click this box to decrease the time quota for such profile.
	Note: A dialog will be popped up to notify how many time remained when a user accesses into Internet through Vigor router successfully.
	When the time is up, all the connection jobs including network, IM, social media, facebook, and etc. will be terminated.
	Internet Access Michael, you are now connected. Time remaining online: **00:32:41** Time used: 01:12:54. Logout
	Enable Data Quota - Data Quota means the total amount for data transmission allowed for the user. The unit is MB/GB.
	[+] – Click this box to set and increase the data quota for such profile.
	[-] – Click this box to decrease the data quota for such profile.
	Reset Quota Automaticlly To - Set default time quota and data quota for such profile. When the scheduling time is up, the router will use the default quota settings automatically.
	Check it to use the default setting for time quota and data quota.
	● **Time Limit** – Type the value for the time manually.
	● **Data Limit** – Type the value for the data manually.
	Login Permission Schedule - When the scheduling time is up, the router will reset the quota with user-defined time/data values automatically.
	<u>Schedule</u> – The router will reset the quota with user-defined time/data values at the starting time configured in the selected schedule profile.
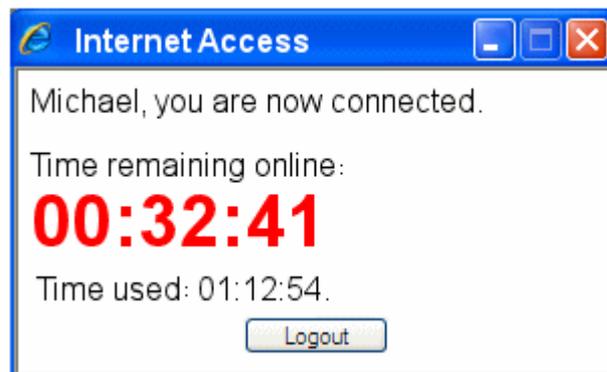
PPPoE Login Setting	Such user account will be used (1) by the client with the IP address specified or (2) by the client with the MAC address bound with the IP address, for accessing into Vigor3910 web user interface.
	PPPoE MAC Bind – Specify a MAC address which is limited and used for such PPPoE account.
	• **Enable/Disable** - Click it to enable/disable the function of PPPoE MAC Bind.
	MAC Address – Type the MAC address to be bound with the IP address set below if **PPPoE MAC Bind** is enabled.
	DHCP From – Use the drop down list to specify LAN/DMZ interface. The IP address for binding with the MAC address (above) set in the selected interface will be assigned from the IP address set in the selected interface.
	Static IP Address (optional)– Type an IP address.

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

V-3-3 User Group

This page allows you to bind several user profiles into one group. These groups will be used in **Firewall>>General Setup** as part of filter rules.

Please click any index number link to open the following page.

Available settings are explained as follows:

Item	Description
Name	Type a name for this user group.
Available User Objects	You can gather user profiles (objects) from **User Profile** page within one user group. All the available user objects that you have created will be shown in this box. Notice that user object, Admin and Dial-In User are factory settings. User defined profiles will be numbered with 3, 4, 5 and so on.
Selected Keyword Objects	Click [»] button to add the selected user objects in this box.

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

V-3-4 User Online Status

This page displays the user(s) connected to the router and refreshes the connection status in an interval of several seconds.

User Management >> User Online Status

Current Time : 01-07 22:01:44   Refresh Seconds: 10 ▼ Page: 1 ▼ | **Refresh** |

Index	User ⌄	IP Address	Profile	Last Login Time	Expired Time	Data Quota	Idle Time	Action
1	admin	192.168.1.5	admin	01-06 16:51:24	Unlimited	Unlimited	Unlimited	**Block Logout Delete**

Note:
1. Please click "IP Address" to view all online users.
2. Dial-in User profiles are linked to VPN clients and therefore cannot be logged-out or deleted while connecting.
3. Information about 802.1X authentication can be found at **Authentication User List.**

Total Number : 1

Available settings are explained as follows:

Item	Description
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.
User	Display the users which connect to Vigor router currently. You can click the link under the username to open the user profile setting page for that user.
IP Address	Display the IP address of the device.
Profile	Display the authority of the account.
Last Login Time	Display the login time that such user connects to the router last time.
Expired Time	Display the expired time of the network connection for the user.
Data Quota	Display the quota for data transmission.
Idle Time	Display the idle timeout setting for such profile.
Action	**Block** - can avoid specified user accessing into Internet. **Unblock** – allow the user to access into Internet. **Logout** - the user will be logged out forcefully.

V-3-5 PPPoE User Online Status

PPPoE User Online Status displays connection information (including IP address, MAC address,user name, transmitted bytes, received bytes, up time and so on) for the LAN client who accesses Internet via the built-in PPPoE server of Vigor router.

User Management >> PPPoE User Online Status

PPPoE User Online Status			Refresh Seconds:	10 ⌄		Refresh	
IP Address	MAC Address	User Name	Rx Bytes	Tx Bytes	Up Time

Available settings are explained as follows:

Item	Description
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.
IP Address	Displays the IP address of the client in LAN.
MAC Address	Displays the MAC address of the client in LAN.
User Name	Displays the name of user connecting to Vigor router currently. You can click the link under the username to open the user profile setting page for that user.
Rx Bytes	Displays the speed of octets received through such PPPoE user.
Tx Bytes	Displays the speed of octets transmitted through such PPPoE user.
Up Time	Displays the connection time of such PPPoE user.

Application Notes

A-1 How to authenticate clients via User Management

Before using the function of User Management, please make sure **User-Based** has been selected as the **Mode** in the **User Management>>General Setup** page.

User Management >> General Setup

General Setup

Mode Selection:

○ **Rule-Based** is a management method based on IP address. Administrator may set different firewall rules to different IP address.

◉ **User-Based** is a management method based on user profiles. Administrator may set different firewall rules to different user profiles.

Notice for User-Based mode:

• In User-Based mode, **Active Rules** in Firewall will be applied to all LAN clients, packets that matches the Active Rules will be blocked or pass immediately, no user authentication is required.

• Only **Inactive Rules** in Firewall can be set for individual user profile. In User-Based mode, packets that do not match Active Rules will need authentication, and the Inactive Rule applied to the specific user profile will then take effect.

With **User Management** authentication function, before a valid username and password have been correctly supplied, a particular client will not be allowed to access Internet through the router. There are three ways for authentication: **Web**, **Alert Tool and Telnet**.

User Management >>User Profile

Profile Index 3
Common Settings

☑ Enable this account

Username   LAN_User_Group_1   (Only support A-Z a-z 0-9 - . @)
Password   ••••••••••
Confirm Password ••••••••••

External Server Authentication   None ▼

Login Settings

Allow Authentication via   ☑ Web ☑ Alert Tool ☑ Telnet
Show Landing Page After Login ☐
Idle Timeout   10   min. (0: Unlimited)
Auto Logout After   0   min. (0: Off)
Pop up Time-Tracking Window ☑
Login Permission Schedule   None ▼ , None ▼ , None ▼ , None ▼

Authentication via Web

■ If a LAN client who hasn't passed the authentication opens an external web site in his browser, he will be redirected to the router's Web authentication interface first. Then, the client is trying to access http://www.draytek.com and but brought to the Vigor router. Since this is an SSL connection, some web browsers will display warning messages.

● With Microsoft Internet Explorer, you may get the following warning message. Please press **Continue to this website (not recommended)**.
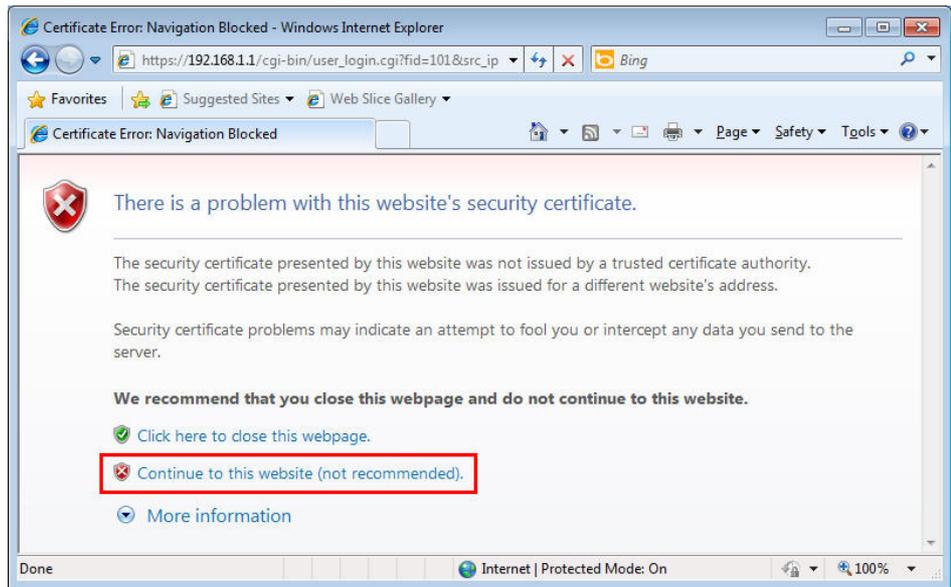
● With Mozilla Firefox, you may get the following warning message. Select **I Understand the Risks**.
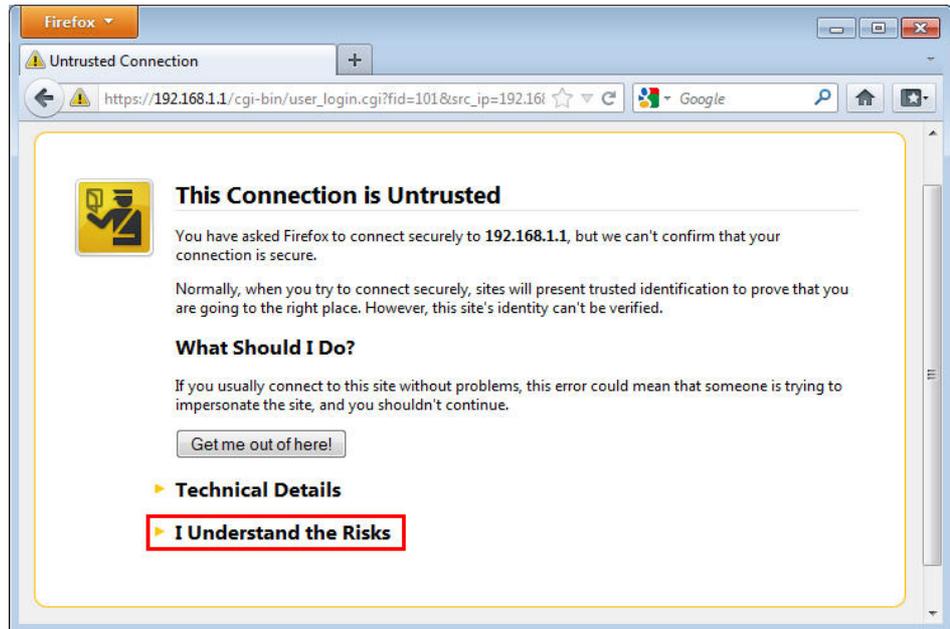
● With Chrome browser, you may get the following warning. Click **Proceed anyway**.
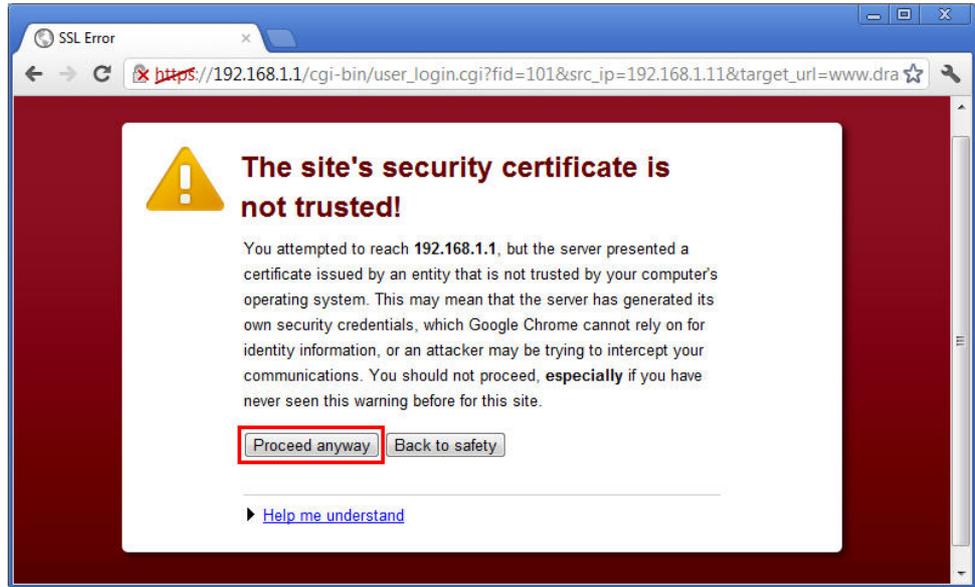
After that, the web authentication window will appear. Input the user name and the password for your account (defined in **User Management**) and click **Login**.
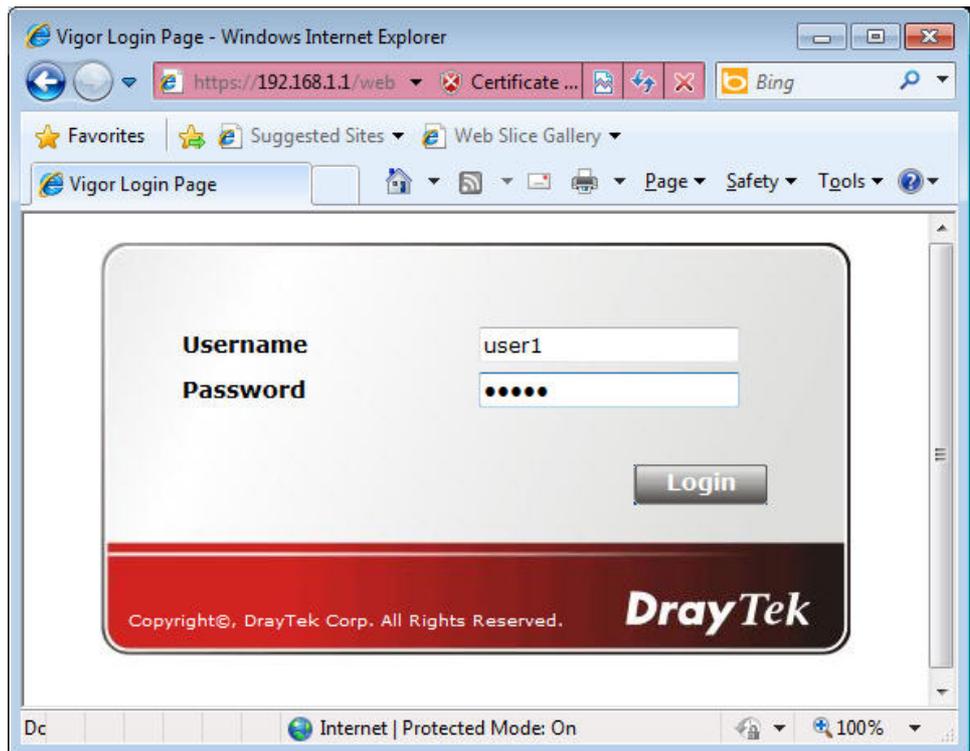
If the authentication is successful, the client will be redirected to the original web site that he tried to access. In this example, it is http://www.draytek.com . Furthermore, you will get a popped up window as the following. Then you can access the Internet.
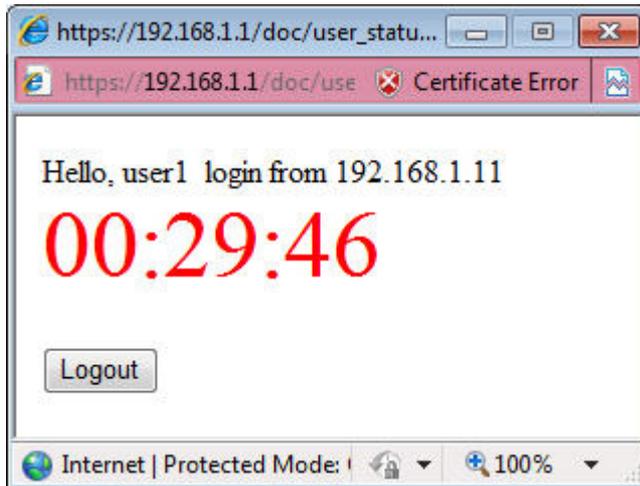
Note, if you block the web browser to pop up any window, you will not see such window.

If the authentication is failed, you will get the error message, **The username or password you entered is incorrect**. Please login again.
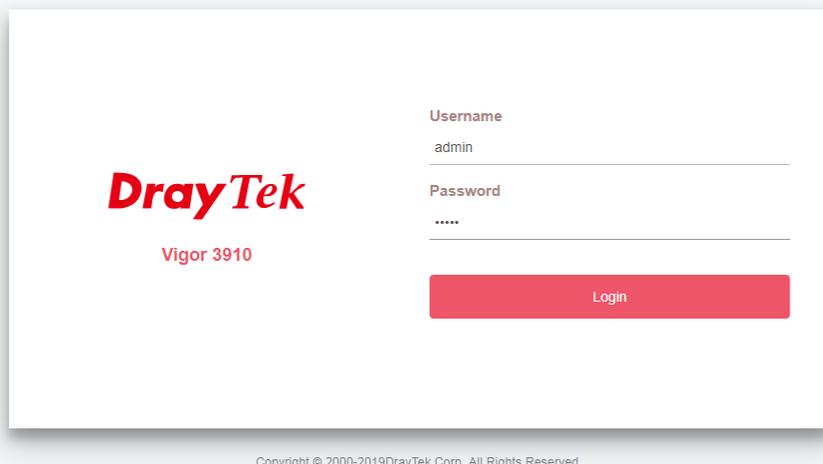
■   In above description, you access an external web site to trigger the authentication. You may also directly access the router's Web UI for authentication. Both HTTP and HTTPS are supported, for example http://192.168.1.1 or https://192.168.1.1 . Replace 192.168.1.1 with your router's real IP address, and add the port number if the default management port has been modified.

If the authentication is successful, you will get the **Welcome Message** that is set in the **User Management >> General Setup** page.

With the default setup **<body stats=1><script language='javascript'> window.location='http://www.draytek.com'</script></body>,** you will be redirected to http://www.draytek.com . You may change it if you want. For example, you will get the following welcome message if you enter **Login Successful** in the **Welcome Message** table.
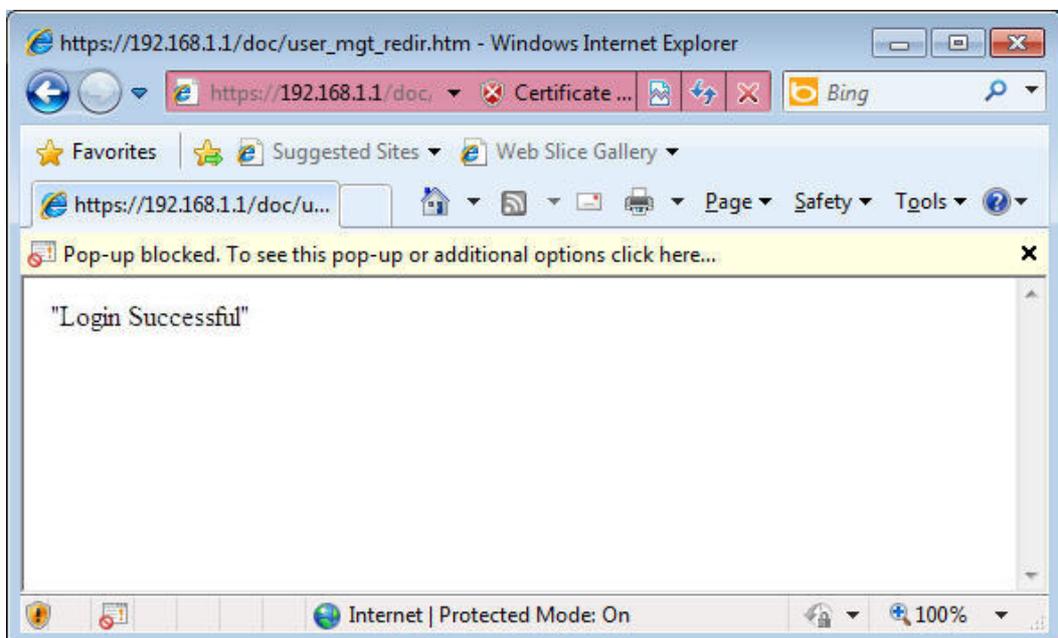
Also you will get a **Tracking Window** if you don't block the pop-up window.

■ Don't setup a user profile in **User Management** and a VPN Remote Dial-in user profile with the same Username. Otherwise, you may get unexpected result. It is because the VPN Remote Dial-in User profiles can be extended to the User profiles in User Management for authentication.

There are two different behaviors when a User Management account and a VPN profile share the same Username:

- If **SSL Tunnel** or **SSL Web Proxy** is enabled in the VPN profile, the user profile in User Management will always be invalid for Web authentication. For example, if you create a user profile in User Management with **chaochen/test** as username/password, while a VPN Remote Dial-in user profile with the same username "chaochen" but a different password "1234", you will always get error message **The username or password you entered is incorrect** when you use **chaochen/test** via Web to do authentication.

VPN and Remote Access >> Remote Dial-in User

Index No. 1

User account and Authentication		Username	chaochen
☑ Enable this account		Password(Max 19 char)	••••••••
Idle Timeout	300 second(s)	☐ Enable Mobile One-Time Passwords(mOTP)	
		PIN Code	
Allowed Dial-In Type		Secret	
☑ PPTP			
☑ IPsec Tunnel		**IKE Authentication Method**	
☑ L2TP with IPsec Policy [None ▼]		☑ Pre-Shared Key	
☑ SSL Tunnel		[IKE Pre-Shared Key]	
☐ Specify Remote Node		☐ Digital Signature(X.509)	
Remote Client IP		[None ▼]	
or Peer ID		**IPsec Security Method**	
Netbios Naming Packet ⦿ Pass ○ Block		☑ Medium(AH)	
Multicast via VPN ○ Pass ⦿ Block		High(ESP) ☑ DES ☑ 3DES ☑ AES	
(for some IGMP,IP-Camera,DHCP Relay..etc.)		Local ID (optional)	
Subnet			
[LAN 1 ▼]			
☐ Assign Static IP Address			
0.0.0.0			

- If **SSL Tunnel** or **SSL Web Proxy** is disabled in the VPN profile, a User Management account and a remote dial-in VPN profile can use the same Username, even with different passwords. However, we recommend you to use different usernames for different user profiles in User Management and VPN profiles.

Authentication via Telnet

The LAN clients can also authenticate their accounts via telnet.

1. Telnet to the router's LAN IP address and input the account name for the authentication:
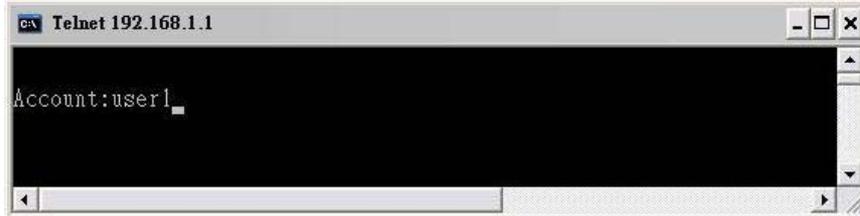
2. Type the password for authentication and press **Enter**. The message **User login successful** will be displayed with the expired time (if configured).
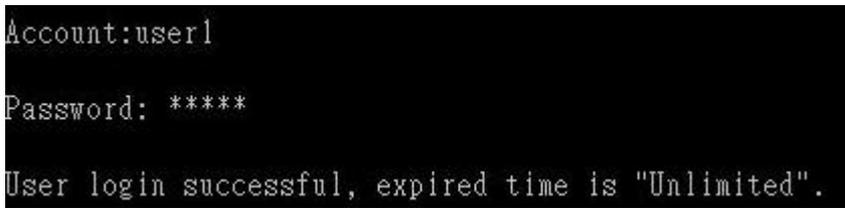
Info	Here expired time is "Unlimited" means the Time Quota function is not enabled for this account. After login, this account will not be expired until it is logout.

3. In the Web interface of router, the configuration page of **Time Quota** is shown as below.
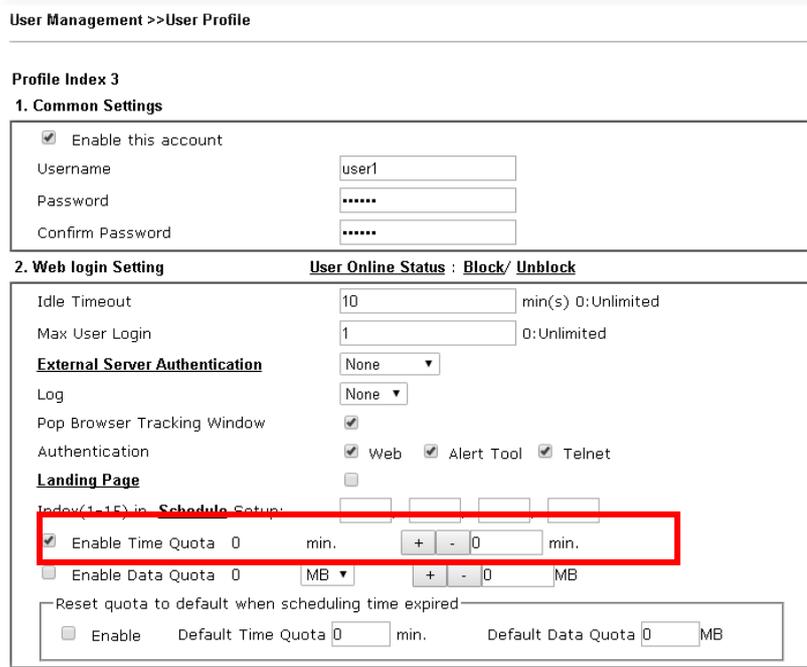
4. If the Time Quota is set with "0" minute, you will get the following message which means this account has no time quota.

If the **Time Quota** is enabled and time is not 0 minute,

You will get the following message. The expired time is shown after you login.

After you run out the available time, you can't use this account any more until the administrator manually adds additional time for you.

Authentication via VigorPro Alert Notice Tool

Authentication via Web or Telnet is convenient for users; however, it has some limitations. The most advantage with VigorPro Alert Notice Tool to operate the authentication is the ability to do **auto login**. If the timeout value set on the router for the user account has been reached, the router will stop the client computer from accessing the Internet until it does an authentication again. Authentication via VigorPro Alert Notice Tool allows user to setup the re-authentication interval so that the utility will send authentication requests periodically. This will keep the client hosts from having to manually authenticate again and again.

The configuration of the VigorPro Alert Notice Tool is as follows:

1. Click **Authenticate Now!!** to start the authentication immediately.

2. You may get the **VigorPro Alert Notice Tool** from the following link:
   http://www.draytek.com/user/SupportDLUtility.php

Info 1	Any modification to the Firewall policy will break down the connections of all current users. They all have to authenticate again for Internet access.
Info 2	The administrator may check the current users from **User Online Status** page.

A-2 How to use Landing Page Feature

Landing Page is a special feature configured under **User Management**. It can specify the message, content to be seen or specify which website to be accessed into when users try to access into the Internet by passing the authentication. Here, we take Vigor3910 Series router as an example.

Example 1：Users can see the message for landing page after logging into Internet successfully

1. Open the web user interface of Vigor3910.

2. Open **User Management** -> **General Setup** to get the following page. In the field of **Landing Page**, please type the words of "**Login Success**". Please note that the maximum number of characters to be typed here is 255.

3. Now you can enable the **Landing Page** function. Open **User Management** -> **User Profile** and click one of the index number (e.g., index number 3) links.

4. In the following page, check the box of **Landing page** and click **OK** to save the settings.

User Management >>User Profile

Profile Index 3
Common Settings

☑ Enable this account

Username	Caca	(Only support A-Z a-z 0-9 - . @)
Password	••••••••••	
Confirm Password		
External Server Authentication	None ▼	

Login Settings   User Online Status : Block/ Unblock

Allow Authentication via	☑ Web ☑ Alert Tool ☑ Telnet	
Show Landing Page After Login	☑	
Idle Timeout	10	min. (0: Unlimited)
Auto Logout After	0	min. (0: Off)
Pop up Time-Tracking Window	☑	
Login Permission Schedule	None ▼ None ▼ None ▼ None ▼	

5. Open any browser (e.g., FireFox, Internet Explorer). The logging page will appear and asks for username and password. Please enter the correct username and password.

DrayTek

Vigor 3910

Username
Caca
Password
••••••••••

Login

6. Click **Login**. If the logging is successful, you will see the message of Login Success from the browser you use.

[Powered by Draytek]

https://192.168.10.1/doc/user_login

DrayTek Group   翻譯字典   電腦科技   其他書籤

Login Success

Example 2：The system will connect to http://www.draytek.com automatically after logging into Internet successfully

1. In the field of **Landing Page**, please type the words as below:

    " <body stats=1><script language='javascript'>

    window.location='http://www.draytek.com'</script></body>"

2. Next, enable the **Landing Page** function. Open **User Management -> User Profile** and click one of the index number (e.g., index number 3) links.

3. In the following page, check the box of **Landing page** and click **OK** to save the settings.

4. Open any browser (e.g., FireFox, Internet Explorer). The logging page will appear and asks for username and password. Please enter the correct username and password.

5. Click **Login**. If the logging is successful, you will be directed into the website of www.draytek.com.
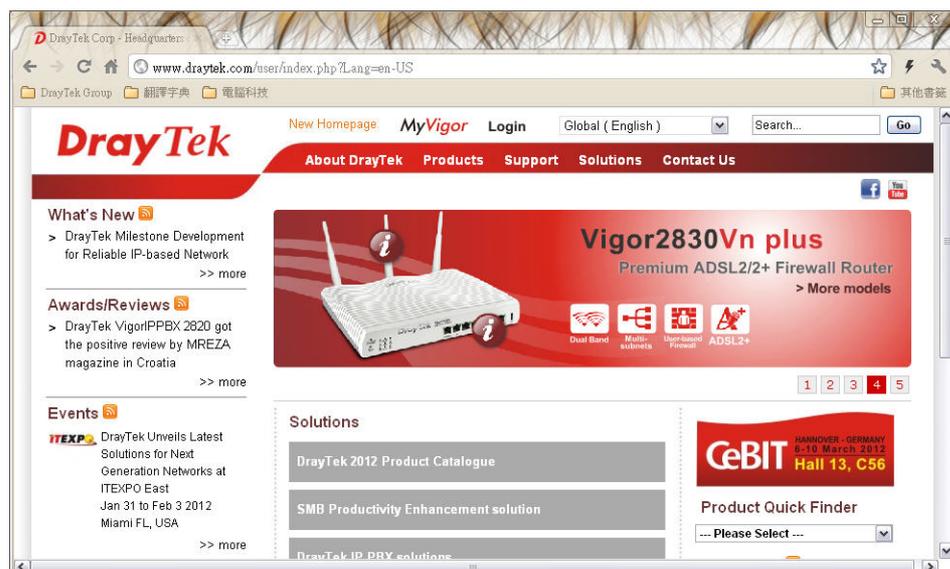
V-4 Hotspot Web Portal

The Hotspot Web Portal feature allows you to set up profiles so that LAN users could either be redirected to specific URLs, or be shown messages when they first attempt to connect to the Internet through the router. Users could be required to read and agree to terms and conditions, or authenticate themselves prior to gaining access to the Internet. Other potential uses include the serving of advertisements and promotional materials, and broadcast of public service announcements.

Web User Interface

V-4-1 Profile Setup

Select **Profile Setup** to create or modify Portal profiles. Up to 4 profiles can be created to meet different requirements according to LAN subnets, WLAN SSIDs, origin and destination IP addresses, etc.

Available settings are explained as follows:

Item	Description
Index	Click the index number link to view or update the profile settings.
Enable	Check the box to enable the profile.
Comments	Shows the description of the profile.
Login Mode	Shows the login mode used by the profile. See the section *Login Mode* for details.
Applied Interface	Shows the interfaces to which this profile applies.
Preview	Click this button to preview the Hotspot Web Portal page that will be displayed to users.

V-4-1-1 Login Method

There are five login methods to choose from for authenticating network clients: **Skip Login**, **Click Through**, **Social Login**, **PIN Login**, and **Social or PIN Login**. Each login mode will present a different web page to users when they connect to the network.

(A) Skip Login, landing page only

This mode does not perform any authentication. The user will be redirected to the landing page. The user can then leave the landing page to visit other websites.

(B) Click-through

The following page will be shown to the users when they first attempt to access the Internet through the router. After clicking **Accept** on the page, users will be directed to the landing page (defined in Captive Portal URL) and be granted access to the Internet.

(C) Various Hotspot Login

An authentication page will appear when users attempt to access the Internet for the first time via the router. After authenticating themselves using a Facebook account, Google account, PIN code, password for RADIUS sever, they will be directed to the landing page and be granted access to the Internet.

(D) External Portal Server

External RADIUS server will authenticate the users when they attempt to access the Internet for the first time via the router.

V-4-1-2 Steps for Configuring a Web Portal Profile

(1) Login Method

Click the index link (e.g., #1) of the selected profile to display the following page.

Available settings are explained as follows:

Item	Description
Enable this profile	Check to enable this profile.
Comments	Enter a brief description to identify this profile.
Portal Server	
Portal Method	There are four methods to be selected as for portal server. ○ Skip Login, landing page only ○ Click through ◉ Various Hotspot Login ○ External Portal Server
*When **Skip Loging, landing page only** or **Click through** is selected as Portal Method*	
Captive Portal URL	Enter the captive portal URL.

When *Various Hotspot Login* is selected as Portal Method	
Captive Portal URL	Enter the captive portal URL.
Login Methods	This setting is available when **Various Hotspot Login** is selected as the portal method.
	Choose Login Method - Select one or more desired login methods.
	● Login with Facebook
	● Login with Google
	● Receive PIN via SMS
	● Login with RADIUS
Facebook (Login with Facebook)	This setting is available when **Login with Facebook** is selected as the login method.
	Facebook APP ID - Enter a valid Facebook developer app ID.
	If you do not already have an app ID, refer to section A-1 *How to create a Facebook App ID for Web Portal Authentication* for instructions on obtaining an APP ID.
	Facebook APP Secret - Enter the secret configured for the APP ID entered above.
	Refer to section A-1 *How to create a Facebook App ID for Web Portal Authentication* for details.
Google (Login with Google)	This setting is available when **Login with Google** is selected as the login method.
	Google App ID - Enter a valid Google app ID.
	If you do not already have an app ID, refer to section A-2 *How to create a Google App ID for Web Portal Authentication* for instructions on obtaining an APP ID.
	Google App Secret - Enter the secret configured for the APP ID entered above.
	Refer to section A-2 *How to create a Google APP ID for Web Portal Authentication* for details.
SMS Provider (Receive PIN via SMS)	This setting is available when **Receive PIN via SMS** is selected as the login method.
	Receiving PIN via SMS Provider - Select the SMS Provider used to send PIN notifications SMS providers are configured in **Objects Setting >> SMS / Mail Service Object**.
Radius Server (Login with RADIUS)	This setting is available when **Login with RADIUS** is selected as the login method.
	Authentication Method – Click link to configure the external RADIUS server for authenticating web portal clients.
	RADIUS MAC Authentication – Check **Enable** to activate user authentication by MAC address.
	MAC Address Format – Select the MAC address format that is used by the RADIUS server.
	RADIUS NAS-Identifier - It is an attribute of the RADIUS server, used by a client as an identification on a RADIUS server. Enter a string with less than 32 characters.
When *External Portal Server* is selected as Portal Method	
Captive Portal URL	Enter the captive portal URL.
Redirection URL	Enter the URL to which the client will be redirected.
RADIUS Server	**Authentication Method** - To configure the RADIUS server, click the External RADIUS Server link and you will be presented with the

	configuration page.
	RADIUS MAC Authentication - If the RADIUS server supports authentication by MAC address, enable **RADIUS MAC Authentication** and select the MAC address format that is used by the RADIUS server.
	RADIUS NAS-Identifier - It is an attribute of the RADIUS server, used by a client as an identification on a RADIUS server. Enter a string with less than 32 characters.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to save the configuration on this page and proceed to the next page.

If you have chosen **Skip Login, landing page only** or **External Portal Server** as the portal method, skip to step 4 *Whitelisting* below.

Otherwise, proceed to configure the login page by following steps 2 and 3.

② **Background**

If you have selected a Login Mode that requires authentication, select a background for the login page.

Available settings are explained as follows:

Item	Description
Choose Login Background	Select either **Color Background** or **Image Background** as the login page background scheme.
Browser Tab Title	Enter the text to be shown as the webpage title in the browser.

Logo Image	The DrayTek Logo will be displayed by default. However, you can enter HTML text or upload an image to replace the default logo.
Login Method Background Color	Select the background color of the login panel from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color.
Opacity (10 ~ 100)	Available when Image Background is selected. Set the opacity of the background image.
Background Image	Available when Image Background is selected. Click **Browse…** to select an image file (.JPG or .PNG format), then click **Upload** to upload it to the router.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

If you have selected **Skip Login**, **landing page only** or **External Portal Server** as the portal method, proceed to Step 4 *Whitelist Setting*; otherwise, continue to Step 3 *Login Page Setup.*

Login Page Setup

In this step you can configure settings for the login page.

Click Through

This section describes the Login Page setup if you have selected **Click Through** as the Login Method.

Available settings are explained as follows:

Item	Description
Welcome Message	Enter the text to be displayed as the welcome message.
Terms and	Enter the text to be displayed as the Terms and Conditions

Conditions Description	hyperlink text.
Terms and Conditions Content	Enter the text to be displayed in the Terms and Conditions pop-up window.
Accept Button Description	Enter the text to be displayed on the accept button
Accept Button Color	Select the color of the accept button from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

Various Hotspot Login

This section describes the Login Page setup step if you have selected Various Hotspot Login the login method. You will see only settings that are relevant to the selected login method(s).

Hotspot Web Portal >> Profile Setup

Settings that are common to Facebook, Google, PIN, and RADIUS authentication are:

Item	Description
Welcome Message	Enter the text to be displayed as the welcome message.
Terms and Conditions Description	Enter the text to be displayed as the Terms and Conditions hyperlink text.
Terms and Conditions Content	Enter the text to be displayed in the Terms and Conditions pop-up window.

If you have selected Facebook login, the setting will appear:

Facebook Login Description

```
Log in with Facebook
```

(Max 170 characters)   Default

Item	Description
Facebook Login Description	Enter the text to be displayed on the Facebook login button.

If you have selected Google login, the setting will appear:

Google Login Description

```
Log in with Google
```

(Max 170 characters)   Default

Item	Description
Google Login Description	Enter the text to be displayed on the Google login button.

If you have selected PIN login, these settings will appear:

Hint Message for PIN	Log in with PIN code.
	(Max 170 characters) [Default]

Receiving PIN via SMS Description	Receive PIN via SMS
	(Max 170 characters) [Default]
Receiving PIN via SMS Content	Welcome to DrayTek Hotspot! Your PIN is <PIN>. This PIN is valid for 10 min.
	(Max 150 characters) [Default]

Enter PIN Description	Enter Existing PIN
	(Max 170 characters) [Default]
Submit Button Description	Submit
	(Max 170 characters) [Default]
Submit Button Color	Customize Color ▾
	A2A2A2 (format : FFFFFF) [Preview] [Default]

Item	Description
Hint Message for PIN	Enter the text used to suggest users to choose SMS authentication.
Receiving PIN via SMS Description	Enter the text to be displayed on the button that the user clicks to receive an SMS PIN.
Receiving PIN via SMS Content	Enter the message to be sent by SMS to inform the user of the PIN. The PIN variable is specified by **<PIN>** within the message.
Enter PIN Description	Enter message to be displayed in the PIN textbox to prompt the user to enter the PIN.
Submit Button Description	Enter the text to be displayed on the submit PIN button
Submit Button Color	Select the color of the submit button from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color.

If you have selected RADIUS account login, these settings will appear:

Hint Message for RADIUS	Log in with your account.
	(Max 170 characters) [Default]
RADIUS Account Description	Username
	(Max 170 characters) [Default]
RADIUS Password Description	Password
	(Max 170 characters) [Default]
Login Button Description	\<span style="color:white;"\>Login\</span\>
	(Max 170 characters) [Default]
Login Button Color	Customize Color ▾
	A2A2A2 (format : FFFFFF) [Preview] [Default]

Item	Description
Hint Message for RADIUS	Enter the text used to prompt the user to login.
RADIUS Account Description	Enter the text to prompt the user to enter the username.
RADIUS Password Description	Enter the text to prompt the user to enter the password.
Login Button Description	Enter the text to be displayed on the login button.
Login Button Color	Select the color of the login button from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color.

And finally, the save and cancel buttons are always displayed.

[Save and Next] [Cancel]

Item	Description
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

2nd-stage Page for PIN Login

If you have selected **PIN Login** as the login method, you will also need to configure the page that is displayed to users when they request a PIN.

Available settings are explained as follows:

Item	Description
Back Button Description	Enter text for the label of the hyperlink to return to the previous page.
PIN Code Message	Enter text to be displayed as the body text on the page.
Default Country	Select the default country code to be displayed using the dropdown

Code	menu.
Enter Mobile Number Description	Enter message to be displayed in the mobile number textbox to prompt the user to enter the mobile number.
Send Button Description	Enter the label text of the send button.
Send Button Color	Select the color of the send button from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color.
Send Succeeded Message	Enter text to be displayed to notify the user after the PIN has been sent.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

![4] Whitelist Setting

In this step you can configure the whitelist settings. Users are allowed to send and receive traffic that satisfies whitelist settings.

Hotspot Web Portal >> Profile Setup

1	2	3	**4**	5
Login Method	Background	Login Page Setup	**Whitelist Setting**	More Options

NAT Rules	Dest Domain	Dest IP	Dest Port	Source IP
Always allow outbound connections from hosts in	☐ NAT >> Port Redirection ☐ NAT >> Open Ports ☐ NAT >> DMZ			

[Save and Next]   [Cancel]

Available settings are explained as follows:

Item	Description
NAT Rules	To prevent web portal settings from conflicting with NAT rules resulting in unexpected behavior, select the NAT rules that are allowed to bypass the web portal. Hosts listed in selected NAT rules can always access the Internet without being intercepted by the web portal.
Dest Domain	Enter up to 30 destination domains that are allowed to be accessed.
Dest IP	Enter up to 30 destination IP addresses that are allowed to be accessed.
Dest Port	Enter up to 30 destination protocols and ports that are allowed through the router.
Source IP	Enter up to 30 source IP addresses that are allowed through the router.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

5 More Options

In this step you can configure advanced options for the Hotspot Web Portal.

Available settings are explained as follows:

Item	Description
Quota Management	
Expired Time After Activation	Enter the time duration that users are allowed to have Internet access after logging in.

Quota Policy Profile	Choose a policy profile to apply to web portal clients.

Web Portal Options

HTTPS Redirection	If this option is selected, unauthenticated clients accessing HTTPS websites will be redirected to the login page, but the browser may alert the user of certificate errors. If this option is not selected, attempts to access to HTTPS website will time out without redirection.
Captive Portal Detection	If this option is selected, the web portal page is triggered automatically when an unauthenticated client tries to access the Internet. This function is not available when the Login Mode is **Social Login**, as the web portal page may not be shown correctly due to the limitations of the operating system's built-in Captive Portal Detection.

Landing Page After Authentication

Fixed URL	Specifies the webpage that will be displayed after the user has successfully authenticated. The user will be redirected to the specified URL. This could be used for displaying advertisements to users, such as guests requesting wireless Internet access in a hotel.
User Requested URL	The user will be redirected to the URL they initially requested.
Bulletin Message	The message configured here will be briefly shown for a few seconds to the user. **Default Message –** This button is enabled when **Bulletin Message** is selected. Click to load the default text into the bulletin message textbox.
Force Landing Page Stay	This option is useful for mobile phone user. The mobile phone users can access into Internet by means of Wi-Fi connection. In general, when **Captive Portal Detection** is enabled on Vigor router, the login page will appear once the mobile phone detects the Wi-Fi signal. After entering the username and password (for authentication), the landing page will appear first on the screen of the mobile phone. Yet, some mobile phone will skip the landing page and access the Internet instead. This feature can force the landing page to stay on the screen of the mobile phone for a while. **Enable -** Select it to enter the period of time for keeping the landing page.

Applied Interfaces

Subnet	The current Hotspot Web Portal profile will be in effect for the selected subnets.
Finish	Click to complete the configuration.
Cancel	Click to abort the configuration process and return to the profile summary page.

V-4-2 Quota Management

The system administrator can specify bandwidth and sessions quota which is only applicable to the web portal clients.

Settings configured in Quota Management will override the policies set in **Bandwidth Management>>Bandwidth Limit** and **Bandwidth Management>>Limit**.

Hotspot Web Portal >> Quota Management

Web Portal Bandwidth and Session Limit

The settings here will apply only to the web portal clients and will override the policies set in Bandwidth Management.

☐ Bandwidth Limit
☐ Session Limit

Quota Policy Profile

Index	Name	Expired Time after First Login	Device Allowed per Account	Reconnection Time Restriction	Bandwidth Limit	Session Limit
1	Default	0d 5h 0m	Unlimited	Unlimited	Unlimited	Unlimited

[Add] (up to 20)

[Cancel] [OK]

Available settings are explained as follows:

Item	Description
Bandwidth Limit	Check the box to override the policy configured in **Bandwidth Management>>Bandwidth Limit**.
Session Limit	Check the box to override the policy configured in **Bandwidth Management>>Session Limit**.
Quota Policy Profile	**Add** - Create up to 20 policy profiles in such page.

To create a new quotal policy profile, click **Add** to open the followining page.

Hotspot Web Portal >> Management >> Quota Policy Profile 2

Profile Name	level 2

Account Validity

Expired Time After the First Login   0 ▼ days   5 ▼ hours   0 ▼ min

☐ Idle Timeout   0   min

Device Control

Devices Allowed per account   Unlimited ▼

☐ Reconnection Time Restriction   ○ At 0 ▼ : 0 ▼ everyday

Block the same user from reconnecting before the set time

◉ 0 ▼ hours 0 ▼ min

Block the same user from reconnecting for the set period

Bandwidth and Session Limit

☐ Bandwidth Limit

     Download Limit   0   ◉ Kbps   ○ Mbps

     Upload Limit   0   ◉ Kbps   ○ Mbps

☐ Session Limit   0   sessions

Cancel   OK

Available settings are explained as follows:

Item	Description
Profile Name	Enter a name for a new profile.
Account Validity	Set the duration for which the login is valid. **Expired Time After the First Login** – Sets the days, hours, and minutes. After the login has expired, Vigor router will block the client from accessing the network/Internet. **Idle Timeout** – When this option is selected, Vigor router will terminate the network connection if the is no activity from the user after the specified idle time has passed.
Device Control	Set the maximum number of devices that can be connected for each account, and the time restriction for the client accessing Internet via the web portal. **Devices Allowed per account** – Use the drop-down list to select the maximum number of devices that can be connected to the network using the same account. **Reconnection Time Restriction** – Blocks the account from being used to connect devices to the network in one of two ways: ● **At …. Everyday** – After the login expires, the account cannot be used to connect devices to the network until the set time of day. ● **Hours.. min** – After the login expires, the account cannot be used to connect devices to the network for a set period of time.
Bandwidth and	**Bandwidth Limit** – Check the box to configure bandwidth limit for

Session Limit	web portal client.
	● **Download/Upload Limits** – Set the maximum upload and download speeds.
	Session Limit- Check the box to configure a maximum session limit for web portal clients.

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

Application Notes

A-1 How to allow users login to Vigor's Hotspot with their social media accounts (e.g., Facebook & Google)

Vigor Router supports Hotspot Web Portal function. The network administrator can set Vigor Router as a Hotspot provider with web authentication and allow users to log in with their social media accounts, such as Facebook and Google. We demonstrate how to set up the hotspot web portal with Facebook login in the following paragraphs.

Vigor Router Setup

1. Make sure the router is connected to the Internet.

2. Go to **Hotspot Web Portal** >> **Profile Setup**, click on an available index.

3. Enter the values as the following figure.

(a) Click **Enable this profile**.

(b) Enter the comments.

(c) Select **Various Hotspot Login** for Portal Method.

(d) Choose **Login with Facebook** or **Login with Google** as Login Method.

   If **Login with Facebook** is selected, the protocol of the **Captive Portal URL** need to be changed to **HTTPS** instead of HTTP because Facebook force to use **HTTPS** URL in their policy.

(e) Enter the **APP ID** and **secret**.

(f) Click **Save and Next**.

4. Choose the **Color Background**, customize the information a logo color, and click **Save and Next**.

Hotspot Web Portal >> ProfileSetup

You can click the Step Icon on the top of the page to go to the step you want. The router will save your setting automatically.

Or choose the **Image Background**, customize the information and background image, and click **Save and Next**.

Hotspot Web Portal >> ProfileSetup

Choose Login Background

○ Color Background

1. Browser Tab Title
2. Logo Image & Logo Background Color
3. Login Methods Background Color

◉ Image Background

1. Browser Tab Title
2. Logo Image
3. Loging Methods Background Color and Opacity
4. Background Image

Login Page URL	portal.draytek.com
Browser Table Title	Draytek Hotspot

Logo Image	Default Draytek Logo Red ▼

DrayTek

Login Method Background Color	Vigor Gold ▼		
	F4E1D0	(format : FFFFFF)	Preview
Opacity(10 ~ 100)	80	%	

Background Image	Choose File No file chosen	(max size: 1MB)	Upload

5. Customize the descriptions on the login page, then click **Save and Next**.

6. You can set the **Whitelist** for the profile here to allow specific clients to access the internet or certain websites can be visited without login.

7. Set up the **Expired Time After Activation** and **Landing Page After Activation** that Hotspot clients will see after they login successfully. Finally, select the interfaces to which you would like this hotspot profile apply to, then click **Finish** to save the setting.

8. Then the Hotspot setup is finished. You may click Preview to check the login page.

Hotspot Clients Login

9. Now, when clients connect to the selected router interface, and try to access internet, they will be redirected to "portal.draytek.com".
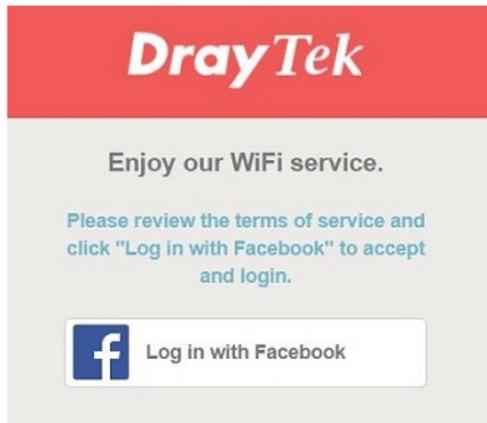
- Due to security concerns, the browser might warns that it cannot verify server identity, the clients would need to tap "Continue" before they can proceed to portal.draytek.com.

- The client might not be able to access "portal.draytek.com" if this domain name is resolved by a DNS server on LAN. If so, set up LAN DNS to make sure the domain name will be resolved to the router's LAN IP.

10. Tap on a login method, and it will open the social media login page. Enter the social media accounts and password to log in.
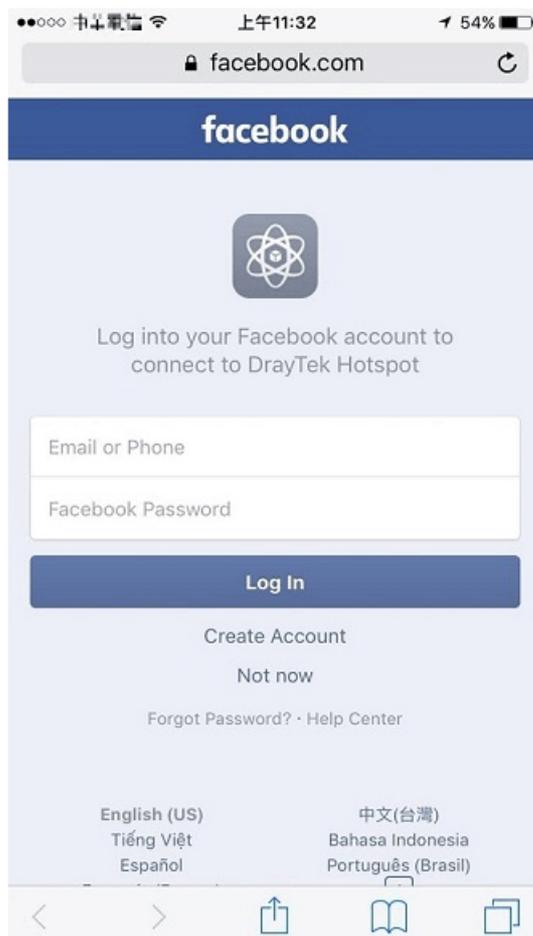
11. If the credentials are correct, the client will be redirected to the landing page and be able to access the Internet afterward.
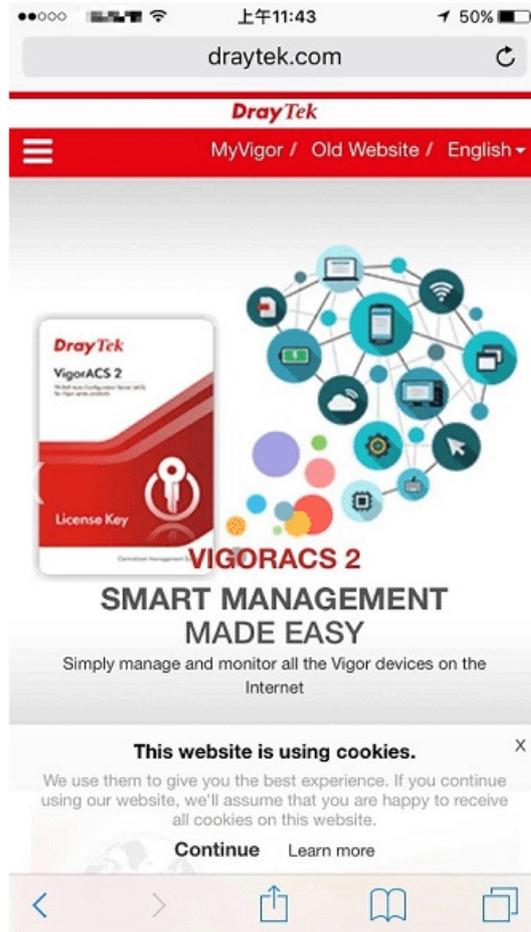
User Information

Network administrator can plug the USB disk to router, to record the basic information of the users who connect to the Wi-Fi and login with their social media accounts. The users' basic information will be listed on Hotspot Web Portal >> Users Information page.

A-2 How to allow hotspot clients to get login PIN code via SMS?

Since 3.8.4.3 version firmware, Vigor Router can act as a hotspot gateway and provide internet access only to the authenticated clients. Network Administrator may set up the router to allow hotspot client to get the login PIN code from an SMS message. This note is going to demonstrate how to set up Vigor Router as a hotspot gateway and be able to send the PIN code to clients by SMS messages.

Vigor Router Setup

1. Make sure the router is connected to the Internet.

2. Create an SMS Object to send SMS messages. Go to **Objects Setting >> SMS Service Object**, and click on an available profile.

3. Enter the Service Provider details, and click **OK** to apply.

Objects Setting >> SMS / Mail Service Object

Profile Index: 1

Profile Name	hotspot
Service Provider	kotsms.com.tw (TW) ▼
Username	m▬▬▬
Password	••••••••••
Quota	10
Sending Interval	3 (seconds)

4. Go to Hotspot Web Portal >> Profile Setup, click on an available profile.

Hotspot Web Portal >> Profile Setup

Hotsport Web Portal Profile:

Index	Enable	Comments	Login Mode	Applied Interface	
1.	☐		Skip Login	None	Preview
2.	☐		Skip Login	None	Preview
3.	☐		Skip Login	None	Preview
4.	☐		Skip Login	None	Preview

5. **Enable** the profile, give a comment, and choose "PIN Code Login". Then click **Next**.

Hotspot Web Portal >> Hotspot Web Portal Setup

Profile 1
☑ Enable
Comments: SMS authenticate

Choose How Users Receive Internet Access

○ Skip Login
skip login phase and redirect to landing page immediately

○ Click-through

DrayTek
Your Reliable Networking Solution Partner
Welcome!
Please log in to enjoy Wifi.
By clicking the button below you agree to the Terms and Conditions.
Accept
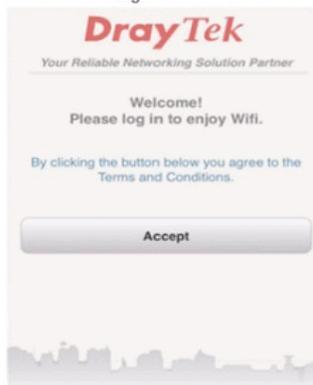
A space for you to display the terms and conditions.Users have to click Accept button (wording configurable) to get WiFi access.

○ Social Login

DrayTek
Your Reliable Networking Solution Partner
Welcome!
Please log in to enjoy Wifi.
By clicking the button below you agree to the Terms and Conditions.
f Login with Facebook
G Login with Google
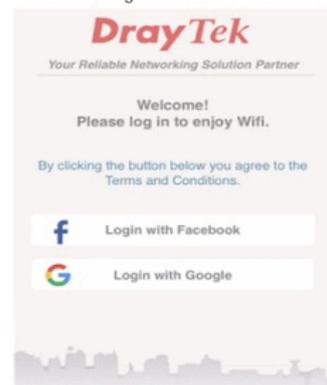
Login with Facebook or Google account.

◉ PIN Code Login

DrayTek
Your Reliable Networking Solution Partner
Welcome!
Please log in to enjoy Wifi.
By clicking the button below you agree to the Terms and Conditions.
Via SMS

○ Social or PIN Login

DrayTek
Your Reliable Networking Solution Partner
Welcome!
Please log in to enjoy Wifi.
By clicking the button below you agree to the Terms and Conditions.
f Login with Facebook
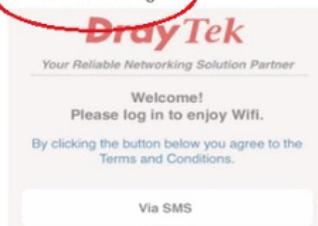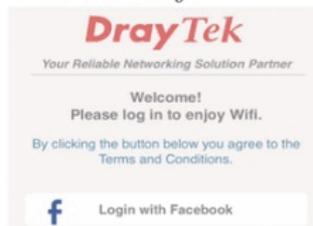
6. Choose a login page design, customize the details, and click **Next**.

Hotspot Web Portal >> Hotspot Web Portal Setup

Profile 1
Design Login Page Appearance

⦿ Color Background

- 1. Browser Tab Title
- 2. Logo Image & Logo Background Color
- 3. Login Methods Background Color

○ Image Background
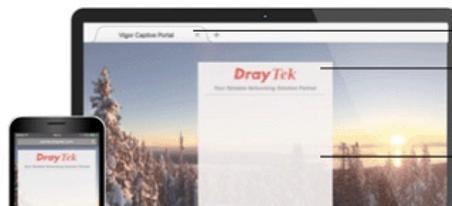
- 1. Browser Tab Title
- 2. Logo Image
- 3. Loging Methods Background Color and Opacity

7. Edit the message on the login page, and click **Next**.

Receiving PIN via SMS Description	Get password via SMS
	(Max 170 characters) Default
Recieving PIN via SMS Content	Welcome to DrayTek Hotspot!Your password is <PIN>.This PIN will be valid for 10 min.
	(Max 150 characters) Default
Recieving PIN via SMS Provider	1 - hotspot ▾ Set SMS Provider in *Objects Setting >> SMS / Mail Service Object*
Enter PIN Description	Enter password
	(Max 170 characters) Default
Submit Button Description	Login
	(Max 170 characters) Default
Submit Button Color	A2A2A2 (format : FFFFFF) Default

Back   Next   Cancel

8. Edit the details for SMS settings, then click **Next**.

Back Button Description	
	(Max 170 characters) [Default]
PIN Code Message	Password will be sent over via SMS.
	(Max 170 characters) [Default]
Default Country Code	+ 886 Taiwan ▼
Enter Mobile Number Description	enter your mobile number
	(Max 170 characters) [Default]
Send Button Description	Get password
	(Max 170 characters) [Default]
Send Button Color	A2A2A2 (format : FFFFFF) [Default]
Send Successed Message	Password has been sent. Click >Get password again if not receiving password in 3 minutes.
	(Max 170 characters) [Default]

9. Edit the landing page, choose the interfaces to which the SMS login should apply, and then click **Finish**.

10. Now, the hotspot settings are applied to the selected interfaces. You may click **Preview** to check how the login page looks.

Hotsport Web Portal Profile:

Index	Enable	Comments	Login Mode	Applied Interface	
1.	☑	SMS authenticate	PIN Code Login	WLAN2.4G(2)	Preview
2.	☐		Skip Login	None	Preview
3.					Preview
4.					Preview

Note:
The router mu

Draytek Hotspot - Google Chrome — □ ×

192.168.86.1/doc/hslogp1.htm

DrayTek

Welcome!
Please log in to enjoy Wifi.

Get password via SMS

Enter password — Login
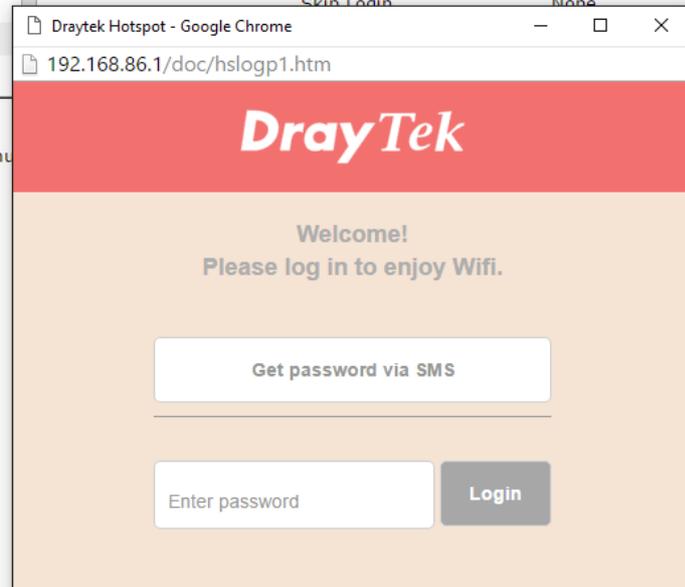
Hotspot Client Login

11. If the client connected to the selected interface of the router and try to open a webpage, they will be redirected to hotspot login page. If they do not have a password yet, they can click on the button to get a password.

●●●●○ 中華電信 🛜　5:01 PM　🔄 ✳ 🔋

portal.draytek.com ↻

DrayTek

Welcome!
Please log in to enjoy Wifi.

Get password via SMS

Enter password — Login
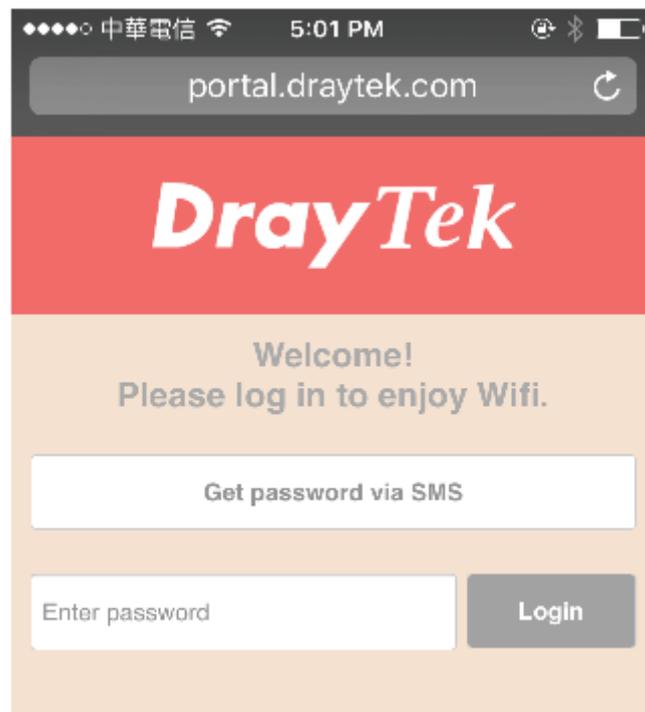
Info
- Due to security concerns, the browser might warns that it cannot verify server identity, the clients would need to tap "continue" before they can proceed to portal.draytek.com.

- The client might not be able to access "portal.draytek.com" if this domain name is resolved by a DNS server on LAN. If so, set up LAN DNS to make sure the domain name will be resolved to the router's LAN IP.

12. Enter the mobile phone number to receive the SMS message.

13. The number will get a message about the password.
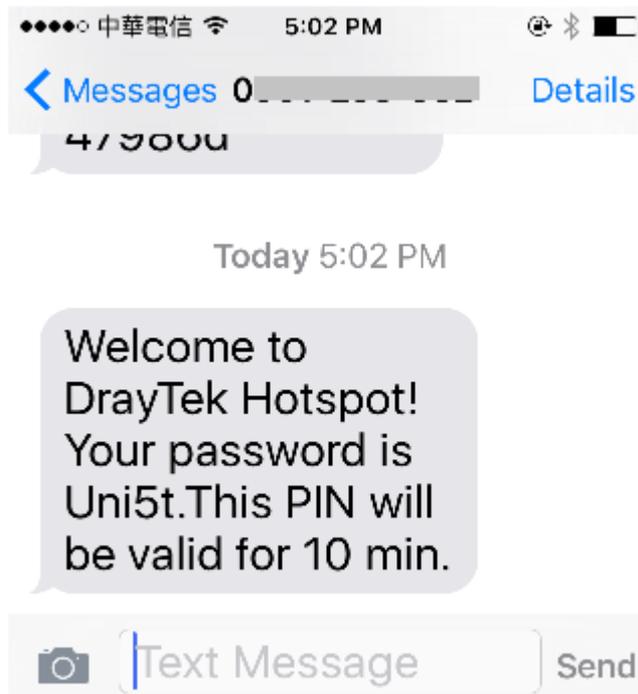
14. Enter the password on the login page, and click **Login**.
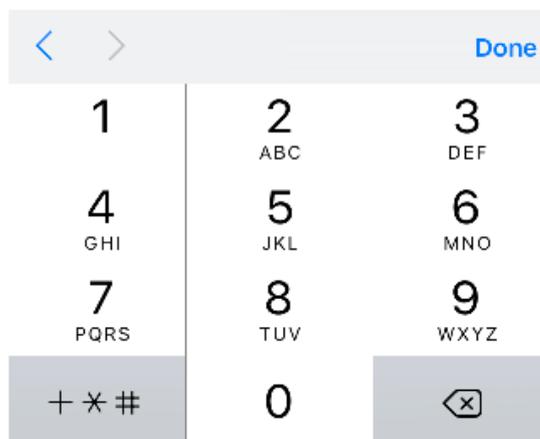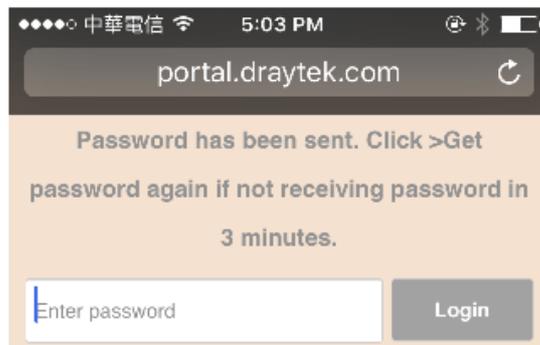
15. If the password is correct, the client will be redirected to the landing page, and after that, they will be able to surf the Internet.
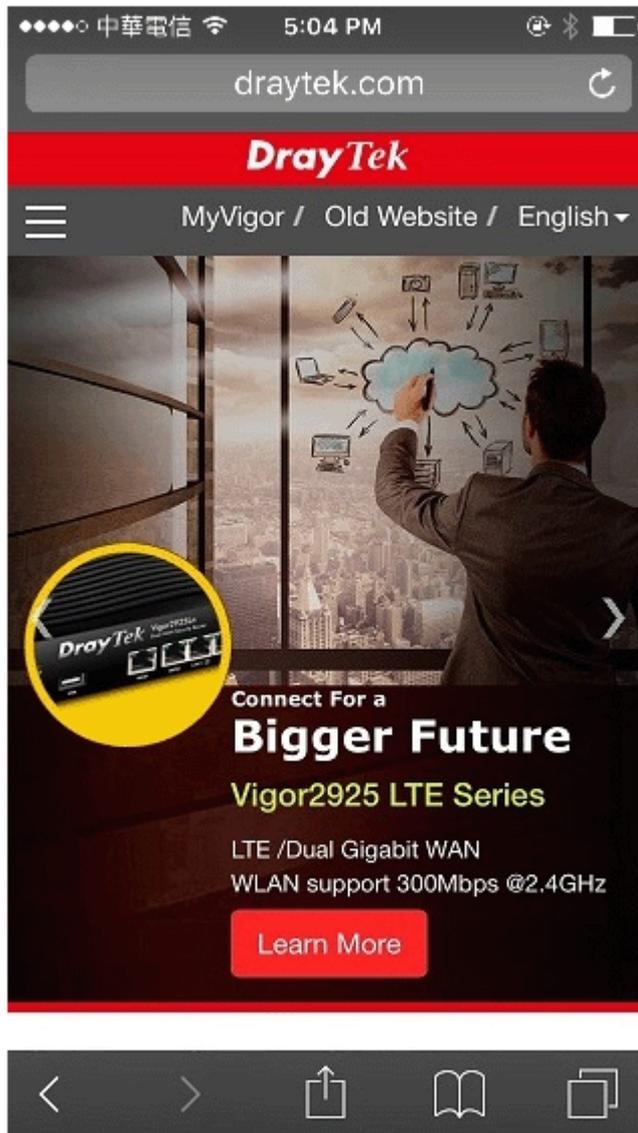
Part VI Others

Objects Settings

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

VI-1 Objects Settings

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

Web User Interface

VI-1-1 IP Object

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

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

Objects Setting >> IP Object

Create from ARP Table
Create from Routing Table

IP Object Profiles: | Set to Factory Default |

View: [All   ▼]   [   ] [Search]

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

<< 1-32 | 33-64 | 65-96 | 97-128 | 129-160 | 161-192 >>   Next >>

Export IP Object	Restore IP Object
● Backup the current IP Objects with a CSV file	選擇檔案 未選擇任何檔案
○ Download the default CSV template to edit	[Restore]
[Download]	

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

Available settings are explained as follows:

Item	Description
View	Use the drop down list to choose a type (Single Address, Range Address, Subnet Address, Mac Address or all) that IP object with the selected type will be shown on this page.
Set to Factory Default	Clear all profiles.
Search	Type a string of the IP object that you want to search.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.
Address	Display the IP address configured for the object profile.
Export IP Object	Usually, the IP objects can be created one by one through the web page of **Objects>>IP Object**. However, to a user who wants to save more time in bulk creating IP objects, a quick method is offered by Vigor router to modify the IP objects with a single file, a CSV file. All of the IP objects (or the template) can be exported as a file by clicking Download. Then the user can open the CSV file through Microsoft Excel and modify all the IP objects at the same time. **Backup the current IP Objects with a CSV file** – Click it to backup current IP objecsts as a CSV file. Such file can be

	restored for future use. **Download the default CSV template to edit** – After clicking it, press Download to store the default CSM template (a table without any input data) to your hard disk. **Download** – Download the CSV file from Vigor router and store in your hard disk.
Restore IP Object	**Select** – Click it to specify a predefined CSV file. **Restore** – Import the selected CSV file onto Vigor router.

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

1.   Click the number (e.g., #1) under Index column for configuration in details.

2.   The configuration page will be shown as follows:

Objects Setting >> IP Object

Profile Index : 1

Name:	RD Department
Interface:	Any ▼
Address Type:	Range Address ▼
Mac Address:	00 : 00 : 00 : 00 : 00 : 00
Start IP Address:	192.168.1.10 [Select]
End IP Address:	192.168.1.10 [Select]
Subnet Mask:	255.255.255.254 / 31 ▼
Invert Selection:	☐

Next >>

[OK]   [Clear]   [Cancel]

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/RT/VPN or any IP address. If you choose LAN/RT/VPN as the **Interface** here, and choose LAN/RT/VPN as the direction setting in **Edit Filter Rule**, then all the IP addresses specified with LAN /RT/VPN interface will be opened for you to choose in **Edit Filter Rule** page.
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.

4.   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

Create from ARP Table
Create from Routing Table

IP Object Profiles:

View: | All ▼ |

Index	Name	Address	Index	Name
1.	RD Department	192.168.1.10 ~ 192.168.1.10	17.	
2.	Financial Dept	Any	18.	
3.	HR Department	211.100.88.0/24	19.	
4.			20.	

VI-1-2 IP Group

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

Objects Setting >> IP Group

IP Group Table: | Set to Factory Default |

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

Available settings are explained as follows:

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

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

1. Click the number (e.g., #1) under Index column for configuration in details.

2. The configuration page will be shown as follows:

Objects Setting >> IP Group

Profile Index : 1

Name: Administration

Interface: Any

Available IP Objects
1-RD Department
2-Financial Dept
3-HR Department

Selected IP Objects

>>
<<

OK   Clear   Cancel

Available settings are explained as follows:

Item	Description
Name	Enter 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.

VI-1-3 IPv6 Object

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

Objects Setting >> IPv6 Object

IPv6 Object Profiles: | Set to Factory Default |

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

<< 1-32 | 33-64 >>   Next >>

Available settings are explained as follows:

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

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

1. Click the number (e.g., #1) under Index column for configuration in details.

2. The configuration page will be shown as follows:

Objects Setting >> IPv6 Object

Profile Index : 1

Name:	
Address Type:	Subnet Address ▾
Mac Address:	00 :00 :00 :00 :00 :00
Start IP Address:	[Select]
End IP Address:	[Select]
Prefix Length:	
Invert Selection:	☐

Next >>

[OK] [Clear] [Cancel]

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Address Type	Determine the address type for the IPv6 address. Select **Single Address** if this object contains one IPv6 address only. Select **Range Address** if this object contains several IPv6s within a range. Select **Subnet Address** if this object contains one subnet for IPv6 address. Select **Any Address** if this object contains any IPv6 address. Select **Mac Address** if this object contains Mac address.
Mac Address	Type the MAC address of the network card which will be controlled.
Start IP Address	Type the start IP address for Single Address type.
End IP Address	Type the end IP address if the Range Address type is selected.
Prefix Length	Type the number (e.g., 64) for the prefix length of IPv6 address.
Invert Selection	If it is checked, all the IPv6 addresses except the ones listed above will be applied later while it is chosen.

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

VI-1-4 IPv6 Group

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

Objects Setting >> IPv6 Group

IPv6 Group Table: | Set to Factory Default |

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

Available settings are explained as follows:

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

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

1. Click the number (e.g., #1) under Index column for configuration in details.

2. The configuration page will be shown as follows:

Objects Setting >> IPv6 Group

Profile Index : 1

Name:

Available IPv6 Objects

Selected IPv6 Objects

[>>]

[<<]

[OK] [Clear] [Cancel]

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Available IPv6 Objects	All the available IPv6 objects with the specified interface chosen above will be shown in this box.
Selected IPv6 Objects	Click >> button to add the selected IPv6 objects in this box.

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

VI-1-5 Service Type Object

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

Objects Setting >> Service Type Object

Service Type Object Profiles: | Set to Factory Default |

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

<< 1-32 | 33-64 | 65-96 >>   Next >>

Available settings are explained as follows:

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

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

1. Click the number (e.g., #1) under Index column for configuration in details.

2. The configuration page will be shown as follows:

Available settings are explained as follows:

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

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

VI-1-6 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.

VI-1-7 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:

Objects Setting >> Keyword Object Setup

Profile Index : 1

Name	
Contents	

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

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

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

[OK]　[Clear]　[Cancel]

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.

VI-1-8 Keyword Group

This page allows you to bind several keyword objects into one group. The keyword groups set here will be chosen as black /white list in CSM >>URL /Web Content Filter Profile.

Objects Setting >> Keyword Group

Keyword Group Table:				Set to Factory Default	
Index	**Name**	**Index**	**Name**
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

Available settings are explained as follows:

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

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

1. Click the number (e.g., #1) under Index column for configuration in details.

2. The configuration page will be shown as follows:

Objects Setting >> Keyword Group Setup

Profile Index : 1

Name: [   ]

Available Keyword Objects
```
1-Key-1
2-Key-2
```

Selected Keyword Objects(Max 16 Objects)

[>>]
[<<]

[OK] [Clear] [Cancel]

Available settings are explained as follows:

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

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

VI-1-9 File Extension Object

This page allows you to set eight profiles which will be applied in **CSM>>URL Content Filter**. All the files with the extension names specified in these profiles will be processed according to the chosen action.

Objects Setting >> File Extension Object

File Extension Object Profiles: | Set to Factory Default |

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

Available settings are explained as follows:

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

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

1. Click the number (e.g., #1) under Profile column for configuration in details.

2. The configuration page will be shown as follows:

Objects Setting >> File Extension Object Setup

Profile Index: 1	Profile Name:

Categories — **File Extensions**

Image
Select All / Clear All
☐ .bmp ☐ .dib ☐ .gif ☐ .jpeg ☐ .jpg ☐ .jpg2 ☐ .jp2
☐ .pct ☐ .pcx ☐ .pic ☐ .pict ☐ .png ☐ .tif ☐ .tiff

Video
Select All / Clear All
☐ .asf ☐ .avi ☐ .mov ☐ .mpe ☐ .mpeg ☐ .mpg ☐ .mp4
☐ .qt ☐ .rm ☐ .wmv ☐ .3gp ☐ .3gpp ☐ .3gpp2 ☐ .3g2
☐ .flv ☐ .swf

Audio
Select All / Clear All
☐ .aac ☐ .aiff ☐ .au ☐ .mp3 ☐ .m4a ☐ .m4p ☐ .ogg
☐ .ra ☐ .ram ☐ .vox ☐ .wav ☐ .wma

Java
Select All / Clear All
☐ .class ☐ .jad ☐ .jar ☐ .jav ☐ .java ☐ .jcm ☐ .js
☐ .jse ☐ .jsp ☐ .jtk

ActiveX
Select All / Clear All
☐ .alx ☐ .apb ☐ .axs ☐ .ocx ☐ .olb ☐ .ole ☐ .tlb
☐ .viv ☐ .vrm

Compression
Select All / Clear All
☐ .ace ☐ .arj ☐ .bzip2 ☐ .bz2 ☐ .cab ☐ .gz ☐ .gzip
☐ .rar ☐ .sit ☐ .zip

Execution
Select All / Clear All
☐ .bas ☐ .bat ☐ .com ☐ .exe ☐ .inf ☐ .pif ☐ .reg
☐ .scr

P2P
Select All / Clear All
☐ .torrent

[OK]   [Clear]   [Cancel]

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for this profile. The maximum length of the name you can set is 7 characters.

3. Type a name for such profile and check all the items of file extension that will be processed in the router. Finally, click **OK** to save this profile.

VI-1-10 SMS/Mail Service Object

SMS Service Object

This page allows you to set ten profiles which will be applied in **Application>>SMS/Mail Alert Service**.

```
Objects Setting >> SMS / Mail Service Object
```

SMS Provider	Mail Server		Set to Factory Default
Index	**Profile Name**	**SMS Provider**	
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.	Custom 1		
10.	Custom 2		

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.
Index	Display the profile number that you can configure.
Profile	Display the name for such SMS profile.
SMS Provider	Display the service provider which offers SMS service.

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

1. Click the **SMS Provider** tab, and click the number (e.g., #1) under Index column for configuration in details.

```
Object Settings >> SMS / Mail Service Object
```

SMS Provider	Mail Server
Index	**Profile Name**
1.	
2.	
3.	
4.	

2. The configuration page will be shown as follows:

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such SMS profile. The maximum length of the name you can set is 31 characters.
Service Provider	Use the drop down list to specify the service provider which offers SMS service.
Username	Type a user name that the sender can use to register to selected SMS provider. The maximum length of the name you can set is 31 characters.
Password	Type a password that the sender can use to register to selected SMS provider. The maximum length of the password you can set is 31 characters.
Quota	Type the number of the credit that you purchase from the service provider chosen above. Note that one credit equals to one SMS text message on the standard route.
Sending Interval	To avoid quota being exhausted soon, type time interval for sending the SMS.

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

Customized SMS Service

Vigor router offers several SMS service provider to offer the SMS service. However, if your service provider cannot be found from the service provider list, simply use Index 9 and Index 10 to make customized SMS service. The profile name for Index 9 and Index 10 are fixed.

You can click the number (e.g., #9) under Index column for configuration in details.

Available settings are explained as follows:

Item	Description
Profile Name	Display the name of this profile. It cannot be modified.
Service Provider	Type the website of the service provider. Type the URL string in the box under the filed of Service Provider. You have to contact your SMS provider to obtain the exact URL string.
Username	Type a user name that the sender can use to register to selected SMS provider. The maximum length of the name you can set is 31

	characters.
Password	Type a password that the sender can use to register to selected SMS provider.
	The maximum length of the password you can set is 31 characters.
Quota	Type the total number of the messages that the router will send out.
Sending Interval	Type the shortest time interval for the system to send SMS.

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

Mail Service Object

This page allows you to set ten profiles which will be applied in **Application**>>**SMS/Mail Alert Service**.

Object Settings >> SMS / Mail Service Object

SMS Provider	Mail Server		Set to Factory Default
Index		**Profile Name**	
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.
Index	Display the profile number that you can configure.
Profile	Display the name for such mail server profile.

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

1. Click the **Mail Server** tab, and click the number (e.g., #1) under Index column for configuration in details.

Object Settings >> SMS / Mail Service Object

SMS Provider	Mail Server
Index	
1.	
2.	
3.	
4.	

2. The configuration page will be shown as follows:

Objects Setting >> SMS / Mail Service Object

Profile Index: 1

Profile Name	Mail_Notify
SMTP Server	192.168.1.98
SMTP Port	25
Sender Address	carrie_@draytek.com
☐ Use SSL	
☐ **Authentication**	
Username	Max: 31 characters
Password	Max: 31 characters
Sending Interval	0 (seconds)

Note:
1. Only one mail can be sent during the "Sending Interval" time.
2. If the "Sending Interval" was set to 0, there will be no limitation.

[OK]   [Clear]   [Cancel]

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such mail service profile. The maximum length of the name you can set is 31 characters.
SMTP Server	Type the IP address of the mail server.
SMTP Port	Type the port number for SMTP server.
Sender Address	Type the e-mail address of the sender.
Use SSL	Check this box to use port 465 for SMTP server for some e-mail server uses https as the transmission method.
Authentication	The mail server must be authenticated with the correct username and password to have the right of sending message out. Check the box to enable the function. **Username** – Type a name for authentication. The maximum length of the name you can set is 31 characters. **Password** – Type a password for authentication. The maximum length of the password you can set is 31 characters.
Sending Interval	Define the interval for the system to send the SMS out.

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

Object Settings >> SMS / Mail Service Object

SMS Provider	Mail Server		Set to Factory Default
Index		**Profile Name**	
1.		Mail_Notify	
2.			
3.			

VI-1-11 Notification Object

This page allows you to set ten profiles which will be applied in **Application>>SMS/Mail Alert Service**.

You can set an object with different monitoring situation.

Object Settings >> Notification Object

			Set to Factory Default
Index	**Profile Name**	**Settings**	
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			

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

1. Open **Object Setting>>Notification Object**, and click the number (e.g., #1) under Index column for configuration in details.

Object Settings >> Notification Object

Index	**Profile Name**
1.	
2.	
3.	
4.	
5.	

2. The configuration page will be shown as follows:

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such notification profile. The maximum length of the name you can set is 15 characters.
Category	Display the types that will be monitored.
Status	Display the status for the category. You can check the box you want to be monitored. For example, the check box of **CPE firmware Upgrade Fail** under the category of **Central VPN Management** is checked. Once such profile is enabled, Vigor router system will send out notification to the recipient via SMS.

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

VI-1-12 String Object

This page allows you to set string profiles which will be applied in route policy (domain name selection for destination), hotspot web portal and etc.

Available settings are explained as follows:

Item	Description
Add	Click it to open the following page for adding a new string object.
Set to Factory Default	Click it to clear all of the settings in this page.
Index	Display the number link of the string profile.
String	Display the string defined.
Clear	Choose the string that you want to remove. Then click this check box to delete the selected string.
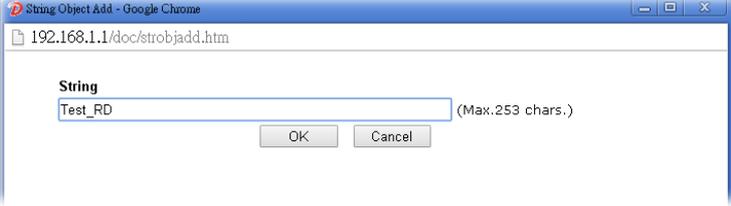
Below shows an example to apply string object (in Route Policy):

VI-1-13 Country Object

The country object profile can determine which country/countries shall be blocked by the Vigor router's Firewall.

Objects Setting >> Country Object

Country Object Table: | **Set to Factory Default** |

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

The country object, by grouping IP addresses for multiple countries, can be applied by other functions such as router policy destination (refer to the following figure for example).

Load-Balance/Route Policy

Index: 1

☐ Enable

Comment	[ ]	Delete

Criteria

Protocol	Any ▾
Source	Any ▾
Destination	Country Object ▾
	1-UK_US ▾
Destination Port	Any ▾

Send via if Criteria Matched

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

1. Open **Object Setting**>>**Country Object**, and click the number (e.g., #1) under Index column for configuration in details.

2. The configuration page will be shown as follows:

Objects Setting >> Country Object

Profile Index : 1

Name: [   ]

Available Country   **Selected Country**

| 220-Taiwan |
| 221-Tajikistan |
| 222-Tanzania, United Republic of |
| 223-Thailand |
| 224-Timor-Leste |
| 225-Togo |
| 226-Tokelau |
| 227-Tonga |
| 228-Trinidad and Tobago |

`>>` `<<`

Note:
The maximum number of Selected Country is 16.

OK   Clear   Cancel

Available settings are explained as follows:

Item	Description
Name	Type a name for such profile. The maximum length of the name you can set is 15 characters.
Available Country / Selected Country	Select any country from Available Country. Click >> to move the selected country and place on Selected Country. Check the box(es) for the country/countries to be blocked by Firewall. Note that one country profile can contain 1 up to 16 countries.

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

Objects Setting >> Country Object

Country Object Table: | **Set to Factory Default** |

Index	Name	Index	Name
1.	Taiwan	**17.**	
2.		**18.**	
3.		**19.**	
4.		**20.**	
5.		**21.**	
6.		**22.**	
7.		**23.**	
8.		**24.**	

Application Notes

A-1 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection

Follow the steps listed below:

1. Log into the web user interface of Vigor router.

2. Configure relational objects first. Open **Object Settings**>>**SMS/Mail Server Object** to get the following page.

Objects Setting >> SMS / Mail Service Object

SMS Provider	Mail Server		Set to Factory Default	
Index	**Profile Name**	**SMS Provider**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.	Custom 1	
10.	Custom 2	

Index 1 to Index 8 allows you to choose the built-in SMS service provider. If the SMS service provider is not on the list, you can configure Index 9 and Index 10 to add the new service provider to Vigor router.

3. Choose any index number (e.g., Index 1 in this case) to configure the SMS Provider setting. In the following page, type the username and password and set the quota that the router can send the message out.

Objects Setting >> SMS / Mail Service Object

Profile Index: 1

Profile Name	Local number
Service Provider	kotsms.com.tw (TW)
Username	abc5026
Password	••••••••••
Quota	10
Sending Interval	3 (seconds)

Note:
1. Only one message can be sent during the "Sending Interval" time.
2. If the "Sending Interval" was set to 0, there will be no limitation.

[OK] [Clear] [Cancel]

4. After finished the settings, click **OK** to return to previous page. Now you have finished the configuration of the SMS Provider profile setting.

Objects Setting >> SMS / Mail Service Object

SMS Provider	Mail Server		Set to Factory Default
Index	**Profile Name**	**SMS Provider**
1.	Local number	kotsms.com.tw (TW)
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.	Custom 1	
10.	Custom 2	

5. Open **Object Settings>>Notification Object** to configure the event conditions of the notification.

Object Settings >> Notification Object

		Set to Factory Default
Index	**Profile Name**	**Settings**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		

6. Choose any index number (e.g., Index 1 in this case) to configure conditions for sending the SMS. In the following page, type the name of the profile and check the Disconnected and Reconnected boxes for WAN to work in concert with the topic of this paper.

Objects Setting >> Notification Object

Profile Index: 1

Profile Name	WAN_Notify

Category	Status
WAN	☑ Disconnected ☑ Reconnected
VPN Tunnel	☐ Disconnected ☐ Reconnected
High Availability	☐ Failover Occurred Config Sync Fail Router Unstable

[OK]   [Clear]   [Cancel]

Note:
When High Availability is enabled, "Sending Interval" of **SMS Provider profile** should set to 0.

7. After finished the settings, click **OK** to return to previous page. You have finished the configuration of the notification object profile setting.

Object Settings >> Notification Object

| Set to Factory Default |

Index	Profile Name	Settings
1.	WAN_Notify	WAN
2.		
3.		
4.		
5.		
6.		
7.		
8.		

8. Now, open **Application >> SMS / Mail Alert Service**. Use the drop down list to choose SMS Provider and the Notify Profile (specify the time of sending SMS). Then, type the phone number in the field of Recipient (the one who will receive the SMS).

Applications >> SMS / Mail Alert Service

SMS Alert		Mail Alert			Set to Factory Default

Index	Enable	SMS Provider	Recipient Number	Notify Profile	Schedule(1-15)	
1	☑	9 - Custom 1	0910222366	1 - WAN_Notify		
2	☐	1 - Local number		1 - WAN_Notify		
3	☐	1 - Local number		1 - WAN_Notify		
4	☐	1 - Local number		1 - WAN_Notify		
5	☐	1 - Local number		1 - WAN_Notify		
6	☐	1 - Local number		1 - WAN_Notify		
7	☐	1 - Local number		1 - WAN_Notify		
8	☐	1 - Local number		1 - WAN_Notify		
9	☐	1 - Local number		1 - WAN_Notify		
10	☐	1 - Local number		1 - WAN_Notify		

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

[OK]   [Cancel]

9. Click **OK** to save the settings. Later, if one of the WAN connections fails in your router, the system will send out SMS to the phone number specified. If the router has only one WAN interface, the system will send out SMS to the phone number while reconnecting the WAN interface successfully.

Remark: How the customize the SMS Provider

Choose one of the Index numbers (9 or 10) allowing you to customize the SMS Provider. In the web page, type the URL string of the SMS provider and type the username and password. After clicking OK, the new added SMS provider will be added and will be available for you to specify for sending SMS out.

Objects Setting >> SMS / Mail Service Object

Profile Index: 9

Profile Name	Custom 1
Service Provider	clickatell

Please contact with your SMS provide to get the exact URL String
eg:bulksms.vsms.net:5567/eapi/submission/send_sms/2/2.0?username=###txtUser###
&password=###txtPwd###&msisdn=###txtDest###&message=###txtMsg###

Username	ilan123
Password	••••••••
Quota	10
Sending Interval	3 (seconds)

Note:
1. Only one message can be sent during the "Sending Interval" time.
2. If the "Sending Interval" was set to 0, there will be no limitation.

[OK] [Clear] [Cancel]

This page is left blank.

Part VII Troubleshooting

Troubleshooting

This part will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration.

VII-1 Diagnostics

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

- Checking if the hardware status is OK or not.

- Checking if the network connection settings on your computer are OK or not.

- Pinging the router from your computer.

- Checking if the ISP settings are OK or not.

- Backing to factory default setting if necessary.

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

Web User Interface

Fisrt, take a look at the menu items under Diagnostics. Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router.
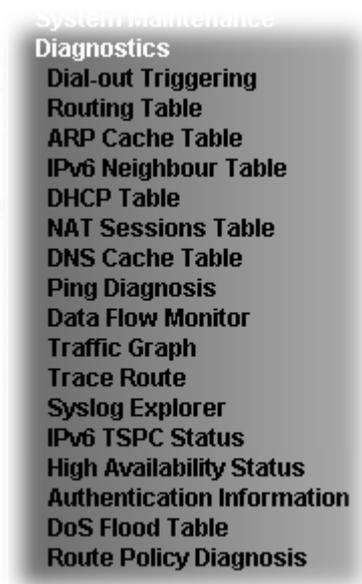
VII-1-1 Dial-out Triggering

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

Available settings are explained as follows:

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

VII-1-2 Routing Table

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

Diagnostics >> View Routing Table

IPv4

| Refresh |

```
Key          Destination              Gateway         Interface
-------------------------------------------------------------------
S~      192.168.10.0/ 255.255.255.0   via 192.168.1.2      LAN1
C~       192.168.1.0/ 255.255.255.0   directly connected   LAN1
S~      211.100.88.0/ 255.255.255.0   via 192.168.1.3      LAN1
```

Key
C: Connected   S: Static   R: RIP   *: default   ~: private   B: BGP   O: OSPF

Note:
1. IPv4 Routing Table Limit 511 entries.
2. If you want to show all entries, please use telnet "ip route status" command.

IPv6

| Refresh |

```
Destination                    Interface Flags   Metric   Next Hop
-------------------------------------------------------------------
FE80::/64                      LAN1       U        256      ::
FE80::/64                      LAN2       U        256      ::
FE80::/64                      LAN3       U        256      ::
FE80::/64                      LAN4       U        256      ::
FE80::/64                      LAN5       U        256      ::
FE80::/64                      LAN6       U        256      ::
FE80::/64                      LAN7       U        256      ::
FE80::/64                      LAN8       U        256      ::
FE80::/64                      LAN9       U        256      ::
FE80::/64                      LAN10      U        256      ::
FE80::/64                      LAN11      U        256      ::
FE80::/64                      LAN12      U        256      ::
FE80::/64                      LAN13      U        256      ::
FE80::/64                      LAN14      U        256      ::
```

☐ Show Detail

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

VII-1-3 ARP Cache Table

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

```
Diagnostics >> View ARP Cache Table

                    LAN                    WAN
Show: ALL LANs    ▼  and  ALL VLANs ▼
Ethernet ARP Cache Table                                              | Clear | Refresh |
IP Address        MAC Address       HOST ID              Interface  VLAN  Port
--------------------------------------------------------------------------------------------
192.168.1.10      60-A4-4C-E6-5A-4F                      LAN1       ---   P9




                                                                      ☐ Show Comment
```

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

VII-1-4 IPv6 Neighbour Table

The table shows a mapping between an Ethernet hardware address (MAC Address) and an IPv6 address. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **IPv6 Neighbour Table** to open the web page.

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

VII-1-5 DHCP Table

The facility provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

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

Diagnostics >> View DHCP Assigned IP Addresses

```
Show : ALL LANs            ▼

  DHCP IP Assignment Table      Other IP Assignment Table                   | Refresh |

Index   IP Address     MAC Address          Leased Time      HOST ID
-------------------------------------------------------------------------------
LAN1       : DHCP Server On    IP Pool: 192.168.1.10 ~ 192.168.1.209
-------------------------------------------------------------------------------
Index   IP Address     MAC Address          Leased Time      HOST ID
-------------------------------------------------------------------------------
LAN1
1       192.168.1.10    60-A4-4C-E6-5A-4F       FIXED IP




                                                              ☐ Show Comment

DHCPv6 IP Assignment Table                                        | Refresh |
Index   IPv6 Address                   IAID      Link-layer Address  Leased Time
-------------------------------------------------------------------------------
```

Available settings are explained as follows:

Item	Description
Index	It displays the connection item number.
IP Address	It displays the IP address assigned by this router for specified PC.
MAC Address	It displays the MAC address for the specified PC that DHCP assigned IP address for it.
Leased Time	It displays the leased time of the specified PC.
HOST ID	It displays the host ID name of the specified PC.
Refresh	Click it to reload the page.

VII-1-6 NAT Sessions Table

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

Diagnostics >> NAT Sessions Table

NAT Active Sessions Table (Limit: 128 entries) | Refresh |

```
-----------------------------------------------------------------------
    Private IP :Port #Pseudo Port        Peer IP :Port  Interface
-----------------------------------------------------------------------
```

Available settings are explained as follows:

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

VII-1-7 DNS Cache Table

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

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

Diagnostics >> DNS Cache Table

IPv4 DNS Cache Table

| Clear | Refresh |

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

IPv6 DNS Cache Table

| Clear | Refresh |

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

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

☐ When an entry's TTL is larger than ⬚ 0 s, this entry will be deleted from the table.

[OK]

Available settings are explained as follows:

Item	Description
Clear	Click 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.

VII-1-8 Ping Diagnosis

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

or

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 **Auto** to be determined by the router automatically.
Ping to	Use the drop down list to choose the destination that you

	want to ping.
IP Address	Type the IP address of the Host/IP that you want to ping.
Ping IPv6 Address	Type the IPv6 address that you want to ping.
Run	Click this button to start the ping work. The result will be displayed on the screen.
Clear	Click this link to remove the result on the window.

VII-1-9 Data Flow Monitor

This page displays the running procedure for the IP address monitored and refreshes the data in an interval of several seconds. The IP address listed here is configured in Bandwidth Management. You have to enable IP bandwidth limit and IP session limit before invoking Data Flow Monitor. If not, a notification dialog box will appear to remind you enabling it.

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 for five minutes. The remaining time will be shown on the session column. Click it to cancel the IP address blocking.
Current /Peak/Speed	**Current** means current transmission rate and receiving rate for WAN interface. **Peak** means the highest peak value detected by the router in data transmission. **Speed** means line speed specified in **WAN>>General Setup**. If you do not specify any rate at that page, here will display **Auto** for instead.

VII-1-10 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to open the web page. Choose WAN1/WAN3/WAN5/WAN6/WAN7/WAN8 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. Click **Reset** to zero the accumulated RX/TX (received and transmitted) data of WAN. Click **Refresh** to renew the graph at any time.
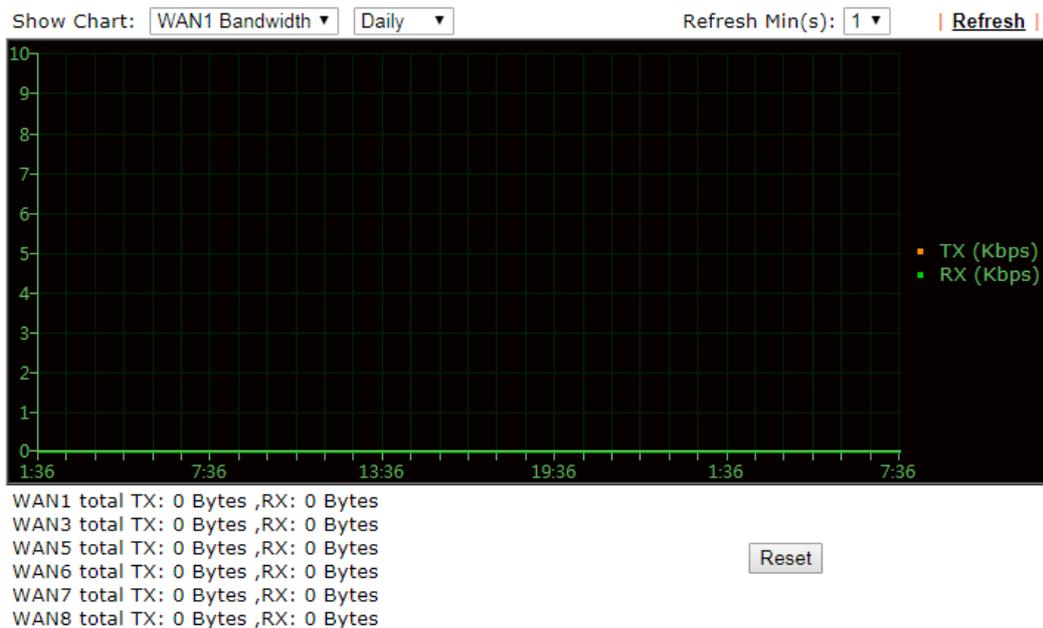
The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1/WAN3/WAN5/WAN6/WAN7/WAN8 Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

For Sessions chart, the numbers displayed on vertical axis represent the numbers of the NAT sessions during the past.

VII-1-11 Trace Route

Click **Diagnostics** and click **Trace Route** to open the web page. This page allows you to trace the routes from router to the host. Simply type the IP address of the host in the box and click **Run**. The result of route trace will be shown on the screen.

or

Available settings are explained as follows:

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

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

VII-1-13 Syslog Explorer

Such page provides real-time syslog and displays the information on the screen.

For Web Syslog

This page displays the time and message for User/Firewall/call/WAN/VPN settings. You can check **Enable Web Syslog,** specify the type of Syslog and choose the display mode you want. Later, the event of Syslog with specified type will be shown for your reference.

Diagnostics >> Syslog Explorer

Web Syslog			
☐ Enable Web Syslog		Export | Refresh | Clear |	
	Syslog Type [User ▾]	Display Mode [Stop record when fulls ▾]	
Time		**Message**	

Available settings are explained as follows:

Item	Description
Enable Web Syslog	Check this box to enable the function of Web Syslog.
Syslog Type	Use the drop down list to specify a type of Syslog to be displayed.
Export	Click this link to save the data as a file.
Refresh	Click this link to refresh this page manually.
Clear	Click this link to clear information on this page.
Display Mode	There are two modes for you to choose. [Stop record when fulls ▾] Stop record when fulls Always record the new event **Stop record when fulls –** when the capacity of syslog is full, the system will stop recording. **Always record the new event –** only the newest events will be recorded by the system.
Time	Display the time of the event occurred.
Message	Display the information for each event.

VII-1-14 IPv6 TSPC Status

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

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

Diagnostics >> IPv6 TSPC Status

| WAN1 WAN3 WAN5 WAN6 WAN7 WAN8 | | Refresh | |

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

Available settings are explained as follows:

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

VII-1-15 High Availability Status

All of the routers under the same DARP (DrayTek Address Resolution Protocol) group can be viewed in such page. However, only partial information of the router status will be displayed.

Vigor routers with the following condtions will be treated as the same DARP group:

- HA enabled
- the same Redundancy method
- the same Group ID
- the same Authentication Key
- the same Management Interface

Open **Diagnostics>>High Availablity Status**.

Diagnostics >> High Availability Status

| Details | HA Setup | Renew | Refresh |

Status	Router Name	IP	Role	Stable	WAN	Sync Status	Cached Time
!	DrayTek	192.168.1.1	Primary	No	All WANs Down - Eth	Ready Sync	-

Note:
1. High Availability Status table displays 10 routers maximum. The local router will always show in the first row of this table.
2. A Status of "!" indicates that an error has occurred, refer to the Details page for more information.

Available settings are explained as follows:

Item	Description
Details/Back	**Details** – Click it to display detailed status about HA configuration for the selected router. **Back** – Return to previous page.
HA Setup	Click it to open **Applications>>High Availability** for modifying the configuration.
Renew	Click it to get the newest status of other router (except the primary router).
Refresh	Click it to get the newest status of the primary router.
Status	"**!**" means an error has occurred. Refer to **Detailed** information and modify HA settings if required.
Router Name	Display the name of the device.
IP	Display the IPv4 address of such router.
Role	"Down" means the function of HA is disabled. "Primary" means such router stands for the primary router in HA. "Secondary" means such router stands for the secondary router in HA.
Stable	"No" means the primary router has not been determined yet. DARP is negotiating. "YES" means the primary router is determined.
WAN	"At Least One UP" means that at least one WAN interface connects to Internet.

	"All WANs Down" means that no WAN interface connects to Internet.
Sync Status	"Not Ready" means configuration synchronization is unable to execute, or configuration synchronization is disabled, or synchronization initialization executes but fails.
	"Ready" means configuration synchronization is ready to execute.
	"Progressing" means configuration synchronization is operating.
	"Fail" means configuration synchronization executed and failed; or wrong model name.
	"Equal" means the corresponding settings are equal to the primary router.
Cached Time	Display the time period since the last time to get the newest status of other router (except the primary router).

Cick the link of **Status**, **Router Name**, **IPv4** or **Details**, the following page will be displayed on the screen.

Diagnostics >> High Availability Status >> Details

[Local Router] | Back | HA Setup | Renew | Refresh |

DrayTek			192.168.1.1(FE80::21D:AAFF:FE21:2858)		
Role	**Stable**	**WAN**	**Sync Status**	**Cached Time**	
Primary	No !	All WANs Down - Eth !	Ready Sync	-	

Config Sync Status	Not Ready	**DHCPv6 Sync Status**	Ready	
MAC	00:1d:aa:21:28:58	**HTTPs Port**	443	
Model	Vigor3910	**Firmware Version**	3.9.1.2_RC4 r1189_86289	
Enable High Availability	Off !	**Redundancy Method**	Active-Standby	
Group ID	1	**Priority ID**	10	
Authentication Key	draytek	**Management Interface**	LAN1	
Update DDNS	Off	**Protocol**	IPv4	
Virtual IPv4	Off !			
		LAN1	FE80::200:5EFF:FE00:101	
		LAN2	FE80::200:5EFF:FE00:101	
		LAN3	FE80::200:5EFF:FE00:101	
		LAN4	FE80::200:5EFF:FE00:101	
		LAN5	FE80::200:5EFF:FE00:101	
		LAN6	FE80::200:5EFF:FE00:101	
		LAN7	FE80::200:5EFF:FE00:101	
		LAN8	FE80::200:5EFF:FE00:101	
		LAN9	FE80::200:5EFF:FE00:101	
		LAN10	FE80::200:5EFF:FE00:101	
		LAN11	FE80::200:5EFF:FE00:101	
		LAN12	FE80::200:5EFF:FE00:101	

VII-1-16 Authentication Information

Authentication User List

Such page displays authentication jobs made by Internal RADIUS or Local 802.1X.

When the mouse cursor moves to the name link under User Name, the connection message (including authentication failed information) about internal RADIUS or local 802.1X service will be shown by a popped up dialog box.

Diagnostics >> Authentication Information

Authentication User List		Authentication Information Log	
			| Refresh | Clear |
User Name	**Authentication Failure Times**	**User Name**	**Authentication Failure Times**
test_1	0	test_sales	0

Note:
1. This is the authentication list for router's **Internal RADIUS** or Local 802.1X
2. For those clients are authenticated by external RADIUS server, please find the information from the server.

Authentication Information Log

This page will display the complete authentication log information.

Diagnostics >> Authentication Information

Authentication User List	Authentication Information Log

☐ Enable   \| Refresh \| Clear \|

Syslog Type [Radius ▾] Display Mode [always record the new event ▾]

Radius
802.1X
ALL

Time	**Message**

Available settings are explained as follows:

Item	Description
Enable	Check the box to enable such function.
Refresh	Click it to update current page.
Clear	Click it to remove all of the records.
Syslog Type	Specify RADIUS, 802.1X or All to display related authentication information log.
Display Mode	Choose the mode you want to display the related information on the following table. ● **Stop record when fulls** – when the capacity of CVM log is full, the system will stop recording. ● **Always record the new event** – only the newest events will be recorded by the system.
Time	Display the time the user authenticated by Vigor3910 series.
Message	Display authentication information done by Vigor3910 series.

VII-1-17 DoS Flood Table

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

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

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

Diagnostics >> DoS Flood Table

IPv4

| SYN Flood | UDP Flood | ICMP Flood | | Refresh | |

Tracing IP   Destination Port

IPv6

| SYN Flood | UDP Flood | ICMP Flood | | Refresh | |

Tracing IP   Destination Port

Note:
You need to enable SYN/UDP/ICMP flood defense in **Firewall >> Defense Setup** to make this table effective.

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

VII-1-18 Route Policy Diagnosis

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

Diagnostics >> Route Policy Diagnosis

Test how the packets will be routed

Mode ⦿ Analyze a single packet
      ○ Analyze multiple packets by uploading an input file

Packet Information
    Protocol ICMP ▾
    Src IP   Specify an IP ▾   192.168.1.2
    Dst IP   Specify an IP ▾
    Dst Port Any Port ▾

                                    Analyze

or

Diagnostics >> Route Policy Diagnosis

Test how the packets will be routed

Mode ○ Analyze a single packet
      ⦿ Analyze multiple packets by uploading an input file

Input File
    選擇檔案 未選擇任何檔案   (download an example input file)
                                    Analyze

Available settings are explained as follows:

Item	Description
Mode	**Analyze a single packet** - Choose such mode to make Vigor router analyze how a single packet will be sent by a route policy. **Analyze multiple packets**... - Choose such mode to make Vigor router analyze how multiple packets in a specified file will be sent by a route policy.
Packet Information	Specify the nature of the packets to be analyzed by Vigor router. **ICMP/UDP/TCP/ANY-** Specify a protocol for diagnosis. **Src IP** – Type an IP address as the source IP. **Dst IP** – Type an IP address as the destination IP. **Dst Port** – Use the drop down list to specify the destination port. **Analyze** – Click it to perform the job of analyzing. The analyzed result will be shown on the page..

Input File	It is available when Analyze multiple packets.. is selected as **Mode.**
	Select – Click the download link to get a blank example file. Then, click such button to select that blank ".csv" file for saving the result of analysis.
	Analyze – Click it to perform the job of analyzing. The analyzed result will be shown on the page. If required, click **export analysis** to export the result as a file.
	Note that the analysis was based on the current "load-balance/route policy" settings, we do not guarantee it will be 100% the same as the real case.

VII-2 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

1. Check the power line and WLAN/LAN cable connections.
   Refer to "**I-2 Hardware Installation**" for details.

2. Turn on the router. Make sure the **ACT LED** blink once per second and the correspondent **LAN LED** is bright.
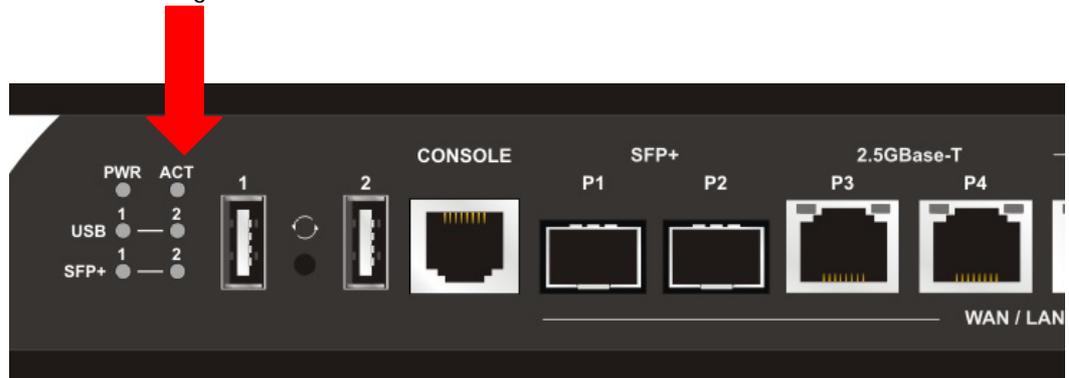
3. If not, it means that there is something wrong with the hardware status. Simply back to "**I-2 Hardware Installation**" to execute the hardware installation again. And then, try again.

VII-3 Checking If the Network Connection Settings on Your Computer Is OK or Not

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

For Windows

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

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

2. In the following window, click **Change adapter settings**.
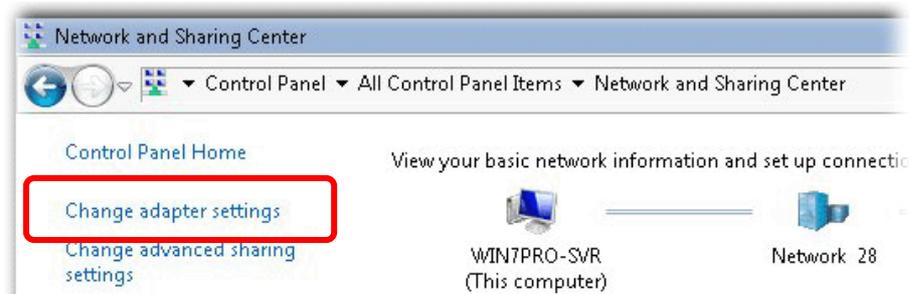
3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.
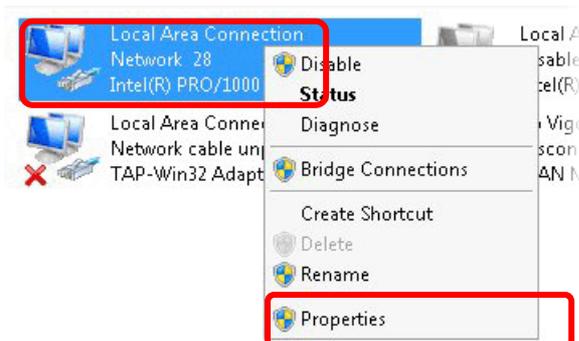
4.   Select **Internet Protocol Version 4 (TCP/IP)** and then click **Properties**.
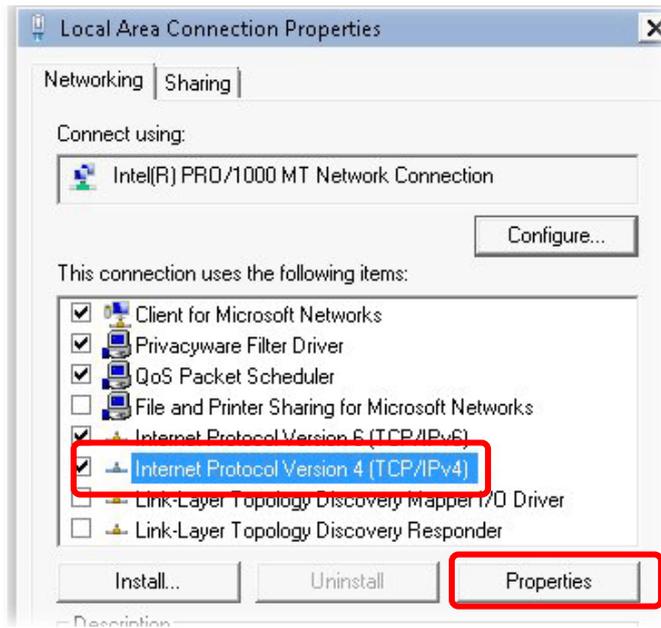
5.   Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.
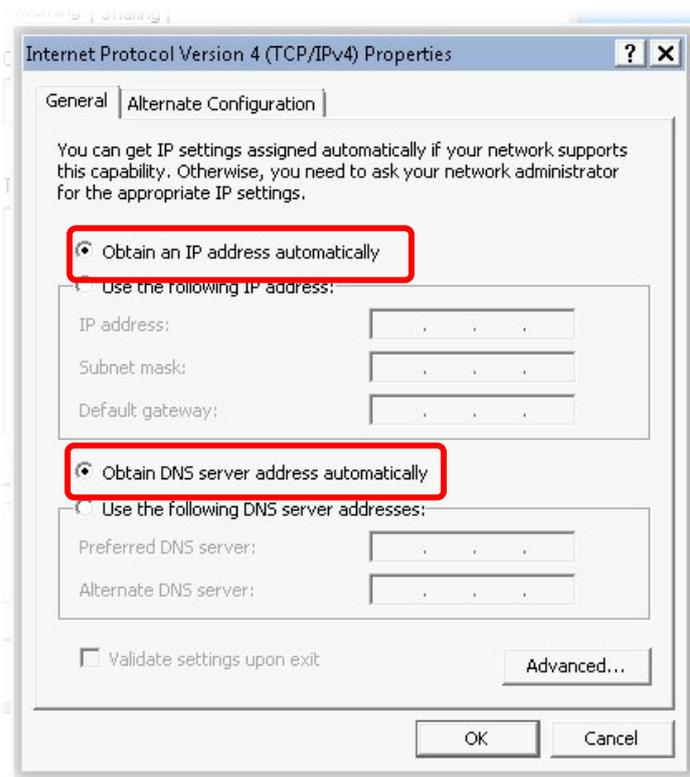
For Mac OS

1. Double click on the current used Mac OS on the desktop.
2. Open the **Application** folder and get into **Network**.
3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.
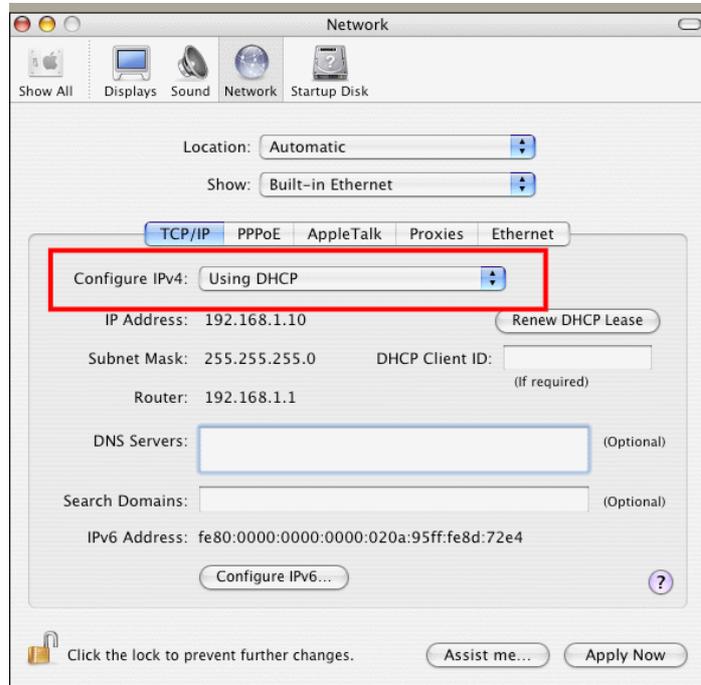
VII-4 Pinging the Router from Your Computer

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use "ping" command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1**. If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section VIII-3)

Please follow the steps below to ping the router correctly.

For Windows

1. Open the **Command** Prompt window (from **Start menu> Run**).

2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista/7/8). The DOS command dialog will appear.
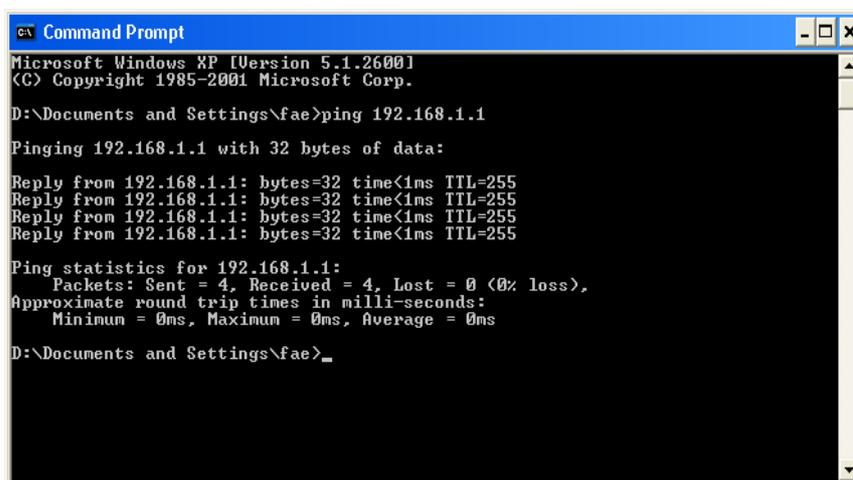
```
Command Prompt                                      _ □ ×
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

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

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

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

3. Type ping 192.168.1.1 and press [Enter]. If the link is OK, the line of "**Reply from 192.168.1.1:bytes=32 time<1ms TTL=255**" will appear.

4. If the line does not appear, please check the IP address setting of your computer.

For Mac OS (Terminal)

1. Double click on the current used MacOs on the desktop.

2. Open the **Application** folder and get into **Utilities**.

3. Double click **Terminal**. The Terminal window will appear.

4. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of "**64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**" will appear.

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

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

● Change the **Physical Type** from **Auto negotiation** to other values (e.g., 100M full duplex).

● Next, change the physical type of modem (e.g., DSL/FTTX(GPON)/Cable modem) offered by ISP with the same value configured in Vigor router. Check if the LEDs on Vigor router are on or not.

● If not, please install an additional switch for connecting both Vigor router and the modem offered by ISP. Then, check if the LEDs on Vigor router are on or not.

● If the problem of LEDs cannot be solved by the above measures, please contact with the nearest reseller, or send an e-mail to DrayTek FAE for technical support.

● Check if the settings offered by ISP are configured well or not.

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

● Open **WAN** >> **Internet Access** page and then check whether the ISP settings are set correctly. Click **Details Page** of WAN1~WAN8 to review the settings that you configured previously.

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode / Port	Access Mode		
WAN1		SFP+ / P1	Static or Dynamic IP ▼ None PPPoE Static or Dynamic IP	Details Page	IPv6
WAN3		Ethernet / P3		Details Page	IPv6
WAN5		Ethernet / P5	Static or Dynamic IP ▼	Details Page	IPv6
WAN6		Ethernet / P6	Static or Dynamic IP ▼	Details Page	IPv6
WAN7		Ethernet / P7	Static or Dynamic IP ▼	Details Page	IPv6
WAN8		Ethernet / P8	Static or Dynamic IP ▼	Details Page	IPv6

DHCP Client Option

VII-6 Backing to Factory Default Setting If Necessary

Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware. Such function is available in **Admin Mode** only.

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

Software Reset

You can reset the router to factory default via Web page. Such function is available in **Admin Mode** only.

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

System Maintenance >> Reboot System

Reboot System

Do you want to reboot your router ?

○ Using current configuration
○ Using factory default configuration

Reboot Now

Auto Reboot Time Schedule

Schedule Profile : None ▼ , None ▼ , None ▼ , None ▼

Note: Action and Idle Timeout settings will be ignored.

OK   Cancel

Hardware Reset

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

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

VII-7 Contacting DrayTek

If the router still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@DrayTek.com.

.

Vigor3910 Series User's Guide

Part VIII DrayTek Tools

VIII-1 SmartVPN Client

VIII-1-1 DrayTek Android-based SmartVPN APP for the establishment of SSL VPN connection

DrayTek has been the world-leading company to integrate VPN with Vigor SOHO routers to serve professionals and business customers with secure data transactions over Internet. The facilities of VPN let businesses are able to receive and send data over Internet with secure tunnels. We provide multiple protocol VPN connections such as IPSec/PPTP/L2TP protocols for secure data exchange and communication. With SSL VPN embedded on Vigor routers, teleworkers can have convenient and simple access to central site VPN. The teleworkers do not need to install any VPN software manually. From regular web browser, you can establish VPN connection back to your main office even in a guest network or web cafe.

DrayTek provided free SmartVPN for Windows-based users to easily establish VPN tunnels. There were million downloads. Now, DrayTek released Android-based SmartVPN app for those who would like to set up SSL VPN connection with the VPN server working at the main office. The SmartVPN app is available for your free download! Then, you can use the SmartVPN App on smartphone/tablet PC to establish SSL VPN tunnels with your main office.

VIII-1-2 How to Use SmartVPN Android APP to Establish SSL VPN Tunnel?

SmartVPN APP for Android is now available on Google play. This document demonstrates how to use the APP to establish a SSL VPN tunnel.

1. On VPN server, create a SSL user account. Please refer to "How to Set up SSL VPN" on www.draytek.com for detailed instructions.

2. Download the APP from Google play, and run the APP.

3. Click "+" to add a new profile.
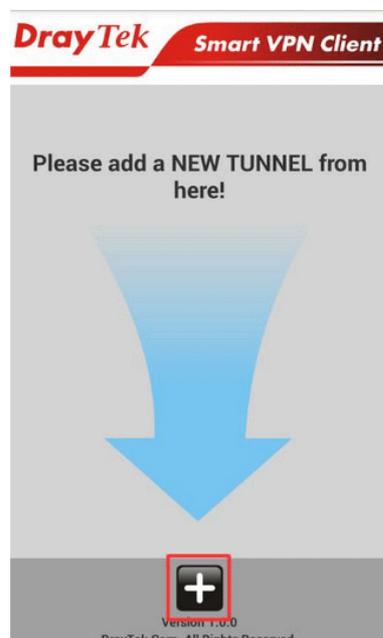
4. Edit the profile.

    a. Enter description of this profile.

    b. Enter VPN Server's IP in Server.

    c. Enter Port as the port which VPN server uses for SSL VPN; for Vigor Routers, it is 443 by default.

    d. Tap SAVE to save the profile or "<" to cancel.

Info	Installation of relevant Root CA is required to enable server certificate authentication.
	If you check "Use default gateway on remote network", all the traffic of this smart device will be forwarded to the remote gateway.

5. Tap the profile bar to establish SSL VPN tunnel.
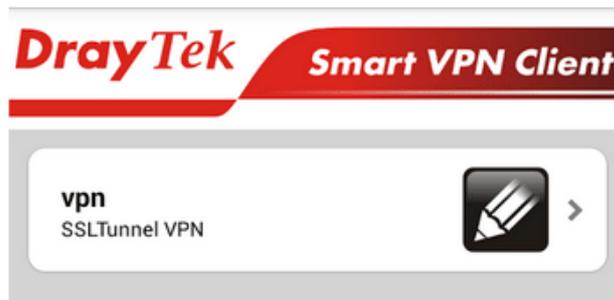
6. Enter Username and Password, then tap Dial.

7. When the tunnel is up, the profile will turn green. Tap the bar again will disconnect the tunnel.

8. Tap the pencil icon to edit or remove the profile.

This page is left blank.

Part IX Telnet Commands

Accessing Telnet of Vigor3910

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

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

Type **cmd** and press Enter. The Telnet terminal will be open later.
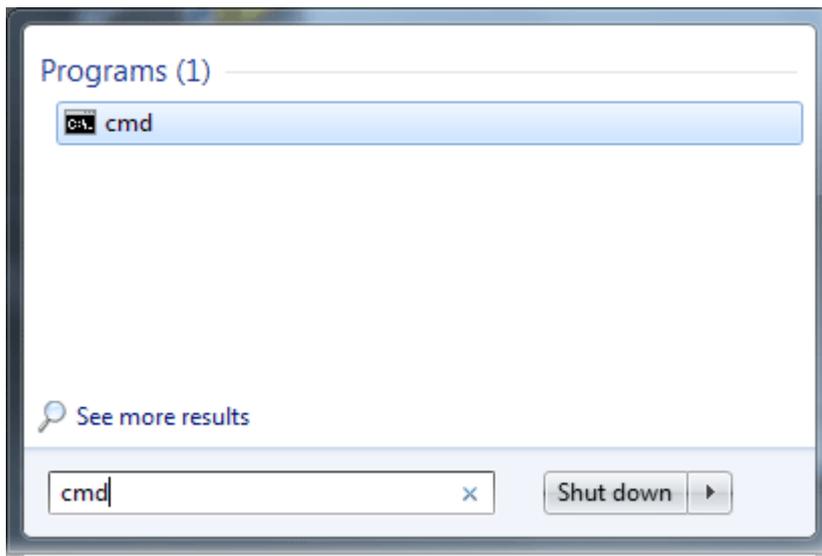
In the following window, type **Telnet 192.168.1.1** as below and press Enter. Note that the IP address in the example is the default address of the router. If you have changed the default, enter the current IP address of the router.
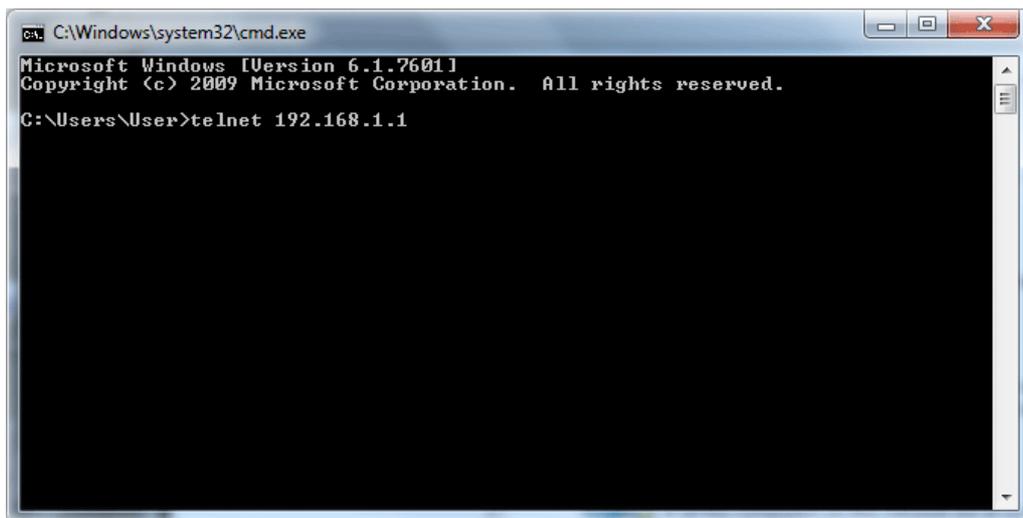
Next, type admin/admin for Account/Password. Then, type **?**. You will see a list of valid/common commands depending on the router that your use.
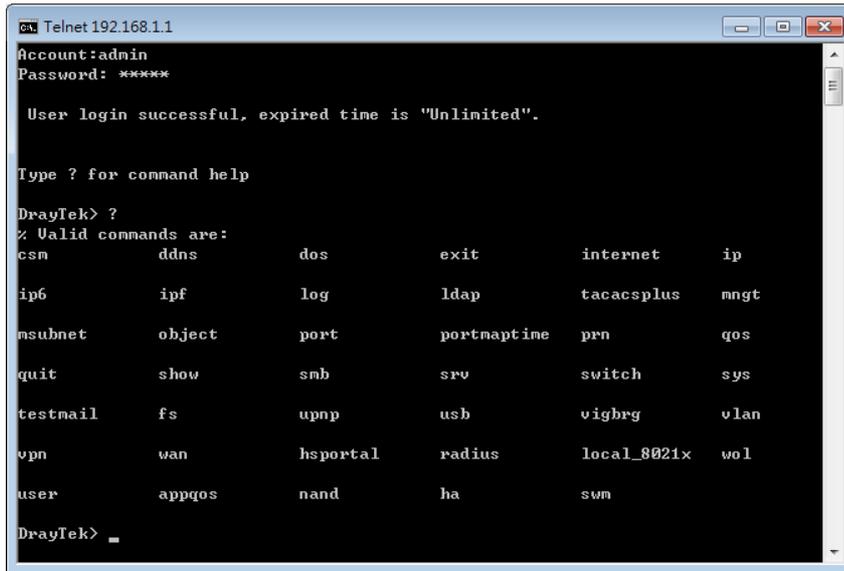
For users using previous Windows system (e.g., 2000/XP), simply click **Start** >> **Run** and type **Telnet 192.168.1.1** in the Open box as below. Next, type admin/admin for Account/Password. And, type **?** to get a list of valid/common commands.
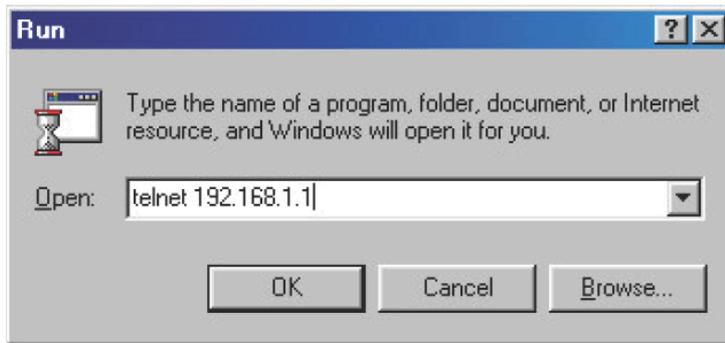
Telnet Command: csm appe prof

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

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

Syntax

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

Syntax Description

Parameter	Description
INDEX	Specify the index number of CSM profile, from 1 to 32.
- v	View the configuration of the CSM profile.
- n	Set a name for the CSM profile.
NAME	Specify a name for the CSM profile, less then 15 characters.
setdefault	Reset to default settings.

Example

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

Telnet Command: csm appe set

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

Syntax

csm appe set *-i INDEX [-v GROUP| -e AP_IDX | -d AP_IDX| -a AP_IDX [ACTION]]*

Syntax Description

Parameter	Description
INDEX	Specify the index number of CSM profile, from 1 to 32.
- v	View the IM/P2P/Protocol and Others configuration of the CSM profile.
-e	Enable to block specific application.
-d	Disable to block specific application.
-a	Set the action of specific application
GROUP	Specify the category of the application. Available options are: IM, P2P, Protocol and Others.
AP_IDX	Each application has independent index number for identification in CLI command.
	Specify the index number of the application here. If you have no idea of the inex number, do the following (Take IM as an example):
	Type "csm appe set –I 1 –v IM", the system will list all of the index numbers of the applications categorized under IM.
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 set –i 1 –a 1 1

Profile 1 - : <NULL> action set to Pass.

>
```

Telnet Command: csm appe show

It is used to display group (IM/P2P/Protocol and Others) information APP Enforcement Profile.

Syntax

csm appe show *[-a/-i/-p/-t/-m]*

Syntax Description

Parameter	Description
-a	View the configuration status for All groups.
-i	View the configuration status of IM group.
-p	View the configuration status of P2P group.
-t	View the configuration status of protocol group.
-m	View the configuration status of Others group.

Example

```
>csm appe show –t

       Type       Index                     Name       Version   Advance
 Advanced Option: (M)essage, (F)ile Transfer, (G)ame, (C)onference, and (O)ther
Activities
 ------------------------------------------------------------
     PROTOCOL     52                DB2
     PROTOCOL     53                DNS
     PROTOCOL     54                FTP
     PROTOCOL     55                HTTP           1.1
     PROTOCOL     56                IMAP           4.1
     PROTOCOL     57           IMAP STARTTLS          4.1
     PROTOCOL     58                IRC          2.4.0          …………
```

Telnet Command: csm appe config

It is used to display the configuration status (enabled or disabled) for IM/P2P/Protocol/Other applications.

Syntax

csm appe config -v *INDEX [-i/-p/-t/-m]*

Syntax Description

Parameter	Description
INDEX	Specify the index number of CSM profile, from 1 to 32.
-i	View the configuration status of IM group.
-p	View the configuration status of P2P group.

-t	View the configuration status of protocol group.
-m	View the configuration status of Others group.

Example

```
> csm appe config -v 1 -m

    Group         Type    Index              Name        Enable     A
vance Enable
 Advance abbreviation: Message, File Transfer, Game, Conference, and Other
 Advance abbreviation: : M, F, G, C, and O
------------------------------------------------------------------
   OTHERS        TUNNEL     75            DNSCrypt         Disable
   OTHERS        TUNNEL     76            DynaPass         Disable
   OTHERS        TUNNEL     77             FreeU           Disable
   OTHERS        TUNNEL     78           HTTP Proxy        Disable
   OTHERS        TUNNEL     79           HTTP Tunnel       Disable
   OTHERS        TUNNEL     80            Hamachi          Disable
   OTHERS        TUNNEL     81         Hotspot Shield       Disable
   OTHERS        TUNNEL     82           MS Teredo         Disable
   OTHERS        TUNNEL     83            PGPNet           Disable
   OTHERS        TUNNEL     84          Ping Tunnel         Disable
.
.
.
------------------------------------------------------------------

Total 66 APPs

>
```

Telnet Command: csm appe interface

It is used to configure APPE signature download interface.

Syntax

csm appe interface *[AUTO/WAN#]*

Syntax Description

Parameter	Description
AUTO	Vigor router specifies WAN interface automatically.
WAN	Specify the WAN interface for signature downloading.

Example

```
> csm appe interface wan1

Download interface is set as "WAN1" now.

> csm appe interface auto

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

Telnet Command: csm appe email

It is used to set notification e-mail for APPE signature based on the settings configured in **System Maintenance>>SysLog/Mail Alert Setup** (in which, the box of **APPE Signature** is checkd under **Enable E-Mail Alert**).

Syntax

csm appe email *[-e|-d|-s]*

Syntax Description

Parameter	Description
-e	Enable notification e-mail mechanism.
-d	Disable notification e-mail mechanism.
-s	Send an example e-mail.

Example

```
> csm appe email –e
Enable APPE email.
```

Telnet Command: csm ucf

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

Syntax

csm ucf show

csm ucf setdefault

csm ucf msg *MSG*

csm ucf obj *INDEX [-n PROFILE_NAME | -l [P|B|A|N] | uac | wf]*

csm ucf obj *INDEX -n PROFILE_NAME*

csm ucf obj *INDEX -p VALUE*

csm ucf obj *INDEX -l P|B|A|N*

csm ucf obj *INDEX uac*

csm ucf obj *INDEX wf*

Syntax Description

Parameter	Description
show	Display all of the profiles.
setdefault	Return to default settings for all of the profile.
msg MSG	Set the administration message. MSG means the content (less than 255 characters) of the message itself.
obj	Specify the object for the profile.
INDEX	Specify the index number of CSM profile, from 1 to 8.
-n	Set the profile name.
PROFILE_NAME	Specify the name of the profile (less than 16 characters)
-p	Set the priority (defined by the number specified in VALUE) for the profile.
VALUE	Number 0 to 3 represent different conditions. 0: It means Bundle: Pass. 1: It means Bundle: Block. 2: It means Either: URL Access Control First. 3: It means Either: Web Feature First.
-l	It means the log type of the profile. They are: P: Pass, B: Block, A: All,

	N: None
MSG	Specify the Administration Message, less then 255 characters
uac	Set URL Access Control part.
wf	Set Web Feature part.

Example

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

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


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

Telnet Command: csm ucf obj INDEX uac

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

Syntax

csm ucf obj *INDEX uac -v*

csm ucf obj *INDEX uac -e*

csm ucf obj *INDEX uac -d*

csm ucf obj *INDEX uac -a P|B*

csm ucf obj *INDEX uac -i E|D*

csm ucf obj *INDEX uac -o KEY_WORD_Object_Index*

csm ucf obj *INDEX uac -g KEY_WORD_Group_Index*

Syntax Description

Parameter	Description
INDEX	Specify the index number of CSM profile, from 1 to 8.
- v	View the protocol configuration of the CSM profile.
-e	Enable the function of URL Access Control.
-d	Disable the function of URL Access Control.
-a	Set the action of specific application, P or B.
	B: Block. The web access meets the URL Access Control will be blocked.
	P: Pass. The web access meets the URL Access Control will be passed.
-i	Prevent the web access from any IP address.
	E: Enable the function. The Internet access from any IP address will

	be blocked.
	D: Disable the function.
-o	Set the keyword object.
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.

Example

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

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

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

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

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

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

Telnet Command: csm ucf obj INDEX wf

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

Syntax

csm ucf obj *INDEX wf -v*

csm ucf obj *INDEX wf -e*

csm ucf obj *INDEX wf -d*

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

csm ucf obj *INDEX wf -s WEB_FEATURE*

csm ucf obj *INDEX wf -u WEB_FEATURE*

csm ucf obj *INDEX wf -f File_Extension_Object_index*

Syntax Description

Parameter	Description
INDEX	Specify the index number of CSM profile, from 1 to 8.
-v	View the protocol configuration of the CSM profile.
-e	Enable the restriction of web feature.
-d	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	Enable the the Web Feature configuration.
	Features available for configuration are:
	c: Cookie
	p: Proxy
	u: Upload
-u	Cancel the web feature configuration.
-f	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).

Syntax

csm wcf show

csm wcf look

csm wcf cache

csm wcf server *WCF_SERVER*

csm wcf msg *MSG*

csm wcf setdefault

csm wcf obj *INDEX -v*

csm wcf obj *INDEX -a P|B*

csm wcf obj *INDEX -n PROFILE_NAME*

csm wcf obj *INDEX -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	Display the web content filter profiles.
Look	Display the license information of WCF.
Cache	Set the cache level for the profile.
Server WCF_SERVER	Set web content filter server.
Msg MSG	Set the administration message. MSG means the content (less than 255 characters) of the message itself.
setdefault	Return to default settings for all of the profile.
obj	Specify the object profile.
INDEX	Specify the index number of web content filter profile, from 1 to 8.
- v	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	Set the profile name.
PROFILE_NAME	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	Set the action for the black and white list.
	E:Enable,
	D:Disable,
	P:Pass,
	B:Block
-s	It means to choose the items under CATEGORY or WEB_GROUP.
-u	It means to discard items under CATEGORY or WEB_GROUP.
WEB_GROUP	Child_Protection, Leisure, Business, Chating, Computer Internet, Other
CATEGORY	Includes:
	Alcohol & Tobacco, Criminal Activity, Gambling, Hate & Intoleranc, Illegal Drug, Nudity, Pornography/Sexually Explicit, Weapons, Violence, School Cheating,Sex Education, Tasteless, Child Abuse Imges, Entertainment, Games, Sports, Travel, Leisure & Recreation, Fashin & Beauty, Business, Job Search, Web-based Emai, Chat, Instant Messaging, Anonymizers, Forums & Newsgroups, Computers & Technology, Download Sites, Streaming Media & Downloads, Phishing & Fraud, Search Engines & Portals, Social Networking, Spam Sites,Malware, Botnets, Hacking, Illegal Software, Information Security,Peer-to-eer, Advertisements & Pop-Ups, Arts, Transportation, Compromised, Dating & Personals, , Education, Finance, Government,Health & Medcine, News, Non-profits & NGOs, Personal Sites,Politics, Real Estate, Rligion, Restaurants & Dining,Shopping, Translators, General, Cults,Greetig cards, Image Sharing, Network Errors, Parked Domains, Private IP Addresses)

Example

```
> csm wcf obj 1 -n test_wcf
Profile Index: 1
Profile Name:[test_wcf]
[]White/Black list
Action:[block]
  No  Obj NO.   Object Name
  --- -------- -------------------------------
  No  Grp NO.   Group Name
  --- -------- -------------------------------
Action:[block]
 Log:[block]

-------------------------------------------------------------------
-------------
child Protection Group:
  [v]Alcohol & Tobacco     [v]Criminal & Activity  [v]Gambling
  [v]Hate & Intolerance    [v]Illegal Drug         [v]Nudity
  [v]Pornography & Sexually explicit  [v]Violence
[v]Weapons


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

Telnet Command: csm dnsf

It means to configure the settings regarding to DNS filter.

Syntax

csm dnsf enable *ON/OFF*

csm dnsf syslog *N/P/B/A*

csm dnsf service WCF_PROFILE

csm dnsf service_ucf UCF_PROFILE

csm dnsf time CACHE_TIME

csm dnsf blockpage *show/on/off*

csm dnsf profile_show

csm dnsf profile_edit *INDEX*

csm dnsf profile_edit *INDEX -n PROFILE_NAME*

csm dnsf profile_edit *INDEX -l N/P/B/A*

csm dnsf profile_edit *INDEX -w WCF_PROFILE*

csm dnsf profile_edit *INDEX -u UCF_PROFILE*

csm dnsf profile_edit *INDEX -c CACHE_TIME*

Syntax Description

Parameter	Description
enable	Enable or disable DNS Filter. ON: enable. OFF: disable.
syslog	Determine the content of records transmitting to Syslog. P: Pass. Records for the packets passing through DNS filter will be sent to Syslog. B: Block. Records for the packets blocked by DNS filter will be sent to Syslog. A: All. Records for the packets passing through or blocked by DNS filter will be sent to Syslog. N: None. No record will be sent to Syslog.
service WCF_PROFILE	WCF_PROFILE: Specify a WCF profile as the base of DNS filtering. Type a number to indicate the index number of WCF profile (1 is first profile, 2 is second profile, and so on …).
time CACHE_TIME	CACHE_TIME: It means to set the time for cache to live (available values are 1 to 24; 1 is one hour, 2 is two hours, and so on …) for DNS filter.
blockpage	DNS sends block page for redirect port. When a web page is blocked by DNS filter, the router system will send a message page to describe that the page is not allowed to be visisted. ON: Enable the function of displaying message page. OFF: Disable the function of displaying message page. SHOW: Display the function of displaying message page is ON or OFF.
profile_show	Display the table of the DNS filter profile.
profile_edit	Modify the content of the DNS filter profile.
-n PROFILE_NAME	PROFILE_NAME: Type the name of the DNS filter profile that you want to modify.
-l N|P|B|A	Specify the log type of the profile. P: Pass. B: Block. A: All. N: None.
-w WCF_PROFILE	WCF_PROFILE: Type the index number of the WCF profile.
-u UCF_PROFILE	UCF_PROFILE: Type the index number of the UCF profile.
-c CACHE_TIME	-c means to set the cache time for DNS filter. CACHE_TIME: It means to set the time for cache to live (available values are 1 to 24; 1 is one hour, 2 is two hours, and so on …) for DNS filter.

Example

```
> csm dnsf service 2
dns service set up!!!
>csm dnsf service 3
wcf profile 3 is empty.....
>csm dnsf cachetime 1
```

```
dns cache time set up!!!
```

Telnet Command: ddns enable

This command allows users to enable or disable the DDNS service.

Syntax

ddns enable *[0/1]*

Syntax Description

Parameter	Description
0/1	0 – Disable the DDNS service. 1 – Enable the DDNS service.

Example

```
> ddns enable 1
 Enable Dynamic DNS Setup
>
```

Telnet Command: ddns set

This command allows users to set Dynamica DNS account.

Syntax

ddns set *[option]*

ddns set *-i [account index] -S [service provider] -T [service type] -D [hostname] -L [username] -P [password]*

Syntax Description

Parameter	Description
-i [value]	It means index number of Dynamic DNS Account. value: 1-6
-E [value]	It means to enable /disable Dynamic DNS Account. value: 0: Disable, 1:Enable
-W [value]	It means to specify WAN Interface. [value]: Must be between 1-8 1: WAN1 First 2: WAN1 Only 3: WAN2 First 4: WAN2 Only example: To set WAN Interface: WAN1 First
-L [value]	It means to type Login Name. [value]: limit up to 64 characters
-P [value]	It means to type Password. [value]: limit up to 24 characters
-C [value]	It means to enable /disable Wildcards. [value]: 0: Disable, 1:Enable
-B [value]	It means to enable / disable Backup MX.

	[value]: 0: Disable, 1:Enable
-M [value]	It means to type Mail Extender.
	[value]: limit up to 60 characters
-R [value]	It means to type Determine Real WAN IP.
	[value]: 0: WAN IP, 1: Internet IP
-S [value]	It means to specify Servive Provider.
	If user want to set User-Defined page, value must select 1.
	[value]: value must be between 1-19.
	1 >> User-Defined
	2 >> 3322 DDNS (www.3322.org)
	3 >> ChangeIP.com (www.changeip.com)
	4 >> ddns.com.cn (www.ddns.com.cn)
	5 >> DtDNS (www.dtdns.com)
	6 >> dyn.com (www.dyn.com)
	7 >> DynAccess (www.dynaccess.com)
	8 >> dynami.co.za (www.dynami.co.za)
	9 >> freedns.afraid.org (freedns.afraid.org)
	10 >> NO-IP.COM Free (www.no-ip.com)
	11 >> opendns.com (www.opendns.com)
	12 >> OVH (www.ovh.com)
	13 >> Strato (www.strato.eu)
	14 >> TwoDNS (www.twodns.de)
	15 >> TZO (www.tzo.com)
	16 >> ubddns.org (ubddns.org)
	17 >> Viettel DDNS (vddns.vn)
	18 >> vigorddns.com (www.vigorddns.com)
	19 >> ZoneEdit DDNS (dynamic.zoneedit.com)
T [value]	It means to type Servive Type.
	[value]: value must be between 1-3.
	1: Dynamic 2: Custom 3: Static
-D <Host Name> <sub Domain Name>	It means to type Domain Name.
	i.e: Account index 1 setting Domain Name for Dynamic Service Type
	>> ddns set -i 1 -T 1 -D "host ddns.com.cn"
	i.e: Account index 2 setting Domain Name for Custom Service Type
	>> ddns set -i 2 -T 2 -D "domain name"
	i.e: Account index 3 setting Domain Name for Static Service Type
	>> ddns set -i 3 -T 3 -D "domain name"
-H [value]	It means to type User-Defined Provider Host.
	[value]: limit up to 64 characters
-A [value]	It means to type User-Defined Service API.
	[value]: limit up to 256 characters
-a [value]	It means to type User-Defined Auth Type.
	[value]: 0: basic 1: URL
-N [value]	It means to type User-Defined Connection Type.
	[value]: 0: Http 1: Https
-O [value]	It means to type User-Defined Server Response.
	[value]: limit up to 32 characters

Example

```
> ddns set –i 1 –S 6 –T 1 –D "hostname dnsalias.net" –L user1 -P pwd1
> Save OK
```

Telnet Command: ddns log

Displays the DDNS log.

Example

```
>ddns log
>
```

Telnet Command: ddns time

Sets and displays the DDNS time.

Syntax

ddns time *<update in minutes>*

Syntax Description

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

Example

```
> ddns time
ddns time <update in minutes>
Valid: 1 ~ 14400
%Now: 14400
> ddns time 1000
ddns time <update in minutes>
Valid: 1 ~ 14400
%Now: 1000
```

Telnet Command: ddns forceupdate

This command will update DDNS automatically.

Example

```
> ddns forceupdate
 Now updating DDNS ...
 Please check result by using command "ddns log"
```

Telnet Command: ddns setdefault

This command will return DDS with factory default settings.

Example

```
>ddns setdefault
>Set to Factory Default.
```

Telnet Command: ddns show

This command allows users to check the content of selected DDNS account.

Syntax

ddns show -i *[value]*

Syntax Description

Parameter	Description
-I [value]	Display the content of selected DDNS account. [value]: value must be between 1-6

Example

```
> ddns show -i 1
-------------------------------------------------
 Index: 1
 [ ] Enable Dynamic DNS Account
 WAN Interface: WAN1 First
 Service Provider: dyn.com (www.dyn.com)
 Service Type: Dynamic
 Domain Name: [].[]
 Login Name:
 [ ] Wildcards
 [ ] Backup MX
 Mail Extender:
 Determine Real WAN IP: WAN IP

DrayTek>
```

Telnet Command: dos

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

Syntax

dos *[-V | D | A]*

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

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

Syntax Description

Parameter	Description
-V	View the configuration of DoS defense system.
-D	Deactivate the DoS defense system.
-A	Activate the DoS defense system.
-s	Enable the defense function for a specific attack and set its parameter(s).
ATTACK_F	Specify the name of flooding attack(s) or portscan, e.g., synflood, udpflood, icmpflood, or 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	Enable the defense function for all attacks listed in ATTACK_0.
-e	Enable defense function for a specific attack(s).
ATTACK_0	Specify a name of the following attacks: ip_option, tcp_flag, land, teardrop, smurf, pingofdeath, traceroute, icmp_frag, syn_frag, unknow_proto, fraggle.
-d	Disable the defense function for a specific attack(s).

Example

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

Telnet Command: exit

Type this command will leave telnet window.

Telnet Command: Internet

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

Syntax

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

Syntax Description

Parameter	Description
-W n	W means to set WAN interface. 1=WAN1, 2=WAN2,.... Default is WAN1.
-M n	M means to set Internet Access Mode (Mandatory) and n means different modes (represented by 0 – 3) n=0: Offline n=1: PPPoE n=2: Dynamic IP n=3: Static IP n=4: PPTP with Dynamic IP, n=5: PPTP with Static IP, n=6: L2TP with Dynamic IP n=7: L2TP with Static IP n=A: 3G/4G USB Modem(PPP mode), n=B: 3G/4G USB Modem(DHCP mode)
<command><parameter>[...]	The available commands with parameters are listed below. *[...]* means that you can type in several commands in one line.
-S <isp name>	Set ISP Name (max. 23 characters).
-P <on/off>	Enable PPPoE Service.
-u <username>	Set username (max. 49 characters) for Internet accessing.
-p <password>	Set password (max. 49 characters) for Internet accessing.
-a n	It means to set PPP Authentication Type and n means different types (represented by 0-1). n=0: PAP/CHAP (this is default setting) n=1: PAP Only
-t n	Set connection duration and n means different conditions. n=-1: Always-on n=1 ~ 999: Idle time for offline (default 180 seconds)
-i <ip address>	It means that *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>	Assign gateway IP for such WAN connection.

-V	View Internet Access profile.
-C <sim pin code>	Set (PPP mode) SIM PIN code (max. 15 characters).
-O <init string>	Set (PPP mode) Modem Initial String (max. 47 characters).
-T <init string2>	Set (PPP mode) Modem Initial String2 (max. 47 characters)
-D <dial string>	Set (PPP mode) Modem Dial String (max. 31 characters).
-v <service name>	Set (PPP mode) Service Name (max. 23 characters).
-m <ppp username>	Set (PPP mode) PPP Username (max. 63 characters).
-o <ppp password>	Set (PPP mode) PPP Password (max. 62 characters).
-e n	Set (PPP mode) PPP Authentication Type. n= 0: PAP/CHAP (default), 1: PAP Only
-q n	(PPP mode) Index(1-15) in Schedule Setup-One
-x n	(PPP mode) Index(1-15) in Schedule Setup-Two
-y n	(PPP mode) Index(1-15) in Schedule Setup-Three
-z n	(PPP mode) Index(1-15) in Schedule Setup-Four
-Q <mode>	Set (PPP mode or DHCP mode) WAN Connection Detection Mode. <mode> 0: ARP Detect; 1: Ping Detect
-I <ping ip>	Set (PPP mode or DHCP mode) WAN Connection Detection Ping IP. <ping ip>= ppp.qqq.rrr.sss: WAN Connection Detection Ping IP
-L n	Set (PPP mode) WAN Connection Detection TTL (1-255) value.
-E <sim pin code>	Set (DHCP mode) SIM PIN code (max. 19 characters).
-G <mode>	Set (DHCP mode) Network Mode. <mode> 0: 4G/3G/2G; 1: 4G Only; 2: 3G Only; 3: 2G Only
-N <apn name>	Set (DHCP mode) APN Name (max. 47 characters)
-U n	(DHCP mode) MTU(1000-1440)

Example

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

```
Idle Timeout: -1
WAN IP: Dynamic IP
> internet -W 1 -M 1 -u link1 -p link1 -a 0
 You are going to watching and setting in WAN 1
 WAN1 Internet Mode set to PPPoE/PPPoA
 WAN1 Username set to link1
 WAN1 Password set successful
 WAN1 PPP Authentication Type set to PAP/CHAP
>
```

Telnet Command: ip pubsubnet

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

Syntax

ip pubsubnet *<Enable/Disable>*

Syntax Description

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

Example

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

Telnet Command: ip pubaddr

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

Syntax

ip pubaddr *?*

ip pubaddr *<public subnet IP address>*

Syntax Description

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

Example

```
> ip pubaddr ?
% ip addr <public subnet IP address>
% Now: 192.168.0.1

> ip pubaddr 192.168.2.5
% Set public subnet IP address done !!!
```

Telnet Command: ip pubmask

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

Syntax

ip pubmask *?*

ip pubmask *<public subnet mask>*

Syntax Description

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

Example

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

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

Telnet Command: ip lanalias

This command is used for configuring LAN IP Alias.

Syntax

ip lanalias *[idx] [-e / -a / -w / -r]*

Syntax Description

Parameter	Description
idx	Enter the index number (from 1 to 5) of the table displayed on your screen.
-e [0/1]	Enable / disable the IP alias.
-a [address]	Set an IP alias. [address] - Enter the IPv4 address (x.x.x.x)
-w [1/0]	Specify a number of WAN interface. "0" means no WAN.
-r	Delete an existed WAN IP address.

Example

```
> ip lanalias 1 –a 192.168.1.56
>
```

Telnet Command: ip addr

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

Syntax

ip addr *[IP address]*

Syntax Description

Parameter	Description
IP address	The LAN IP address.

Example

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

Info	When the LAN IP address is changed, the start IP address of DHCP server are still the same. To make the IP assignment of the DHCP server being consistent with this new IP address (they should be in the same network segment), the IP address of the PC must be fixed with the same LAN IP address (network segment) set by this command for accessing into the web user interface of the router. Later, modify the start addresses for the DHCP server.

Telnet Command: ip nmask

This command allows users to set/add a specified netmask for your router.

Syntax

ip nmask *[IP netmask]*

Syntax Description

Parameter	Description
IP netmask	The netmask of LAN IP.

Example

```
> ip nmask 255.255.0.0
% Set IP netmask OK !!!
```

Telnet Command: ip arp

ARP displays the matching condition for IP and MAC address.

Syntax

ip arp add *[IP address] [MAC address] [LAN or WAN]*

ip arp del *[IP address] [LAN or WAN]*

ip arp flush

ip arp status

ip arp accept *[0/1/2/3/4/5status]*

ip arp setCacheLife *[time]*

In which, **arp add** allows users to add a new IP address into the ARP table; **arp del** allows users to remove an IP address; **arp flush** allows users to clear arp cache; **arp status** allows users to review current status for the arp table; **arp accept** allows to accept or reject the source /destination MAC address; arp **setCacheLife** allows users to configure the duration in which ARP caches can be stored on the system. If **ip arp setCacheLife** is set with "60", it means you have an ARP cache at 0 second. Sixty seconds later without any ARP messages received, the

system will think such ARP cache is expired. The system will issue a few ARP request to see if this cache is still valid.

Syntax Description

Parameter	Description
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 status
[ARP Table]
 Index IP Address     MAC Address          Netbios Name    Interface  VLAN
Port
   1   192.168.1.5   00-05-5D-E4-D8-EE                      LAN1
VLAN0   P1


>
```

Telnet Command: ip dhcpc

This command is available for WAN DHCP.

Syntax

ip dhcpc *option*

ip dhcpc *option -h|l*

ip dhcpc *option -d [idx]*

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

ip dhcpc *option -u [idx unmber]*

ip dhcpc *release [wan number]*

ip dhcpc *renew [wan number]*

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 for verifying if the WAN connection is OK or not.

Syntax

ip ping *[IP address] [WAN1/WAN2]*

Syntax Description

Parameter	Description
IP address	It means the WAN IP address.
WAN1/WAN2	It means the WAN interface that the above IP address passes through.

Example

```
>ip ping 172.16.3.229 WAN1
Pinging 172.16.3.229 with 64 bytes of Data:
Receive reply from 172.16.3.229, time=0ms
Receive reply from 172.16.3.229, time=0ms
Receive reply from 172.16.3.229, time=0ms
```

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

Telnet Command: ip tracert

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

Syntax

ip tracert *[Host/IP address] [WAN1 / WAN2 / WAN3 / WAN4 / WAN5 / WAN6 / WAN7 / WAN8 / WAN9 / WAN10 / WAN11 / WAN12] [Udp/Icmp]*

Syntax Description

Parameter	Description
IP address	The target IP address.
WAN1 ~ WAN12	It means the WAN port that the above IP address passes through.
Udp/Icmp	The UDP or ICMP.

Example

```
>ip tracert 22.128.2.62 WAN1
Traceroute to 22.128.2.62, 30 hops max
1    172.16.3.7   10ms
2    172.16.1.2   10ms
3    Request Time out.
4    168.95.90.6650ms
5    211.22.38.134    50ms
6    220.128.2.6250ms
Trace complete
```

Telnet Command: ip telnet

This command allows users to access specified device by telnet.

Syntax

ip telnet *[IP address][Port]*

Syntax Description

Parameter	Description
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.

Syntax

ip rip *[0/1/2]*

Syntax Description

Parameter	Description
0/1/2	0 means disable; 1 means LAN1 and 2 means IP Routed.

Example

```
> ip rip 1
%% Set RIP LAN1.
```

Telnet Command: ip wanrip

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

Syntax

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

Syntax Description

Parameter	Description
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.

Syntax

ip route *add [dst] [netmask][gateway][ifno][rtype]*

ip route *del [dst] [netmask][rtype]*

ip route *status*

ip route *cnc*

ip route *default [wan1/wan2/off/?]*

ip route *clean [1/0]*

Syntax Description

Parameter	Description
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, 4=WAN2, 5=WAN3, 6=WAN4
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~      192.168.9.0/   255.255.255.0 is directly connected, DMZ
C~      192.168.1.0/   255.255.255.0 is directly connected, LAN1
S        172.16.2.0/   255.255.255.0 via 172.16.2.4, WAN1
```

Telnet Command: **ip igmp_proxy**

This command allows users to enable/disable igmp proxy server.

Syntax

ip igmp_proxy *set*

ip igmp_proxy *reset*

ip igmp_proxy *wan*

ip igmp_proxy *query*

ip igmp_proxy *ppp [0/1]*

ip igmp_proxy *status*

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.
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

```
This command is for setting IGMP General Query Interval
 The default value is 125000 ms
 Current Setting is:130000 ms
> ip igmp_proxy set
% ip igmp_proxy [set|reset|wan|status], IGMP Proxy is ON
> ip igmp_proxy status
%% ip igmp_proxy [set|reset|wan|status], IGMP Proxy is ON
%%% igmp_proxy WAN:
    239.255.255.250    state=1
    239.255.255.250    timer=0
```

Telnet Command: ip igmp_snoop

This command is used to enable/disable igmp snoop server.

Syntax

ip igmp_snoop *enable*

ip igmp_snoop *disable*

ip igmp_snoop *status*

ip igmp_snoop *table*

ip igmp_snoop *txquery [on|off] [v2|v3]*

ip igmp_snoop *mode [hw/sw]*

ip igmp_snoop *chkleave [on|off]*

ip igmp_snoop *separate [on|off]*

ip igmp_snoop *portchk [on|off]*

Syntax Description

Parameter	Description
enable	It means to enable proxy server.
disable	It means to disable proxy server.
status	It means to display current status for proxy server.
table	Display the whole table of IGMP Snoop configuration.
txquery [on|off] [v2|v3]	IGMP query will be sent out to LAN periodically.
mode [hw/sw]	Make IGMP snooping work on software or hardware.
chkleave [on|off]	Off - Vigor router will drop LEAVE if clients still on the same group.
separate [on|off]	On - IGMP packets will be separated by NAT/Bridge mode.

Example

```
> ip igmp_snoop mode sw
 igmp snooping works on SW mode now.
```

Telnet Command: ip session

This command allows users to set maximum session limit number for the specified IP; set message for exceeding session limit and set how many seconds the IP session block works.

Syntax

ip session *on*

ip session *off*

ip session *default [num]*

ip session *defaultp2p [num]*

ip session *status*

ip session *show*

ip session *timer [num]*

ip session *[block/unblock][IP]*

ip session *[add/del][IP1-IP2][num][p2pnum]*

Syntax Description

Parameter	Description
on	Turn on session limit for each IP.
off	Turn off session limit for each IP.
default [num]	Set the default number of session num limit.
Defautlp2p [num]	Set the default number of session num limit for p2p.
status	Display the current settings.
show	Display all session limit settings in the IP range.
timer [num]	Set when the IP session block works. The unit is second.
[block/unblock][IP]	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	Add the session limits in an IP range.
del	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.

Syntax

ip bandwidth *on*

ip bandwidth *off*

ip bandwidth *default [tx_rate][rx_rate]*

ip bandwidth *status*

ip bandwidth *show*

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

Syntax Description

Parameter	Description
on	Turn on the IP bandwidth limit.
off	Turn off the IP bandwidth limit.
default [tx_rate][rx_rate]	Set default tx and rx rate of bandwidth limit. The range is from 0 - 65535 Kpbs.
status	Display the current settings.
show	Display all the bandwidth limits settings within the IP range.
add	Add the bandwidth within the IP range.
del	Delete the bandwidth within the IP range.
IP1-IP2	It means the range of IP address specified for this command.
tx	Set transmission rate for bandwidth limit.
rx	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.

Syntax

ip bindmac *on*

ip bindmac *off*

ip bindmac *strict_on*

ip bindmac *show*

ip bindmac *add [IP][MAC][Comment]*

ip bindmac *del [IP]/all*

Syntax Description

Parameter	Description
on	Turn on IP bandmac policy. Even the IP is not in the policy table, it can still access into network.
off	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	Display the IP address and MAC address of the pair of binded one.
add	Add one IP bindmac.
del	Delete one IP bindmac.
IP	Type the IP address for binding with specified MAC address.
MAC	Type the MAC address for binding with the IP address specified.
Comment	Type words as a brief description.
All	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 bgp

This command allows users to configure settings for BGP.

Syntax

ip bgp mode *[0/1]*

ip bgp as *[value]*

ip bgp hold *[value]*

ip bgp retry *[value]*

ip bgp id *[value]*

ip bgp show

ip bgp neighbor *[idx]* **mode** *[0/1]*

ip bgp neighbor *[idx]* **name** *[max len: 20]*

ip bgp neighbor *[idx]* **ip** *[x.x.x.x]*

ip bgp neighbor *[idx]* **as** *[1~4294967295]*

ip bgp neighbor *[idx]* **md5** *<0/1>*

ip bgp neighbor *[idx]* **key** *[max len: 20]*

ip bgp neighbor *[idx]* **show**

ip bgp neighbor show all

ip bgp static *[sidx][ip][<netmask]*

ip bgp static *[sidx]* **delete**

ip bgp static show

Syntax Description

Parameter	Description
mode <0/1>	It means to enable / disable BGP mode. 0: disable 1: enable

as <value>	It means to set the AS number for local router. <value>: Available number is between 0 and 4294967295.
hold <value>	It means to set the time interval to determine the peer is dead when the router is unable to receive any keepalive message from the peer within the time. <value>: Available number is between 10 and 65535 (unit: second). The default is 180 (seconds).
retry <value>	It means to set a period of time to reconnect if the router fails to connect to the neighboring router. <value>: Available number is between 3 and 255 (unit: second). The default is 120 (seconds).
id <value>	It means to specify the LAN subnet <1~16> as router ID. <value>: Available number is between 1 and 16.
show	It means to display information related to BGP settings.
neighbor <idx> mode <0/1>	It means to enable / disable the basic BGP function for neighboring router. <idx>: Available profile number is between 1 and 8. <0/1>: 0- disable; 1- enable
neighbor <idx> name <max len: 20>	It means to define a profile name for neighboring router. <idx>: Available profile number is between 1 and 8. <max len>: The maximum name length shall not be over 20 characters.
neighbor <idx> ip <x.x.x.x>	It means to set the IP address specified for the neighboring router. <idx>: Available profile number is between 1 and 8. <x.x.x.x>: Enter the IP address, e.g., 100.100.100.100.
neighbor <idx> as <1~4294967295>	It means to set the AS number for the neightboring router. <idx>: Available profile number is between 1 and 8. <value>: Available number is between 1 and 4294967295.
neighbor <idx> md5 <0/1>	It means to enable or disable (1/0) for MD5 function for the neightboring router.
neighbor <idx> key <max len: 20>	It menas to define a key for the neightboring router. <max len>: The maximum name length shall not be over 20 characters.
neighbor <idx> show	It means to display information for the specified profile. <idx>: Available profile number is between 1 and 8.
neighbor show all	It means to display information for all neighboring routers.
static <sidx> <ip> <netmask>	It means to configure the neighboring router(s) for exchanging the routing information with the local router. <sidx>: Available profile number is between 1 and 16. <ip>: Enter the IP address, e.g., 100.100.100.200. <netmask>: Enter the subnet mask for the neighboring router, e.g., 255.255.255.0.
static <sidx> delete	It means to delete static network settings for neighboring router. <sidx>: Available profile number is between 1 and 16.
static show	It means to display setting information for exchanging the routing information with the local router.

Example

```
> ip bgp static 1 192.168.2.56 255.255.255.0
Set static network index: 1
```

```
IP addr: 192.168.2.56
Net mask: 255.255.255.0
> ip bgp static show
BGP static networks:
Index: 1, IP addr: 192.168.2.56, mask: 255.255.255.0
```

Telnet Command: **ip maxnatuser**

This command is used to set the maximum number of NAT users.

Syntax

ip maxnatuser *user no*

Syntax Description

Parameter	Description
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: **ip policy_rt**

This command is used to set the IP policy route profile.

Syntax

ip policy_rt *[-<command> <parameter> | …]*

Syntax Description

Parameter	Description
<command><parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
General Setup for Policy Route	
-i [value]	Specify an index number for setting policy route profile. Value: 1 to 60. "-1" means to get a free policy index automatically.
-e [0/1]	0: Disable the selected policy route profile. 1: Enable the selected policy route profile.
-o [value]	Determine the operation of the policy route. Value: add - Create a new policy rotue profile. del - Remove an existed policy route profile. edit - Modify an existed policy route profile. flush - Reset policy route to default setting.
-1 [any/range]	Specify the source IP mode. Range: Indicate a range of IP addresses. Any: It means any IP address will be treated as source IP address.
-2 [any/ip_range/ip_subnet/domain]	Specify the destination IP mode. Any: No need to specify an IP address for any IP address will be treated as destination IP address. ip_range: Indicates a range of IP addresses. ip_subnet: Indicates the IP subnet. domain: Indicates the domain name.
-3 [any/range]	Specify the destination port mode. Range: Indicate a range of port number.

	Any: It means any port number can be used as destination port.
-G [default/specific]	Specify the gateway mode.
-L [default/specific]	Specify the failover gateway mode.
-s [value]	Indicate the source IP start. Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.1.0)
-S [value]	Indicate the source IP end. Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.1.100)
-d [value]	Indicate the destination IP start. Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.2.0)
-D [value]	Indicate the destination IP end. Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.2.100)
-p [value]	Indicate the destination port start. Value: Type a number (1 ~ 65535) as the port start (e.g., 1000).
-P [value]	Indicate the destination port end. Value: Type a number (1 ~ 65535) as the port end (e.g., 2000).
-y [value]	Indicate the priority of the policy route profile. Value: Type a number (0 ~ 250). The default value is "150".
-I [value]	Indicate the interface specified for the policy route profile. Value: Available interfaces include, LAN1 ~ LAN8, IP_Routed_Subnet, DMZ_Subnet, WAN1 ~ WAN5, VPN_PROFILE_1 ~ VPN_PROFILE_100, WAN_1_IP_ALIAS_1 ~ WAN_4_IP_ALIAS_8
-g [value]	Indicate the gateway IP address. Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.3.1)
-I [value]	Indicate the failover IP address. Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.4.1)
-t [value]	It means "protocol". Value: Available settings include "TCP", "UDP", "TCP/UDP", "ICMP" and "Any".
-n [0/1]	Indicates the function of "Force NAT". 0: Disable the function. 1: Enable the function.
-a [0/1]	Indicates to enable the function of failover. 0: Disable the function. 1: Enable the function.
-f [value]	It means to specify the interface for failover. Value: Avaialbe interfaces include, NO_FAILOVER, Default_WAN, Policy1 ~ Policy60 LAN1 ~ LAN8 IP_Routed_Subnet, DMZ_Subnet, WAN1 ~ WAN5, VPN_PROFILE_1 ~ VPN_PROFILE_100, WAN_1_IP_ALIAS_1 ~ WAN_4_IP_ALIAS_8
-b [value]	It means "failback".

	Value: Available settings include,
	0: Disable the function of "failback".
	1: Enable the function of "failback".
	-v: View current failback setting.

Diagnose for Policy Route

-s [value]	It means "source IP".
	Value: Available settings include:
	Any: It indicates any IP address can be used as source IP address.
	"xxx.xxx.xxx.xxx": The type format (e.g, 192.168.1.0).
-d [value]	It means "destination IP".
	Value : Available settings include:
	Any: It indicates any IP address can be used as destination IP address.
	"xxx.xxx.xxx.xxx": Specify an IP address.
-p [value]	It means "destination port".
	Value: Specify a number or type Any (indicating any number).
-t [value]	It means "protocol".
	Value: Available settings include "ICMP", "TCP", "UDP" and "Any".

Example

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


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


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

    * Conclusion:The packet was dropped because the send-to interface
of the mat
ched policy "policy 1" was inactive and there was no failover setting
> ip policy_rt -i -1 -o add -1 range -s 192.168.1.10 -S 192.168.1.20 -2
ip_range -d 202.211.100.10 -D 202.211.100.20 -g 202.211.100.1 -I WAN2
```

Telnet Command: ip lanDNSRes

This command is used to set LAN DNS profile.

Syntax

ip lanDNSRes *[-<command> <parameter> | …]*

Syntax Description

Parameter	Description
<command><parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-a <IP Address>	Set IP Address that domain name mapped.
-c <CNAME>	Set CNAME value.
-d <address mapping index number>	Delete the selected LAN DNS profile.
-e <0/1>	0: disable the selected LAN DNS profile. 1: enable the selected LAN DNS profile.
-i <profile setting index number>	Type the index number of the profile.
-l	List the content of LAN DNS profile (including domain name, IP address and message).
-n <domain name>	Set domain name.
-p <profile name>	Set profile name for LAN DNS.
-r	Reset the settings for selected profile.
-s *<0/1>*	0:reply all 1:reply only same subnet packet.
-z	Update LAN DNS config to DNS Cache.

Example

```
>
ip lanDNSRes -i 1 -p test
% Configure Set1's Profile:test
> ip lanDNSRes -i 1 -l
% Idx: 1
% State: Disable
% Profile: test
% Domain Name:
% -------- Address Mapping Table --------
% Not Set Address Mapping.
>
```

Telnet Command: ip dnsforward

This command is used to set LAN DNS profile for conditional DNS forwarding.

Syntax

ip dnsforward *[-<command> <parameter> | …]*

Syntax Description

Parameter	Description
[<command><parameter>|...]	The available commands with parameters are listed below. *[...]* means that you can type in several commands in one line.
-a <IP Address>	Set forwarded DNS server IP Address.
-d <DNS server mapping index number>	Delete the selected LAN DNS profile.
-e <0/1>	0: disable such function. 1: enable such function.
-i <profile setting index number>	Type the index number of the profile.
-l	List the content of LAN DNS profile (including domain name, IP address and message).
-n <domain name>	Set domain name.
-p <profile name>	Set profile name for LAN DNS.
-r	Reset the settings for selected profile.

Example

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

Telnet Command: ip6 addr

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

Syntax

ip6 addr -s *[prefix] [prefix-length] [LAN|WAN1|WAN2|iface#]*

ip6 addr -d *[prefix] [prefix-length] [LAN|WAN1|WAN2|iface#]*

ip6 addr -a *[LAN|WAN1|WAN2|iface#]*

Syntax Description

Parameter	Description
-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.

Syntax

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.

Syntax

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.

Syntax

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.
-i<pool_min_addr>	It means to set the start IPv6 address of the address pool.
-x<pool_max_addr>	It means to set the end IPv6 address of the address pool.
-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.

Syntax

ip6 internet *-W n -M n [-<command> <parameter> | …]*

Syntax Description

Parameter	Description
-W n	**W** means to set WAN interface and **n** means different selections. Default is WAN1. n=1: WAN1 n=2: WAN2 n=3: WAN3 . . n=X: WANx
-M n	M means to set Internet Access Mode (Mandatory) and n means different modes (represented by 0 – 5) n= 0: Offline, n=1: PPP, n=2: TSPC, n=3: AICCU, n=4: DHCPv6,

	n=5: Static
	n=6:6in4-Static
	n=7:6rd
[<command> <parameter>|...]	The available commands with parameters are listed below.
	[...] means that you can type in several commands in one line.
-m n	It means to set IPv6 MTU.
	N = any value (0 means "unspecified").
-u <username>	It means to set Username.
	<username>= type a name as the username (maximum 63 characters).
-p <password>	It means to set Password.
	<password> = type a password (maximum 63 characters).
-s <server>	It means to set Tunnel Server IP.
	<server>= IPv4 address or URL (maximum 63 characters).
-d <server>	It means to set the primary DNS Server IP.
	<server>= type an IPv6 address for first DNS server.
-D <server>	It means to set the secondary DNS Server IP.
	<server>= type an IPv6 address for second DNS server.
-t <dhcp/ra/none>	It means to set IPv6 PPP WAN test mode for DHCP or RADVD.
	<dhcp/ra/none>= type IPv6 address.
-V	It means to view IPv6 Internet Access Profile.
-o	It means to set AICCU always on.
	1=On,
	0=Off

Example

```
> ip6 internet -W 2 -M 2 -u 88886666 -p draytek123456 -s
amsterdam.freenet6.net
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
> system reboot
```

Telnet Command: ip6 neigh

This command allows you to display IPv6 neighbour table.

Syntax

ip6 neigh *-s[inet6_addr] [eth_addr] [LAN|WAN1|WAN2]*

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

ip6 neigh *-a [inet6_addr] [-N LAN|WAN1|WAN2]*

Syntax Description

Parameter	Description
-s	It means to add a neighbour.
-d	It means to delete a neighbour.
-a	It means to show neighbour status.
inet6_addr	Type an IPv6 address
eth_addr	Type submask address.

| LAN/WAN1/WAN2 | Specify an interface for the neighbor. |

Example

```
> ip6 neigh -s 2001:2222:3333::1111 00:50:7F:11:ac:22:WAN2
       Neighbour 2001:2222:3333::1111 successfully added!
> ip6 neigh -a

I/F  ADDR                                  MAC                 STATE
-------------------------------------------------------------------
LAN FF02::1                                33-33-00-00-00-01   CONNECTED
WAN2 2001:5C0:1400:B::10B8                 00-00-00-00-00-00   CONNECTED
WAN2 2001:2222:3333::1111                  00-00-00-00-00-00   CONNECTED
WAN2 2001:2222:6666::1111                  00-00-00-00-00-00   CONNECTED
WAN2 ::                                    00-00-00-00-00-00   CONNECTED
LAN  ::                                                        NONE
>
```

Telnet Command: ip6 pneigh

This command allows you to add a proxy neighbour.

Syntax

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	Specify an interface for the proxy neighbor.

Example

```
> ip6 neigh -s FE80::250:7FFF:FE12:300 LAN
%      Neighbour FE80::250:7FFF:FE12:300 successfully added!
```

Telnet Command: ip6 route

This command allows you to

Syntax

ip6 route *-s [prefix] [prefix-length] [gateway] [LAN|WAN1|WAN2|iface#> [-D]*

ip6 route *-d [prefix] [prefix-length]*

ip6 route *-a [LAN|WAN1|WAN2|iface#]*

Syntax Description

Parameter	Description
-s	It means to add a route.
-d	It means to delete a route.
-a	It means to show the route status.
-D	It means that such route will be treated as the default route.
prefix	It means to type the prefix number of IPv6 address.
prefix-length	It means to type a fixed value as the length of the prefix.
gateway	It means the gateway of the router.
LAN|WAN1|WAN2|iface#	It means to specify LAN or WAN interface for such address.

Example

```
> ip6 route -s FE80::250:7FFF:FE12:500 16 FE80::250:7FFF:FE12:100 LAN
%      Route FE80::250:7FFF:FE12:500/16 successfully added!
> ip6 route -a LAN
```

```
 PREFIX/PREFIX-LEN _EXPIRES_ _NEXT-HOP_  I/F  METRIC   STATE      FLAGS
----------------------------------------------------------------------
------
 FE80::/128                              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.

Syntax

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.

Syntax

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::2:0:66$^E$        340 ms
  9 Request timed out.          *
 10 2001:4860:4860::8888      350 ms
Trace complete.
>
```

Telnet Command: ip6 tspc

This command allows you to display TSPC status.

Syntax

ip6 tspc *[ifno]*

Syntax Description

Parameter	Description
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.

Syntax

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.

Syntax

ip6 mngt list

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

ip6 mngt status

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

Syntax Description

Parameter	Description
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|https|ssh	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.

Syntax

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.

Syntax

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.

Syntax

ip6 ntp –h

ip6 ntp –v

ip6 ntp -p [0/1]

Syntax Description

Parameter	Description
-h	It is used to display the usage of such command.
-v	It is used to show the NTP state.
-p <0/1>	It is used to specify NTP server for IPv6. 0 - Auto 1 - First Query IPv6 NTP Server.

Example

```
> ip6 ntp -p 1
% Set NTP Priority: IPv6 First
```

Telnet Command: ip6 lan

This command allows you to set IPv6 settings for LAN interface.

Syntax

ip6 lan -l n *[-<l:w:d:D:m:o:s> <parameter> | …]*

Syntax Description

Parameter	Description
-h	It is used to display the usage of such command.
-l n	It means to selete LAN interface to be set. n= 1: LAN1 n= 2: LAN2, … x: LANx. Default is LAN1
-w n	It means to selete WAN interface to be primary interface. n= 0: None, n=1: WAN1 , n=2: WAN2, … x: WANx.
-d <server>	It means to set 1st DNS Server IP. <server>= IPv6 Address
-D <server>	It means to set 2nd DNS Server IP. <server>= IPv6 Address
-m n	It means to set ipv6 LAN management. n=0:OFF n=1:SLAAC. Default is SLAAC n=2:DHCPv6
-o n	It means to enable Other option(O-bit) flag. (O-bit is redundant when management is DHCPv6) n=0: Disable

	n=1: Enable.
-e n	It means to add an extension WAN.
	n: 1: WAN1, 2: WAN2, ... x: WANx.
-E n	It means to delete an extension WAN.
	n: 1: WAN1 ,2: WAN2, ... x: WANx.
-b map	It means to set bit map(decimal) for extension WAN.
	map:
	bit 0: WAN1
	bit 1: WAN2, ... bit n: WAN(n+1).
-f n	It means to disable IPv6.
	n= 1: Disable IPv6,
	n=0: Enable IPv6.
-R n	It means to enable /disable RIPng.
	n=1: Enable RIPng,
	n=0: Disable RIPng.
-s n	It means to show IPv6 LAN setting.
	n=0:show all. Default is show all.
	n=1: LAN1
	n=2: LAN2, ... 50: LAN50,
	n=51: DMZ.

Example

```
> ip6 lan -l 1 -w 1 -d 2001:4860:4860::8888 -o 1 -f 0 -s 2
%    Set LAN1!
%    Set primary WAN1!
%  Set 1st DNS server 2001:4860:4860::8888
%    Set Other Option Enable!
%    [LAN1] support ipv6!
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
% [LAN2] setting:
% Primary WAN   : WAN1
% Management    : SLAAC
% Other Option  : Disable
% WAN Exten     : None
% Subnet ID     : 2
% Static IP(0)  : ::/0
%               [ifno: 0, enable: 0]
% Static IP(1)  : ::/0
%               [ifno: 0, enable: 0]
% Static IP(2)  : ::/0
%               [ifno: 0, enable: 0]
% Static IP(3)  : ::/0
%               [ifno: 0, enable: 0]
% DNS1          : 2001:4860:4860::8888
```

```
%  DNS2            : 2001:4860:4860::8844
%  ULA Type        : OFF
%  RIPng           : Enable
```

Telnet Command: ip6 session

This command allows you to set sessions limit for IPv6 address.

Syntax

ip6 session *[on/off/default num/status/show]*

ip6 session *[add/del] [IP1-IP2] [num]*

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.
status	It means to display the current settings.
show	It means to display all IP range session limit settings.
add	It means to add the session limit for an IPv6 range. <IP1-IP2> - Specify a range for IPv6 addresses.
del	It means to delete the session limit for an IPv6 range by first IP (IP1) or 'del all'.

Example

```
> ip6 session on
> ip6 session add 2100:ABCD::2-2100:ABCD::10 100
> ip6 session status

  IPv6 range:
    2100:ABCD::2 - 2100:ABCD::10 : 100

  Current ip6 session limit is turn on

  Current default session number is 100
```

Telnet Command: ip6 bandwidth

This command allows you to set IPv6 settings

Syntax

ip6 Bandwidth [*on/off/default tx_rate rx_rate/status/show***]**

ip6 Bandwidth *[add/del] [IP1-IP2] [tx][rx][shared]*

Syntax Description

Parameter	Description
on	It means to turn on bandwidth limit for each IP.
off	It means to turn off bandwidth limit for each IP.

default <tx> <rx>	It means to set the default transmission (tx), receiving (rx) rate of bandwidth limit (0-30000 Kbps/Mbps).
status	It means to display the current settings.
show	It means to display all IP range bandwidth limit settings.
add	It means to add the bandwidth limit for an IPv6 range. <IP1-IP2> - Specify a range for IPv6 addresses.
del	It means to delete the bandwidth limit for an IPv6 range by first IP (IP1) or 'del all'.

Example

```
> ip6 bandwidth on
> ip6 bandwidth add 2001:ABCD::2-2001:ABCD::10 512 5M shared
> ip6 bandwidth status

  IPv6 range:
    2001:ABCD::2 - 2001:ABCD::10 : Tx:512K Rx:5M shared

  Current ip6 Bandwidth limit is turn on


  Current default ip6 Bandwidth rate is Tx:2000K Rx:8000K bps
```

Telnet Command: ipf view

IPF users to view the version of the IP filter, to view/set the log flag, to view the running IP filter rules.

Syntax

ipf view *[-VcdhrtzZ]*

Syntax Description

Parameter	Description
-V	It means to show the version of this IP filter.
-c	It means to show the running call filter rules.
-d	It means to show the running data filter rules.
-h	It means to show the hit-number of the filter rules.
-r	It means to show the running call and data filter rules.
-t	It means to display all the information at one time.
-z	It means to clear a filter rule's statistics.
-Z	It means to clear IP filter's gross statistics.

Example

```
> ipf view -V -c -d
ipf: IP Filter: v3.3.1 (1824)
```

```
Kernel: IP Filter: v3.3.1
Running: yes
Log Flags: 0x80947278 = nonip
Default: pass all, Logging: available
```

Telnet Command: ipf set

This command is used to set general rule for firewall.

Syntax

ipf set *[Options]*

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

Syntax Description

Parameter	Description
Options	There are several options provided here, such as *-v, -c [SET_NO], -d [SET_NO],… and etc.*
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.
-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 -c 1  #set call filter start from set 1
```

```
Setting saved.

> ipf set -d 2  #set data filter start from set 2
Setting saved.
> ipf set -v

Call Filter: Enable (Start Filter Set = 1)
Data Filter: Enable (Start Filter Set = 2)
Log Flag  : None

Actions for packet not matching any rule:
  Pass or Block    : Pass
  CodePage         : ANSI(1252)-Latin I
  Max Sessions Limit: 60000
  Current Sessions : 0
  Mac Bind IP      : Non-Strict
  QOS Class        : None
  APP Enforcement  : None
  URL Content Filter: None
  Load-Balance policy : Auto-select
  ----------------------------------------------------------------
  CodePage              : ANSI(1252)-Latin I
  Window size           : 65535
  Session timeout       : 1440
  DrayTek Banner        : Enable
  ----------------------------------------------------------------
  Apply IP filter to VPN incoming packets          : Enable
  Accept large incoming fragmented UDP or ICMP packets: Enable
  ----------------------------------------------------------------
  Strict Security Checking
    [ ]APP Enforcement
>
```

Telnet Command: ipf rule

This command is used to set filter rule for firewall.

Syntax

ipf rule *s r [-<command> <parameter> | …*

ipf rule s r -v

Syntax Description

Parameter	Description
s	Such word means Filter Set, range form 1~12.
r	Such word means Filter Rule, range from 1~7.
[<command><parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-e	It means to enable or disable the rule setting. 0- disable 1- enable

Vigor3910 Series User's Guide

-s o:g <obj>	It means to specify source IP object and IP group. o - indicates "object". g - indicates "group". obj - indicates index number of object or index number of group. Available settings range from 1-192. For example, "-s g 3" means the third source IP group profile.
–s u <Address Type> <Start IP Address> <End IP Address> / <Address Mask>	It means to configure **source** IP address including address type, start IP address, end IP address and address mask. u – It means "user defined". *Address Type* - Type the number (representing different address type). 0 - Subnet Address 1 - Single Address 2 - Any Address 3 - Range Address Example: Set Subnet Address => -s u 0 192.168.1.10 255.255.255.0 Set Single Address => -s u 1 192.168.1.10 Set Any Address => -s u 2 Set Range Address => -s u 3 192.168.1.10 192.168.1.15
–d u <Address Type> <Start IP Address> <End IP Address> / <Address Mask>	It means to configure **destination** IP address including address type, start IP address, end IP address and address mask. u – It means "user defined". *Address Type* - Type the number (representing different address type). 0 - Subnet Address 1 - Single Address 2 - Any Address 3 - Range Address Example: Set Subnet Address => -d u 0 192.168.1.10 255.255.255.0 Set Single Address => -d u 1 192.168.1.10 Set Any Address => -d u 2 Set Range Address => -d u 3 192.168.1.10 192.168.1.15
-d o:g <obj>	It means to specify destination IP object and IP group. o – indicates "object". g – indicates "group" <obj>– indicates index number of object or index number of group. Available settings range from 1-192. For example, "-d g 1" means the first destination IP group profile.
-S o:g <obj>	It means to specify Service Type object and IP group. o – indicates "object". g – indicates "group" <obj> – indicates index number of object or index number of group. Available settings range from 1-96. For example, "-S 0 1" means the first service type object profile.

-S u <protocol> <source_port__value> <destination_port_vale>	It means to configure advanced settings for Service Type, such as protocol and port range.
	
	u – it means "user defined".
	
	<protocol> – It means TCP(6),UDP(17), TCP/UDP(255).
	
	<source_port__value> –
	
	     1 – Port OP, range is 0-3. 0:= =, 1:!=, 2:>, 3:<
	
	     3 – Port range of the Start Port Number, range is

	1-65535.
	5 – Port range of the End Port Number, range is 1-65535.
	\<destination_port_value\>:
	2 – Port OP, range is 0-3, 0:==, 1:!=, 2:\>, 3:\<
	4 – Port range of the Start Port Number, range is 1-65535.
	6 - Port range of the End Port Number, range is 1-65535.
-F	It means the Filter action you can specify.
	0 –Pass Immediately,
	1 - Block Immediately,
	2 - Pass if no further match,
	3 - Block if no further match.
-q	It means the classification for QoS.
	1- Class 1,
	2 - Class 2,
	3 - Class 3,
	4 - Other
-l	It means load balance policy.
	Such function is used for "debug" only.
-E	It means to enable APP Enforcement.
-a\<index\>	It means to specify which APP Enforcement profile will be applied.
	\<index\> – Available settings range from 0 ~ 32. "0" means no profile will be applied.
-u\<index\>	It means to specify which URL Content Filter profile will be applied.
	\<index\> – Available settings range from 0 ~ 8. "0" means no profile will be applied.
-c	It means to set code page. Different number represents different code page.
	0. None
	1. ANSI(1250)-Central Europe
	2. ANSI(1251)-Cyrillic
	3. ANSI(1252)-Latin I
	4. ANSI(1253)-Greek
	5. ANSI(1254)-Turkish
	6. ANSI(1255)-Hebrew
	7. ANSI(1256)-Arabic
	8. ANSI(1257)-Baltic
	9. ANSI(1258)-Viet Nam
	10. OEM(437)-United States
	11. OEM(850)-Multilingual Latin I
	12. OEM(860)-Portuguese
	13. OEM(861)-Icelandic
	14. OEM(863)-Canadian French
	15. OEM(865)-Nordic
	16. ANSI/OEM(874)-Thai
	17. ANSI/OEM(932)-Japanese Shift-JIS
	18. ANSI/OEM(936)-Simplified Chinese GBK
	19. ANSI/OEM(949)-Korean
	20. ANSI/OEM(950)-Traditional Chinese Big5
-C \<Windows Size\> \<Session_Timeout\>	It means to set Window size and Session timeout (Minute).
	\<Windows Size\> - Available settings range from 1 ~ 65535.

	<Session_Timeout> - Make the best utilization of network resources.
-v	It is used to show current filter/rule settings.

Example

```
> ipf rule 2 1 -e 1 -s "o 1" -d "o 2" -S "o 1" -F 2
> ipf rule 2 1 -v

Filter Set 2 Rule 1:

Status  : Enable
Comments: xNetBios -> DNS
Index(1-15) in Schedule Setup: <null>, <null>, <null>, <null>

Direction   : LAN -> WAN
Source IP   : Group1,
Destination IP: Group2,
Service Type  : TCP/UDPGroup1,
Fragments   : Don't Care

Pass or Block          : Block Immediately
Branch to Other Filter Set: None
Max Sessions Limit     : 32000
Current Sessions       : 0
Mac Bind IP            : Non-Strict
Qos Class              : None
APP Enforcement        : None
URL Content Filter     : None
Load-Balance policy    : Auto-select
Log                    : Disable
-------------------------------------------------------------------
----
CodePage               : ANSI(1252)-Latin I
Window size            : 65535
Session timeout        : 1440
DrayTek Banner         : Enable

-------------------------------------------------------------------
---
  Strict Security Checking
    [ ]APP Enforcement

```

Telnet Command: ipf flowtrack

This command is used to set and view flowtrack sessions.

Syntax

ipf flowtrack set *[-re]*

ipf flowtrack view *[-f]*

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

Syntax Description

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

Telnet Command: Log

This command allows users to view log for WAN interface such as call log, IP filter log, flush log buffer, etc.

Syntax

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

Syntax Description

Parameter	Description
-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: ldap user

This command is used to configure the LDAP profile.

Syntax

ldap user *[INDEX][OPTION]*

Syntax Description

Parameter	Description
INDEX	Specify the index number (1 to 8) of the LDAP profile.
OPTION	
-n VALUE	Setup Profile Name.
-b VALUE	Setup Base Distinguished Name.
-a VALUE	If you have added containers to be published, you may need to specify additional LDAP filters for each class of objects included in these containers.
	Creating LDAP filters is a fairly complex task that should be performed by advanced users only. LDAP filters must be RFC2254-compliant.
	For example, to exclude from publication all users who either belong to the HR department of your company or are members of the HR Group. For example:
	>ldap user 1 -a "(!(|(department=HR)(memberOf=CN=HRGroup,OU=Groups, DC=acme,DC=com)))"
	Additional Filter has been updated.
-g VALUE	Setup Group Distinguished Name.
-c VALUE	Setup Common Name Identifier.
-v	View detail information of the LDAP profile.

Example

```
>ldap user 1 -n LD_user_test1
Profile Name has been updated!
> ldap user 1 -v
Profile Index:1
Profile Name:LD_user_test1
Common Name Identifier:
Base Distinguished Name:
Additional Filter:
Group distinguished Name:
>ldap user 1 -b ou=People,dc=example,dc=com
```

Telnet Command: ldap set

This command is used to set general settings (e.g., IP address, port number) for LDAP server.

Syntax

ldap set *[Options][Value]*

Syntax Description

Parameter	Description
enable [0-1]	Enable or disable LDAP function.
	0 - Disable the function.
	1 - Enable the function.
type [0-2]	Set the bind type as Simple(0),Anonymous(1), and Regular(2).
ssl [0-1]	Enable or disable LDAP function via SSL tunnel.
	0 - Disable the function.
	1 - Enable the function.
IP <VALUE>	Set IP address for LDAP server.

port <VALUE>	Set port number for LDAP server.
dn <VALUE>	Set Regular DN value
PWD <VALUE>	Set Regular password value.

Example

```
>ldap set enable 1
>ldap enabled.
> ldap set ssl 1
LDAP with SSL has been enabled!
> ldap set IP 192.168.100.155
LDAP Server IP has been setting.
> ldap set port 389
LDAP Server Port has been setting.
> ldap set dn dc=example,dc=com
LDAP Regular DN has been setting.
> ldap set PWD 123456
LDAP Regular Password has been setting.
```

Telnet Command: ldap view

This command is used to check current status of LDAP settings configuration.

Syntax

ldap view

Example

```
> ldap view ?
LDAP Enable:Disabled.
LDAP Bind Type:Simple
LDAP with SSL:Disabled
LDAP Regular DN:
LDAP Regular Password:
LDAP Server IP:
LDAP Server Port:389
```

Telnet Command: tacacsplus set

This command allows users to configure general settings for TACACS+ server

Syntax

tacacspluse set *[Options][Value]*

Syntax Description

Parameter	Description
enable [0-1]	Disable (0)/enable(1) the TACACS+ server.
IP <VALUE>	Set the IP address of TACACS+ server.
port <VALUE>	Set the port number of TACACS+ server.
shared_secret <VALUE>	Set the Shared Secret value of TACACS+ Server.

Example

```
> tacacsplus set enable 1
TACACS+ enabled!
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.


> tacacsplus set IP 192.168.1.59
TACACS+ Server IP has been setting.
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
> tacacsplus view
TACACS+ Enable:Enable.
TACACS+ Server IP:192.168.1.59
TACACS+ Server Port:49
TACACS+ Type:ASCII
TACACS+ Shared Secret:
```

Telnet Command: tacacsplus view

This command allows users to check the general settings for TACACS+ server

Syntax

tacacspluse view

Example

```
> tacacsplus view
TACACS+ Enable:Enable.
TACACS+ Server IP:192.168.1.59
TACACS+ Server Port:49
TACACS+ Type:ASCII
TACACS+ Shared Secret:
```

Telnet Command: mngt ftpport

This command allows users to set FTP port for management.

Syntax

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.

Syntax

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.

Syntax

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.

Syntax

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.

Syntax

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.

Syntax

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.

Syntax

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.

Syntax

mngt defenseworm *[on]*

mngt defenseworm *[off]*

mngt defenseworm *[add port]*

mngt defenseworm *[del port]*

mngt defenseworm *[viewlog]*

mngt defenseworm *[clearlog]*

Syntax Description

Parameter	Description
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.

Syntax

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 ftp on
Enable server fail
Remote configure function has been disabled
please enable by enter mngt rmtcfg enable

> mngt rmtcfg enable
%% Remote configure function has been enabled.
> mngt rmtcfg ftp on
%% FTP server has been enabled.
```

Telnet Command: mngt lanaccess

This command allows users to manage accessing into Vigor router through LAN port.

Syntax

mngt lanaccess *-e [0/1] –s [value] –i [value]*

mngt lanaccess *–f*

mngt lanaccess *–d*

mngt lanaccess *–v*

mngt lanaccess *–h*

Syntax Description

Parameter	Description
-e[0/1]	It means to enable/disable the function. 0-disable the function. 1-enable the function.
-s[value]	It means to specify service offered. Available values include: FTP, HTTP, HTTPS, TELNET, SSH, None, All
-i[value]	It means the interface which is allowed to access. Available values include: LAN2~LAN6, DMZ, IP Routed Subnet, None, All **Note**: LAN1 is always allowed for accessing into the router.
-f	It means to flush all of the settings.
-d	It means to restore the factory default settings.
-v	It means to view current settings.
-h	It means to get the usage of such command.

Example

```
> mngt lanaccess -e 1
> mngt lanaccess -s FTP,TELNET
```

```
> mngt lanaccess -i LAN3
> > mngt lanaccess -v
Current LAN Access Control Setting:
* Enable:Yes
* Service:
  - FTP:Yes
  - HTTP:No
  - HTTPS:No
  - TELNET:Yes
  - SSH:No
* Subnet:
  - LAN 2: disabled
  - LAN 3: enabled
  - LAN 4: disabled
  - LAN 5: disabled
  - LAN 6: disabled
  - DMZ: disabled
  - IP Routed Subnet: disabled


Note: the settings do NOT apply to LAN1, LAN1 is always allowed to access
the router
```

Telnet Command: mngt echoicmp

This command allows users to reject or accept PING packets from the Internet.

Syntax

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.

Syntax

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.

Syntax

mngt snmp *[-<command> <parameter> | …]*

Syntax Description

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

Example

```
> mngt snmp -e 1 -g draytek -s DK -m 192.168.1.1 -t trapcom -n 10.20.3.40
```

```
-T 88
 SNMP Agent Turn on!!!
 Get Community set to draytek
 Set Community set to DK
 Manager Host IP set to 192.168.1.1
 Trap Community set to trapcom
 Notification Host IP set to 10.20.3.40
 Trap Timeout set to 88 seconds
```

Telnet Command: mngt bfp

This command allows you to configure brute force protect (BFP) for system management.

Syntax

mngt bfp *[<command><parameter>|...]*

Syntax Description

Parameter	Description
[<command> <parameter>|...]	The available commands with parameters are listed below. *[...]* means that you can type in several commands in one line.
-e 0/1	Enable / disable the BFP function. 0 - Disable 1 - Enable
-s [service]	It means to enable different service. service - Available types are FTP, HTTP, HTTPS, TELNET, TR069, SSH, None and All.
-l [failure]	It means to set login failure retry times. failure - Available number is from 1 to 255.
-p [penalty]	It means to set penalty time for BFP. The unit is sec.
-v	It means to view current settings.

Example

```
> mngt bfp -e 1
> mngt bfp -s FTP
> mngt bfp -l 10
> mngt bfp -v
Current Brute Force Protection Setting:
* Enable: yes
* Service:
 - FTP:        yes
 - HTTP:       no
 - HTTPS:      no
 - TELNET:     no
 - TR069:      no
 - SSH:        no
* Maximum login failures: 10
* Penalty period: 0
```

Telnet Command: msubnet switch

This command is used to configure multi-subnet.

Syntax

msubnet switch *[2/3/4/5/6][On/Off]*

Syntax Description

Parameter	Description
2/3/4/5/6	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6
On/Off	On means turning on the subnet for the specified LAN interface. Off means turning off the subnet.

Example

```
> msubnet switch 2 On
% LAN2        Subnet On!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet addr

This command is used to configure IP address for the specified LAN interface.

Syntax

msubnet addr *[2~50][IP address]*

Syntax Description

Parameter	Description
2 ~50	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 ....
IP address	Type the private IP address for the specified LAN interface.

Example

```
> msubnet addr 2 192.168.5.1
% Set LAN2 subnet IP address done !!!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet nmask

This command is used to configure net mask address for the specified LAN interface.

Syntax

msubnet nmask *[2~50][IP address]*

Syntax Description

Parameter	Description
2~50	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 ....
IP address	Type the subnet mask address for the specified LAN interface.

Example

```
>  msubnet nmask 2 255.255.0.0
% Set 3/44/45/46/47/48/49/50 subnet mask done !!!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet status

This command is used to display current status of subnet.

Syntax

msubnet status *[2~50]*

Syntax Description

Parameter	Description
2~50	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 ....

Example

```
> msubnet status 2
% LAN2      Off: 0.0.0.0/0.0.0.0, PPP Start IP: 0.0.0.60
% DHCP server: Off
% Dhcp Gateway: 0.0.0.0, Start IP: 0.0.0.10, Pool Count: 50
```

Telnet Command: msubnet dhcps

This command allows you to enable or disable DHCP server for the subnet.

Syntax

msubnet dhcps *[2~50 [On/Off]*

Syntax Description

Parameter	Description
2~50	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 …………………
On/Off	On means enabling the DHCP server for the specified LAN interface. Off means disabling the DHCP server.

Example

```
> msubnet dhcps 3 off
% LAN3        Subnet DHCP Server disabled!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet nat

This command is used to configure the subnet for NAT or Routing usage.

Syntax

msubnet nat *[2~50] [On/Off]*

Syntax Description

Parameter	Description
2~50	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 ………………
On/Off	On – It means the subnet will be configured for NAT usage. Off – It means the subnet will be configured for Routing usage.

Example

```
> > msubnet nat 2 off
% LAN2 Subnet is for Routing usage!
%Note: If you have multiple WAN connections, please be reminded to setup
a Load-Balance policy so that packets from this subnet will be forwarded
to the right WAN interface!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet gateway

This command is used to configure an IP address as the gateway used for subnet.

Syntax

msubnet gateway *[2~50] [Gateway IP]*

Syntax Description

Parameter	Description
2~50	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6................
Gateway IP	Specify an IP address as the gateway IP.

Example

```
> msubnet gateway 2 192.168.1.13
% Set LAN2 Dhcp Gateway IP done !!!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet ipcnt

This command is used to defined the total number allowed for each LAN interface.

Syntax

msubnet ipcnt *[2~50] [IP counts]*

Syntax Description

Parameter	Description
2~50	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 .....
IP counts	Specify a total number of IP address allowed for each LAN interface. The available range is from 0 to 220.

Example

```
> msubnet ipcnt 2 15
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet talk

This command is used to establish a route between two LAN interfaces.

Syntax

msubnet talk *[2~50] [2~50] [On/Off]*

Syntax Description

Parameter	Description

2~50	It means LAN interface.
	1=LAN1
	2=LAN2
	3=LAN3
	4=LAN4
	5=LAN5
	6=LAN6…..
On/Off	On - It means
	Off - It means

Example

```
> msubnet talk 1 2 on
% Enable routing between LAN1       and LAN2      !

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
> msubnet talk ?
% msubnet talk <1/2/3/4/5/6> <1/2/3/4/5/6> <On/Off>
% where 1:LAN1, 2:LAN2, 3:LAN3, 4:LAN4, 5:LAN5, 6:LAN6
% Now:
%            LAN1   LAN2   LAN3   LAN4   LAN5   LAN6
% LAN1          V
% LAN2          V      V
% LAN3                        V
% LAN4                               V
% LAN5                                      V
% LAN6                                             V
...
```

Telnet Command: msubnet startip

This command is used to configure a starting IP address for DCHP.

Syntax

msubnet startip *[2~50] [Gateway IP]*

Syntax Description

Parameter	Description
2~50	It means LAN interface.
	2=LAN2
	3=LAN3
	4=LAN4
	5=LAN5
	6=LAN6 ……
Gateway IP	Type an IP address as the starting IP address for a subnet.

Example

```
> msubnet startip 2 192.168.2.90
%Set LAN2 Dhcp Start IP done !!!
```

```
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
> msubnet startip ?
% msubnet startip <2/3/4/5/6> <Gateway IP>
% Now: LAN2 192.168.2.90; LAN3 192.168.3.10; LAN4 192.168.4.10; LAN5
192.168.5.1
0; LAN6 192.168.6.10
```

Telnet Command: msubnet pppip

This command is used to configure a starting IP address for PPP connection.

Syntax

msubnet pppip *[2~50] [Start IP]*

Syntax Description

Parameter	Description
2~50	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 ……
Start IP	Type an IP address as the starting IP address for PPP connection.

Example

```
> msubnet pppip 2 192.168.2.250
% Set LAN2 PPP(IPCP) Start IP done !!!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.

> msubnet pppip ?
% msubnet pppip <2/3/4/5/6> <Start IP>
% Now: LAN2 192.168.2.250; LAN3 192.168.3.200; LAN4 192.168.4.200; LAN5
192.168.5.200; LAN6 192.168.6.200
```

Telnet Command: msubnet nodetype

This command is used to specify the type for node which is required by DHCP option.

Syntax

msubnet nodetype *[2~50][count]*

Syntax Description

Parameter	Description
2~50	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5

	6=LAN6 ……
count	Choose the following number for specifying different node type.
	1= B-node
	2= P-node
	4= M-node
	8= H-node
	0= Not specify any type for node.

Example

```
> msubnet nodetype ?
% msubnet nodetype <2/3/4/5/6> <count>
% Now: LAN2 0; LAN3 0; LAN4 0; LAN5 0; LAN6 0

% count: 1. B-node 2. P-node 4. M-node 8. H-node

>  msubnet nodetype 2 1
% Set LAN2 Dhcp Node Type done !!!

> msubnet nodetype ?
% msubnet nodetype <2/3/4/5/6> <count>
% Now: LAN2 1; LAN3 0; LAN4 0; LAN5 0; LAN6 0

% count: 1. B-node 2. P-node 4. M-node 8. H-node
```

Telnet Command: msubnet primWINS

This command is used to configure primary WINS server.

Syntax

msubnet primWINS *[2~50] [WINS IP]*

Syntax Description

Parameter	Description
2~50	It means LAN interface.
	2=LAN2
	3=LAN3
	4=LAN4
	5=LAN5
	6=LAN6 ……
WINS IP	Type the IP address as the WINS IP.

Example

```
> msubnet primWINS ?
% msubnet primWINS
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24
/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/
47/48/49/50>
<WINS IP>
% Now: 3/44/45/46/47/48/49/50 0.0.0.0; 7/48/49/50 0.0.0.0;  0.0.0.0;
```

```
0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;
0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0
> msubnet primWINS 2 192.168.3.5
DrayTek> msubnet primWINS 2 192.168.3.5
% Set 3/44/45/46/47/48/49/50 Dhcp Primary WINS IP done !!!


> msubnet primWINS ?
% msubnet primWINS
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24
/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/
47/48/49/50>
<WINS IP>
% Now: 3/44/45/46/47/48/49/50 192.168.3.5; 7/48/49/50 0.0.0.0;
0.0.0.0;  0.0.0.
0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0.
```

Telnet Command: msubnet secWINS

This command is used to configure secondary WINS server.

Syntax

msubnet secWINS *[2~50 [WINS IP]*

Syntax Description

Parameter	Description
2~50	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 ……
WINS IP	Type the IP address as the WINS IP.

Example

```
> msubnet secWINS 2 192.168.3.89
% Set 3/44/45/46/47/48/49/50 Dhcp Secondary WINS IP done !!!


> msubnet secWINS ?
DrayTek> msubnet secWINS ?
```

```
% msubnet secWINS
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/
25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/
47/48/49/50> <
WINS IP>
% Now: 3/44/45/46/47/48/49/50 192.168.3.89; 7/48/49/50 0.0.0.0;
0.0.0.0;  0.0.0
.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;  0.0.0.0;
0.0.0.0;  0.0.0
```

Telnet Command: msubnet tftp

This command is used to set TFTP server for multi-subnet.

Syntax

msubnet tftp *[2~50] [TFTP server name]*

Syntax Description

Parameter	Description
2~50	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 ……
TFTP server name	Type a name to indicate the TFTP server.

Example

```
DrayTek> msubnet tftp ?
% msubnet tftp
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/
26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/4
8/49/50> <TFTP server name>
% Now: 3/44/45/46/47/48/49/50
        7/48/49/50

DrayTek>  msubnet tftp 2 publish
% Set 3/44/45/46/47/48/49/50 TFTP Server Name done !!!

> msubnet tftp ?
DrayTek> msubnet tftp ?
% msubnet tftp
<2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23/24/25/
26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/4
8/49/50> <TFTP server name>
% Now: 3/44/45/46/47/48/49/50 publish
        7/48/49/50......
```

Telnet Command: msubnet mtu

This command allows you to configure MTU value for LAN/DMZ/IP Routed Subnet.

Syntax

msubnet mtu *[interface][value]*

Syntax Description

Parameter	Description
interface	Available settings include LAN1~LAN50, IP_Routed_Subnet.
value	1000 ~ 1508 (Bytes), default: 1500 (Bytes)

Example

```
> msubnet mtu LAN1 1492
> msubnet mtu ?
Usage:

  >msubnet mtu <interface> <value>

  <interface>: LAN1~LAN6,IP_Routed_Subnet,DMZ
  <value>:    1000 ~ 1508 (Bytes), default: 1500 (Bytes)

  e.x: >msubnet mtu LAN1 1492

Current Settings:

  LAN1 MTU:           1492 (Bytes)
  LAN2 MTU:           1500 (Bytes)
  LAN3 MTU:           1500 (Bytes)
  LAN4 MTU:           1500 (Bytes)
  LAN5 MTU:           1500 (Bytes)
  LAN6 MTU:           1500 (Bytes)
  ...
  LAN46 MTU:          1500 (Bytes)
  LAN47 MTU:          1500 (Bytes)
  LAN48 MTU:          1500 (Bytes)
  LAN49 MTU:          1500 (Bytes)
  LAN50 MTU:          1500 (Bytes)
  IP Routed Subnet MTU: 1500 (Bytes)
```

Telnet Command: msubnet leasetime

This command allows you to set leasetime for DHCP server. It is helpful to manage the IP address(es) assigned by DHCP server.

Syntax

msubnet leasetime *[1~50][Lease Time (sec.)]*

Syntax Description

Parameter	Description
1~50	1 - 50 represent LAN1 to LAN50.
Lease Time (sec.)	Range from 1 to 259200. If no value specified here, Vigor router system will use the maximum value, 259200, as the leasetime.

Example

```
> DrayTek> msubnet leasetime ?
% msubnet leasetime
<1/2/3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/20/21/22/23
/24/25/26/27/28/29/30/31/32/33/34/35/36/37/38/39/40/41/42/43/44/45/46/47/4
```

```
8/49/50> <Lease Time (sec.)>
% Now:9/40/41/42/43/44/45/46/47/48/49/50 86400; 3/44/45/46/47/48/49/50
259200; 7/48/49/50 259200; 259200; 259200; 259200; 259200; 259200;
259200; 259200; 259200; 259200; 259200; 259200; 259200; 259200;
259200; 259200; 259200; 259200; 259200; 259200; 259200; 259200;
259200; 259200; 259200; 259200; 259200; 259200; 259200; 259200;
259200; 259200; 259200; 259200; 259200; 259200; 259200; 259200;
259200; 259200; 259200; 259200; 259200; 259200; 259200; 259200;
259200; 259200
DrayTek> msubnet leasetime 1
% Set 9/40/41/42/43/44/45/46/47/48/49/50 lease time: 259200
```

Telnet Command: object ip obj

This command is used to create an IP object profile.

Syntax

object ip obj setdefault

object ip obj *INDEX -v*

object ip obj *INDEX -n NAME*

object ip obj *INDEX -i INTERFACE*

object ip obj *INDEX -s INVERT*

object ip obj 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.

Syntax

object ip grp setdefault

object ip grp *INDEX -v*

object ip grp *INDEX -n NAME*

object ip grp *INDEX -i INTERFACE*

object ip grp *INDEX -a IP_OBJ_INDEX*

Syntax Description

Parameter	Description
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 ipv6 obj

This comman is used to create an IP object profile.

Syntax

object ip obj setdefault

object ip obj *INDEX -v*

object ip obj *INDEX -n NAME*

object ip obj *INDEX -i INTERFACE*

object ip obj *INDEX -s INVERT*

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

Syntax Description

Parameter	Description
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 ipv6 grp

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

Syntax

object ip grp setdefault

object ip grp *INDEX -v*

object ip grp *INDEX -n NAME*

object ip grp *INDEX -i INTERFACE*

object ip grp *INDEX -a IP_OBJ_INDEX*

Syntax Description

Parameter	Description
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.

Syntax

object service obj setdefault

object service obj *INDEX -v*

object service obj *INDEX -n NAME*

object service obj *INDEX -p PROTOCOL*

object service obj *INDEX -s CHK [START_P] [END_P]*

object service obj *INDEX -d CHK [START_P] [END_P]*

Syntax Description

Parameter	Description
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.

Syntax

object service grp setdefault

object service grp *INDEX -v*

object service grp *INDEX -n NAME*

object service grp *INDEX -a SER_OBJ_INDEX*

Syntax Description

Parameter	Description
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.

Syntax

object kw obj setdefault

object kw obj show PAGE

object kw obj *INDEX -v*

object kw obj *INDEX -n NAME*

object kw obj *INDEX -a CONTENTS*

Syntax Description

Parameter	Description
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.

Syntax

object fe show

object fe setdefault

object fe obj *INDEX -v*

object fe obj *INDEX -n NAME*

object fe obj *INDEX -e CATEGORY|FILE_EXTENSION*

object fe obj *INDEX -d CATEGORY|FILE_EXTENSION*

Syntax Description

Parameter	Description
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, Execution 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: object sms

This command is used to create short message object profile.

Syntax

object sms show
object sms setdefault
object sms obj *INDEX -v*
object sms obj *INDEX -n NAME*
object sms obj *INDEX -s Service Provider*
object sms obj *INDEX -u Username*
object sms obj *INDEX -p Password*
object sms obj *INDEX -q Quota*
object sms obj *INDEX -i Interval*
object sms obj *INDEX -I URL*

Syntax Description

Parameter	Description
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 10) of the specified SMS object profile.
-v	It means to view the information of the specified SMS object profile.
-n [NAME]	It means to define a name for the SMS object profile. NAME: Type a name with less than 15 characters.
-s [Service Provider]	It means to specify the number of the service provider which offers the service of SMS. Different numbers represent different service provider. 0 : kotsms.com.tw (TW) 2 : textmarketer.co.uk (UK) 4 : messagemedia.co.uk (UK) 5 : bulksms.com (INT) 6 : bulksms.co.uk (UK) 7 : bulksms.2way.co.za (ZA) 8 : bulksms.com.es (ES) 9 : usa.bulksms.com (US) 10 : bulksms.de (DE) 11 : www.pswin.com (EU) 12 : www.messagebird.com (EU) 13 : www.lusosms.com (EU) 14 : www.vibeactivemedia.com (UK)
-u [Username]	It means to define a user name for the SMS object profile. Type a user name that the sender can use to register to selected SMS provider.
-p [Password]	It means to define a password for the SMS object profile. Type a password that the sender can use to register to selected SMS provider.
-q [Quota]	Enter the number of the credit that you purchase from the service provider.

	Note that one credit equals to one SMS text message on the standard route.
-I [Interval]	It means to set the sending interval for the SMS to be delivered. Enter the shortest time interval for the system to send SMS.
-l [URL]	It means to set the URL for Custom 1 and Custom 2 profiles. The profile name for Custom 1 and Custom 2 are defined in default and can not be changed.

Example

```
> object sms obj 1 -n CTC
> object sms obj 1 -n CTC
> object sms obj 1 -s 0
> object sms obj 1 -u carrie
> object sms obj 1 -p 19971125cm
> object sms obj 1 -q 2
> object sms obj 1 -i 50
> object sms obj 1 -v
Profile Index: 1
Profile Name:[CTC]
SMS Provider:[kotsms.com.tw (TW)]
Username:[carrie]
Password:[******]
Quota:[2]
Sending Interval:[50(seconds)]
```

Telnet Command: object mail

This command is used to create mail object profile.

Syntax
object mail show
object mail setdefault
object mail obj *INDEX -v*
object mail obj *INDEX -n Profile Name*
object mail obj *INDEX -s SMTP Server*
object mail obj *INDEX -l Use SSL*
object mail obj *INDEX -m SMTP Port*
object mail obj *INDEX -a Sender Address*
object mail obj *INDEX -t Authentication*
object mail obj *INDEX -u Username*
object mail obj *INDEX -p Password*
object mail obj *INDEX -i Sending Interval*

Syntax Description

Parameter	Description
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 10) of the specified mail object profile.
-v	It means to view the information of the specified mail object profile.
-n [Profile Name]	It means to define a name for the mail object profile. *Profile Name*: Type a name with less than 15 characters.
-s [SMTP Server]	It means to set the IP address of the mail server.

-l [Use SSL]	It means to use port 465 for SMTP server for some e-mail server uses https as the transmission method. 0 - disable 1 - enable to use the port number.
-m [SMTP Port]	It means to set the port number for SMTP server.
-a [Sender Address]	It means to set the e-mail address (e.g., johnwash@abc.com.tw) of the sender.
-t Authentication	The mail server must be authenticated with the correct username and password to have the right of sending message out. 0 - disable 1 - enable to use the port number.
-u Username	Type a name for authentication. The maximum length of the name you can set is 31 characters.
-p Password	Type a password for authentication. The maximum length of the password you can set is 31 characters.
-i Sending Interval	Define the interval for the system to send the SMS out. The unit is second.

Example

```
> object mail obj 1 -n buyer
> object mail obj 1 -n buyer
> object mail obj 1 -s 192.168.1.98
> object mail obj 1 -m 25
> object mail obj 1 -t 1
> object mail obj 1 -u john
> object mail obj 1 -p happy123456
> object mail obj 1 -i 25
> object mail obj 1 -v
Profile Index: 1
Profile Name:[buyer]
SMTP Server:[192.168.1.98]
SMTP Port:[25]
Sender Address:[]
Use SSL:[disable]
Authentication:[enable]
Username:[john]
Password:[******]
Sending Interval:[25(seconds)]
```

Telnet Command: object noti

This command is used to create notification object profile.

Syntax

object noti show
object noti setdefault
object noti obj *INDEX -v*
object noti obj *INDEX -n Profile Name*
object mail obj *INDEX -e Category Status*
object mail obj *INDEX -d Category Status*

Syntax Description

Parameter	Description
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 notification object profile.
-v	It means to view the information of the specified notification object profile.
-n [Profile Name]	It means to define a name for the notification object profile. *Profile Name*: Type a name with less than 15 characters.
-e	It means to enable the status of specified category.
-d	It means to disable the status of specified category.
[Category]	Available categories are: 1: WAN; 2: VPN Tunnel; 3: Temperature Alert; 4: WAN Budget; 5: CVM; 6: High Availability
[status]	For WAN – 1: Disconnected; 2: Reconnected. For VPN Tunnel - 1: Disconnected; 2: Reconnected. For Temperature Alert - 1: Out of Range. For WAN Budget - 1: Limit Reached. For CVM - 1: CPE Offline; 2: Backup Fail; 3: Restore Fail; 4: FW Update Fail; 5: VPN Profile Setup Fail. For High Availability - 1: Failover Occurred, Config Sync Fail, and Router Unstable

Example

```
> object noti obj 1 –n markbei
> object noti obj 1 -e 1 1
> object noti obj 1 -e 2 1
> object noti obj 1 -e 5 3
> object noti obj 1 -v
> object noti obj 1 -e 1 1
> object noti obj 1 -e 2 1
> object noti obj 1 -e 5 3
> object noti obj 1 -v
Profile Index: 1
Profile Name:[]
    Category                  Status
  WAN                [v]Disconnected     [ ]Reconnected
  VPN Tunnel         [v]Disconnected     [ ]Reconnected
  Temperature Alert [ ]Out of Range
  WAN Budget Alert   [ ]Limit Reached
  CVM Alert          [ ]CPE Offline
                     [ ]CPE Config Backup Fail
                     [v]CPE Config Restore Fail
                     [ ]CPE Firmware Fpgrade Fail
                     [ ]CPE VPN Profile Setup Fail
  High Availability  [ ]Failover Occurred
                        Config Sync Fail
                        Router Unstable
```

Telnet Command: object schedule

This command is used to create schedule object profile.

Syntax
object schedule set *INDEX option*
object schedule view
object schedule setdefault

Syntax Description

Parameter	Description
set	It means to set the schedule profile.
[INDEX]	It means the index number (from 1 to 15) of the specified object profile.
option	Available options for schedule includes: -e
-e [value]	It means to enable the schedule setup. 0 – disable 1 – enable
-c [comment]	It means to set brief description for the specified profile. The length range of the comment: 1 ~ 32 characters.
-D [year][month][day]	It means to set the starting date of the profile. [year] – Must be between 2000-2049. [month] - Must be between 1-12. [day] - Must be between 1-31. For example: To set Start Date 2015/10/6, type *> object schedule set 1 -D "2015 10 6"*
-T [hour][minute]	It means to set the starting time of the profile. [hour] - Must be between 0-23. [minute] - Must be between 0-59. For example: To set Start Time 10:20, type *> object schedule set 1 -T "10 20"*
-d [hour][minute]	It means to set the duration time of the profile. [hour] - Must be between 0-23. [minute] - Must be between 0-59. For example: To set Duration Time 3:30, type *> object schedule set 1 -d "3 30"*
-a [value]	It means to set the action used for the profile. [value] – 0:Force On, 1:Force Down, 2:Enable Dial-On-Demand, 3:Disable Dial-On-Demand
-l [value]	It means to set idle time. [value] – Must be between 0-255(minute). The default is 0.
-h [option] [day]	Set how often the schedule will be applied. [option] – 0: Once, 1: Weekdays [day] – Sun, Mon, Tue, Wed, Thu, Fri, Sat If the [option] set Weekdays, then must select which days of Week. example: To select Sunday, Monday, Thursday, type *> object schedule set 1 -h "1 Sun Mon Thu"*

view [INDEX]	It means to show the content of the profile.
setdefault	It means to return to default settings for all profiles.

Example

```
> object schedule set 1 –e 1
> object schedule set 1 –c Working
> object schedule set 1 –D "2016 11 8"
> object schedule set 1 –T "8 1"
> object schedule set 1 –d "2 30"
> object schedule set 1 –a 0
> object schedule set 1 –h "1 Mon Wed"
> object schedule view 1
Index No.1

---------------------------------------------------
[v] Enable Schedule Setup
      Comment [ Working ]
      Start Date (yyyy-mm-dd) [ 2016 ]-[ 11 ]-[  8 ]
      Start Time (hh:mm)      [ 8 ]:[  1 ]
      Duration Time (hh:mm)   [  2 ]:[ 30 ]
      Action                  [ Force On ]
      Idle Timeout            [ 0 ] minute(s).(max. 255, 0 for
                              default)
      ----------------------------------------------------------------
      How Often
       [ ] Once
       [v] Weekdays
          [ ]Sun  [v]Mon  [ ]Tue  [v]Wed  [ ]Thu  [ ]Fri  [ ]Sat
>
```

Telnet Command: port

This command allows users to set the speed for specific port of the router.

Syntax

port *[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, all][AN, 100F, 100H, 10F, 10H, status]*

port status

port jumbo

port wanfc

Syntax Description

Parameter	Description
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, all	It means the number of LAN port and WAN port.
AN… 10H	It means the physical type for the specific port. AN: auto-negotiate. 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.

Syntax

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: prn

This command allows you to view current status (interface and driver) of USB printer.

Syntax

prn status

Example

```
> prn status ?
Interface: USB bus 2.0
Printer: READY
Connect speed: 0K bps
Status: (null)
Info: (null)


VR9 USB host : USB1: READY , USB2: READY
```

Telnet Command: qos setup

This command allows user to set general settings for QoS.

Syntax

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

Syntax Description

Parameter	Description
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-h	Type it to display the usage of this command.
-m <mode>	It means to define which traffic the QoS control settings will apply to and 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.

Syntax

qos class -c *[no] -[a|e|d] [no][-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
[<command> <parameter>|...]	The available commands with parameters are listed below. *[...]* means that you can type in several commands in one line.
-h	Type it to display the usage of this command.
-c <no>	Specify the inde number for the class. Available value for <no> contains 1, 2 and 3. The default setting is class 1.
-n <name>	It means to type a name for the class.
-a	It means to add rule for specified class.
-e <no>	It means to edit specified rule. <no>: type the index number for the rule.
-d <no>	It means to delete specified rule. <no>: type the index number for the rule.
-m <mode>	It means to enable or disable the specified rule. 0: disable, 1: enable
-l <addr>	Set the local address. *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 "-*I*" to specify any address for this command.
-p <DSCP id>	Specify the ID.
-s <Service type>	Specify the service type by typing the number. The available types are listed as below: 1:ANY 2:DNS 3:FTP 4:GRE 5:H.323 6:HTTP 7:HTTPS 8:IKE 9:IPSEC-AH 10:IPSEC-ESP 11:IRC 12:L2TP 13:NEWS 14:NFS 15:NNTP 16:PING 17:POP3 18:PPTP 19:REAL-AUDIO 20:RTSP 21:SFTP 22:SIP 23:SMTP 24:SNMP 25:SNMP-TRAPS 26:SQL-NET 27:SSH 28:SYSLOG 29:TELNET 30:TFTP
-S <d/s>	Show the content for specified DSCP ID/Service type.
-V <1/2/3>	Show the rule in the specified class.
[…]	It means that you can type in several commands in one line.

Example

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

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

Telnet Command: qos type

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

Syntax

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

Syntax Description

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

Example

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

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

Telnet Command: quit

This command can exit the telnet command screen.

Telnet Command: show lan

This command displays current status of LAN IP address settings.

Example

```
> show lan
The LAN settings:
        ip            mask       dhcp star_ip          pool  gateway
-------------------------------------------------------------------------
-----
[V]LAN1 192.168.1.1   255.255.255.0  [V]  192.168.1.10     200
192.168.1.1
[X]LAN2 192.168.2.1   255.255.255.0  [V]  192.168.2.10     100
192.168.2.1
[X]LAN3 192.168.3.1   255.255.255.0  [V]  192.168.3.10     100
192.168.3.1
[X]LAN4 192.168.4.1   255.255.255.0  [V]  192.168.4.10     100
192.168.4.1
[X]LAN5 192.168.5.1   255.255.255.0  [V]  192.168.5.10     100
192.168.5.1
[X]LAN6 192.168.6.1   255.255.255.0  [V]  192.168.6.10     100
192.168.6.1
[X]Route 192.168.0.1  255.255.255.0  [V]  0.0.0.0     0 192.168.0.1
```

Telnet Command: show dmz

This command displays current status of DMZ host.

Example

```
> show dmz
%     WAN1 DMZ mapping status:
 Index  Status  WAN1 aux IP     Private IP
----------------------------------------------------
   1    Disable 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 statistic

This command displays statistics for WAN interface.

Syntax

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 public

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

Syntax

srv dhcp public *start [IP address]*

srv dhcp public *cnt [IP counts]*

srv dhcp public *status*

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

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

Syntax Description

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

Example

```
Vigor> ip route add 192.168.1.56 255.255.255.0 192.168.1.12 3 default
Vigor> srv dhcp public status
Index   MAC Address
```

Telnet Command: srv dhcp dns1

This command allows users to set Primary IP Address for DNS Server in LAN.

Syntax

srv dhcp dns1 *[?]*

srv dhcp dns1 *[DNS IP address]*

Syntax Description

Parameter	Description
?	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.

Syntax

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.

Syntax

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.

Syntax

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.

Syntax

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.

Syntax

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

Syntax

srv dhcp startip *[?]*

srv dhcp startip *[IP address]*

Syntax Description

Parameter	Description
?	It means to display current used start IP address.
IP address	It means the IP address that you can specify for the DHCP server as the starting point.

Example

```
> srv dhcp startip 192.168.1.53
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: srv dhcp status

This command can display general information for the DHCP server, such as IP address, MAC address, leased time, host ID and so on.

Example

```
> srv dhcp status
DHCP server: Relay Agent
Default gateway: 192.168.1.1
Index    IP Address     MAC Address          Leased Time    HOST ID
1       192.168.1.113  00-05-5D-E4-D8-EE     17:20:08       A1000351
```

Telnet Command: srv dhcp leasetime

This command can set the lease time for the DHCP server.

Syntax

srv dhcp leasetime *[?]*

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

Syntax Description

Parameter	Description
?	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.

Syntax

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.

Syntax

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.

Syntax

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.

Syntax

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.

Syntax

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.

Syntax

srv dhcp option *-h*

srv dhcp option *-l*

srv dhcp option *-d [idx]*

srv dhcp option *-e [1 or 0] -c [option number] -v [option value]*

srv dhcp option *-e [1 or 0] -c [option number] -a [option value]*

srv dhcp option *-e [1 or 0] -c [option number] -x [option value]*

srv dhcp option *-u [idx 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.

Syntax

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

Syntax Description

Parameter	Description
n	It means to map selected WAN IP to certain host.
	1: wan1
	2: wan2
m	It means the index number of the DMZ host.
	Default setting is "1" (WAN 1). It is only available for Static IP mode. If you use other mode, you can set 1 ~ 8 in this field. If WAN IP alias has been configured, then the number of DMZ host can be added more.
[<command> <parameter>|...]	The available commands with parameters are listed below.
	[...] means that you can type in several commands in one line.
-e	It means to enable/disable such feature.
	1:enable
	0:disable
-i	It means to specify the private IP address of the DMZ host.
-r	It means to remove DMZ host setting.
-v	It means to display current status.

Example

```
> srv nat dmz 1 1 -i 192.168.1.96
> srv nat dmz -v
%     WAN1 DMZ mapping status:
 Index  Status  WAN1 aux IP     Private IP
-----------------------------------------------------
   1    Disable 0.0.0.0 192.168.1.96
```

Telnet Command: srv nat ipsecpass

This command allows users to enable or disable IPSec ESP tunnel passthrough and IKE source port (500) preservation.

Syntax

Srv nat ipsecpass *[options]*

Syntax Description

Parameter	Description
[options]	The available commands with parameters are listed below.
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.

Syntax

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.

Syntax

srv nat portmap *add [idx][serv name][proto][pub port][pri ip][pri port][wan1/wan2]*

srv nat portmap *del [idx]*

srv nat portmap *disable [idx]*

srv nat portmap *enable [idx] [proto]*

srv nat portmap *flush*

srv nat portmap *table*

Syntax Description

Parameter	Description
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: switch -i

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

Syntax

switch -i *[switch idx_no] [option]*

Syntax Description

Parameter	Description
switch idx_no	It means the index number of the switch profile.
option	The available commands with parameters are listed below. *cmd* *acc* *traffic [on/off/status/tx/rx]*

cmd	It means to send command to the client.
acc	It means to set the client authentication account and password.
traffic *[on/off/status/tx/rx]*	It means to turn on/off or display the data transmission from the client.

Example

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

Telnet Command: switch on

This command is used to turn on the auto discovery for external devices.

Example

```
>  switch on
Enable Extrnal Device auto discovery!
```

Telnet Command: switch off

This command is used to turn off the auto discovery for external devices.

Example

```
>  switch off
Disable External Device auto discovery!
```

Telnet Command: switch list

This command is used to display the connection status of the switch.

Example

```
> switch list?
No.     Mac             IP          status  Dur Time   Model_Name
--------------------------------------------------------------------
---------
[1]  00-50-7f-cd-07-48  192.168.1.3    On-Line   00:01:01
Vigor2920 Series
```

Telnet Command: switch clear

This command is used to reset the switch table and reboot the router.

Syntax

switch clear *[idx]*

Syntax Description

Parameter	Description
idx	It means the index number of each item shown on the table. The range is from 1 to 8.
-f	It means to clear all of the data.

Example

```
> switch clear 1
Switch Data clear successful

> switch clear -f
Switch Data clear successful
```

Telnet Command: switch query

This command is used to enable or disable the switch query.

Example

```
> switch query on
Extern Device status query is Enable
> switch query off
Extern Device status query is Disable
```

Telnet Command: sys admin

This command is used for RD engineer to access into test mode of Vigor router.

Telnet Command: sys adminuser

This command is used to create user account and specify LDAP server. The server will authenticate the local user who wants to access into the web user interface of Vigor router.

Syntax

sys adminuser *[option]*

sys adminuser edit *[index] username password*

Syntax Description

Parameter	Description
option	Available options includes: Local [0-1] LDAP [0-1] edit [INDEX] delete [INDEX] view [INDEX]
Local [0-1]	0 - Disable the local user. 1 - Enable the local user.
LDAP [0-1]	0 - Disable the LDAP. 1 - Enable the LDAP.
edit [INDEX] username password	Edit an existed user account or create a new local user account. [INDEX] - 1 ~8. There are eight profiles to be added / edited. Username - Type a new name for local user. Password - Type a password for local user.
delete [INDEX]	Delete a local user account.
view [INDEX]	Show the user account/password detail information.

Example

```
> sys adminuser Local 1
Local User has enabled!
```

```
> sys adminuser LDAP 1
LDAP has enabled!
> sys adminuser edit 1 carrie test123
Updated!
> sys adminuser view 1


Index:1
User Name:carrie
User Password:test123
```

Telnet Command: sys bonjour

This command is used to disable/enable and configure the Bonjour service.

Syntax

sys bonjour *[-<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 <enable>	It is used to disable/enable bonjour service (0: disable, 1: enable).
-h <enable>	It is used to disable/enable http (web) service (0: disable, 1: enable).
-t <enable>	It is used to disable/enable telnet service (0: disable, 1: enable).
-f <enable>	It is used to disable/enable FTP service (0: disable, 1: enable).
-s <enable>	It is used to disable/enable SSH service (0: disable, 1: enable).
-p <enable>	It is used to disable/enable printer service (0: disable, 1: enable).
-6 <enable>	It is used to disable/enable IPv6 (0: disable, 1: enable).

Example

```
> sys bonjour -s 1
>
```

Telnet Command: sys cfg

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

Syntax

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.

Syntax

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.

Syntax

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

sys domainname *[wan1/wan2] clear*

Syntax Description

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

Syntax

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.

Syntax

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.

Syntax

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 country code and wireless region of this device.

Example

```
> sys cc
Country Code      : 0x 0 [International]
Wireless Region Code: 0x30
>
```

Telnet Command: sys version

This command can display current version for the system.

Example

```
> sys version
Router Model: Vigor3910Vn+   Version: 3.7.4.1 English
Profile version: 3.0.0   Status: 1 (0x49165e6c)
Router IP: 192.168.1.1   Netmask: 255.255.255.0
Firmware Build Date/Time: Mar 20 2014 14:09:50
Router Name: drayrouter
Revision: 40055 2860_374
VDSL2 Firmware Version: 05-04-08-00-00-06
```

Telnet Command: sys qrybuf

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

Example

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

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

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

Telnet Command: sys pollbuf

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

Syntax

sys pollbuf *[on]*

sys pollbuf *[off]*

Syntax Description

Parameter	Description
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 tr069

This command can set CPE settings for applying in VigorACS.

Syntax

sys tr069 get *[parm] [option]*

sys tr069 set *[parm] [value]*

sys tr069 getnoti *[parm]*

sys tr069 setnoti *[parm] [value]*

sys tr069 log

sys tr069 debug *[on/off]*

sys tr069 save

sys tr069 inform *[event code]*

sys tr069 port *[port num]*

sys tr069 cert_auth *[on/off]*

Syntax Description

Parameter	Description
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.

Syntax

sys sip_alg *[1]*

sys sip_alg *[0]*

Syntax Description

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

Example

```
> sys sip_alg ?
```

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

Telnet Command: sys license

This command can process the system license.

Syntax

sys license *licmsg*

sys license *licauth*

sys license *regser*

sys license *licera*

sys license *licifno*

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

sys license *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: testmail

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

Example

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

Telnet Command: upnp off

This command can close UPnP function.

Example

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

Telnet Command: upnp on

This command can enable UPnP function.

Example

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

Telnet Command: upnp nat

This command can display IGD NAT status.

Example

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

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

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

Telnet Command: upnp service

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

Example

```
> upnp on
UPNP start.

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

>>>>> SERVICE TABLE2 <<<<<
  serviceType
urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1
  serviceId   urn:upnp-org:serviceId:WANCommonIFC1
  SCPDURL     /upnp/WComIFCX.xml
  controlURL  /upnp?control=WANCommonIFC1
  eventURL    /upnp?event=WANCommonIFC1
  UDN         uuid:2608d902-03e2-46a5-9968-4a54ca499148
.
.
.
```

Telnet Command: upnp subscribe

This command can show all UPnP services subscribed.

Example

```
> upnp on
UPNP start.
> upnp subscribe
Vigor> upnp subscribe
>>>> (1) serviceType urn:schemas-microsoft-com:service:OSInfo:1

  ----- Subscribtion1 -------

    sid = 7a2bbdd0-0047-4fc8-b870-4597b34da7fb

    eventKey =1, ToSendEventKey = 1

    expireTime =6926

    active =1

    DeliveryURLs
=<http://192.168.1.113:2869/upnp/eventing/twtnpnsiun>
```

```
>>>> (2) serviceType
urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1

  ----- Subscribtion1 -------

    sid = d9cd47a5-d9c9-4d3d-8043-d03a82f27983

    eventKey =1, ToSendEventKey = 1
.
.
.
```

Telnet Command: upnp tmpvs

This command can display current status of temp Virtual Server of your router.

Example

```
Vigor> upnp tmpvs
*****************  Temp virtual server status  ***************

((0))
real_addr  >>192.168.1.10<<, pseudo_addr >>172.16.3.229<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>TCP<<
time >>0<<

((1))
real_addr  >>0.0.0.0<<, pseudo_addr >>0.0.0.0<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>0<<
time >>0<<
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
```

Telnet Command: upnp wan

This command is used to specify WAN interface to apply UPnP.

Syntax

upnp wan *[n]*

Syntax Description

Parameter	Description
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

Vigor3910 Series User's Guide

```
> upnp wan 1
use wan1 now.
```

Telnet Command: usb list

This command is use to display the information about the brand name and model name of the USB modems which are supported by Vigor router.

Example

```
> usb list ?
Brand        Module              Standard
-----------------------          --------
Aiko         Aiko 83D            3.5G               Y
BandRich     Bandluxe C170       3.5G                Y
BandRich     Bandluxe C270       3.5G                Y
BandRich     Bandluxe C321       3.5G                Y
BandRich     Bandluxe C330       3.5G                Y
BandRich     Bandluxe C331       3.5G                Y
BandRich     Bandluxe C502       3.5G                Y
Huawei       Huawei E169u        3.5G               Y
Huawei       Huawei E220         3.5G               Y
Huawei       Huawei E303D        3.5G               Y
Huawei       Huawei E392         3.5G               Y
Huawei       Huawei E398         3.5G               Y
Sony Erics   Sony Ericsson MD30   3.5G                Y
TP-LINK      TP-LINK MA180       3.5G               Y
TP-LINK      TP-LINK MA260       3.5G               Y
Vodafone     Vodafone K3765-Z    3.5G                Y
Vodafone     Vodafone K4605      3.5G                Y
ZTE          ZTE MF626           3.5G               Y
ZTE          ZTE MF627 plus      3.5G                Y
ZTE          ZTE MF633           3.5G               Y
ZTE          ZTE MF636           3.5G               Y


SpinCom      SpinCom GPRS Modem   3.5G                Y
- MORE - ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] -
```

Telnet Command: 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.

Syntax

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: vpn l2lset

This command allows users to set advanced parameters for LAN to LAN function.

Syntax

vpn l2lset *[list index]* **peerid** *[peerid]*

vpn l2lset *[list index]* **localid** *[localid]*

vpn l2lset *[list index]***main** *[auto/proposal index]*

vpn l2lset *[list index]* **aggressive** *[g1/g2]*

vpn l2lset *[list index]***pfs** *[on/off]*

vpn l2lset *[list index]* **phase***1[lifetime]*

vpn l2lset *[list index]* **phase2***[lifetime]*

Syntax Description

Parameter	Description
list index	It means the index number of L2L (LAN to LAN) profile.
peerid	It means the peer identity for aggressive mode.
localid	It means the local identity for aggressive mode.
main	It means to choose proposal for main mode.
auto index	It means to choose default proposals.
proposal index	It means to choose specified proposal.
aggressive	It means the chosen DH group for aggressive mode
pfs	It means "perfect forward secrete".
on/off	It means to turn on or off the PFS function.
phase1	It means phase 1 of IKE.
lifetime	It means the lifetime value (in second) for phase 1 and phase 2.
phase2	It means phase 2 of IKE.

Example

```
> VPN l2lset 1 peerid 10226
```

Telnet Command: vpn l2lDrop

This command allows users to terminate current LAN to LAN VPN connection.

Example

```
> vpn l2lDrop
>
```

Telnet Command: vpn dinset

This command allows users to configure setting for remote dial-in VPN profile.

Syntax

vpn dinset *<list index>*

vpn dinset *<list index>* *<on/off>*

vpn dinset *<list index>* **motp** *<on/off>*

vpn dinset *<list index>* **pin_secret** *<pin>* *<secret>*

Syntax Description

Parameter	Description
<list index>	It means the index number of the profile.
<on/off>	It means to enable or disable the profile. on – Enable. off – Disable.
motp <on/off>	It means to enable or disable the authentication with mOTP function. on – Enable. off – Disable.
pin_secret<pin> <secret>	It means to set PIN code with secret. *<pin>* - Type the code for authentication (e.g, 1234). *<secret>* - Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6)

Example

```
> vpn dinset 1

Dial-in profile index 1

Profile Name: ???
Status: Deactive

Mobile OTP: Disabled

Password:

Idle Timeout: 300 sec
```

```
> vpn dinset 1 on
% set profile active

> vpn dinset 1 motp on
% Enable Mobile OTP mode!>
> vpn dinset 1 pin_secret 1234 e759bb6f0e94c7ab4fe6
> vpn dinset 1

Dial-in profile index 1

Profile Name: ???
Status: Active

Mobile OTP: Enabled

PIN: 1234

Secret: e759bb6f0e94c7ab4fe6

Idle Timeout: 300 sec
```

Telnet Command: vpn subnet

This command allows users to specify a subnet selection for the specified remote dial-in VPN profile.

Syntax

vpn subnet *[index] [1/2/3/4/5/6]*

Syntax Description

Parameter	Description
<index>	It means the index number of the VPN profile.
<1/2/3/4/5/6>	1 - it means LAN1 2 - it means LAN2. 3 - it means LAN3 4 - it means LAN4. 5 - it means LAN51 6 - it means LAN6.

Example

```
> vpn subnet 1 2
>
```

Telnet Command: vpn setup

This command allows users to setup VPN for different types.

Syntax

Command of PPTP Dial-Out

  vpn setup *<index> <name>* **pptp_out** *<ip> <usr> <pwd> <nip> <nmask>*

Command of IPSec Dial-Out

   vpn setup *<index> <name>* **ipsec_out** *<ip> <key> <nip> <nmask>*

Command of L2Tp Dial-Out

   vpn setup *<index> <name>* **l2tp_out** *<ip> <usr> <pwd> <nip> <nmask>*

Command of Dial-In

   vpn setup *<index> <name>* **dialin** *<ip> <usr> <pwd> <key> <nip> <nmask>*

Syntax Description

Parameter	Description
For PPTP Dial-Out	
<index>	It means the index number of the profile.
<name>	It means the name of the profile.
<ip>	It means the IP address to dial to.
<usr> <pwd>	It means the user and the password required for the PPTP connection.
<nip> <nmask>	It means the remote network IP and the mask. e.g., vpn setup 1 name1 pptp_out 1.2.3.4 vigor 1234 192.168.1.0 255.255.255.0
For IPsec Dial-Out	
<index>	It means the index number of the profile.
<name>	It means the name of the profile.
<ip>	It means the IP address to dial to.
<key>	It means the value of IPsec Pre-Shared Key.
<nip> <nmask>	It means the remote network IP and the mask. e.g., vpn setup 1 name1 ipsec_out 1.2.3.4 1234 192.168.1.0 255.255.255.0
For L2TP Dial-Out	
<index>	It means the index number of the profile.
<name>	It means the name of the profile.
<ip>	It means the IP address to dial to.
<usr> <pwd>	It means the user and the password required for the L2TP connection.
<nip> <nmask>	It means the remote network IP and the mask. e.g.,, vpn setup 1 name1 l2tp_out 1.2.3.4 vigor 1234 192.168.1.0 255.255.255.0
For Dial-In	
<index>	It means the index number of the profile.
<name>	It means the name of the profile.
<ip>	It means the IP address allowed to dial in.
<usr> <pwd>	It means the user and the password required for the PPTP/L2TP connection.
<key>	It means the value of IPsec Pre-Shared Key.

<nip> <nmask>	It means the remote network IP and the mask.
	e.g.,
	vpn setup 1 name1 dialin 1.2.3.4 vigor 1234 abc 192.168.1.0 255.255.255.0

Example

```
> vpn setup 1 name1 dialin 1.2.3.4 vigor 1234 abc 192.168.1.0
255.255.255.0
% Profile Change Log ...

% Profile Index : 1
% Profile Name : name1
% Username : vigor
% Password : 1234
% Pre-share Key : abc
% Call Direction : Dial-In
% Type of Server :  ISDN PPTP IPSec L2TP
% Dial from : 1.2.3.4
% Remote NEtwork IP : 192.168.1.0
% Remote NEtwork Mask : 255.255.255.0
>
```

Telnet Command: vpn option

This command allows users to configure settings for LAN to LAN profile.

Syntax

vpn option *<index> <cmd1>=<param1> [<cmd2>=<para2> | ...]*

Syntax Description

Parameter	Description
<index>	It means the index number of the profile.
	Available index numbers:
	1 ~ 32
For Common Settings	
<index>	It means the index number of the profile.
pname	It means the name of the profile.
ena	It means to enable or disable the profile.
	on – Enable
	off - Disable
thr	It means the way that VPN connection passes through. Available settings are w1f, w1o, w2f, and w2o.
	w1f – WAN1 First.
	w1o – WAN1 Only.
	w2f – WAN2 First.
	w2o – WAN2 Only.
nnpkt	It means the NetBios Naming Packet.
	on – Enable the function to pass the packet.
	off – Disable the function to block the packet.

dir	It means the call direction. Available settings are b, o and i. b – Both o – Dial-Out i – Dial-In.
idle=[value]	It means Always on and Idle Time out. Available values include: -1 – it means always on for dial-out. 0 – it means always on for dial-in. Other numbers (e.g., idle=200, idle=300, idle=500) mean the router will be idle after the interval (seconds) configured here.
palive	It means to enable PING to keep alive. -1 – disable the function. 1,2,3,4 – Enable the function and PING IP 1.2.3.4 to keep alive.
For Dial-Out Settings	
ctype	It means "Type of Server I am calling". "ctype=t" means PPTP. "ctype=s" means IPSec. "ctype= l" means L2TP(IPSec Policy None). "ctype= l1" means L2TP(IPSec Policy Nice to Have). "ctype= l2" means L2TP(IPSec Policy Must).
dialto	It means Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89).
ltype	It means Link Type. "ltype=0" means "Disable". "ltype=1" means "64kbps". "ltype=2" means "128kbps". "ltype=3" means "BOD".
oname	It means Dial-Out Username. "oname=admin" means to set Username = admin.
opwd	It means Dial-Out Password "opwd=1234" means to set Password = 1234.
pauth	It means PPP Authentication. "pauth=pc" means to set PPP Authentication = PAP&CHAP. "pauth=p" means to set PPP Authentication = PAP Only
ovj	It means VJ Compression. "ovj=on/off" means to enable/disable VJ Compression.
okey	It means IKE Pre-Shared Key. "okey=abcd" means to set IKE Pre-Shared Key = abcd.
ometh	It means IPSec Security Method. "ometh=ah/" means AH. "ometh=espd/espda/" means ESP DES without/with Authentication. "ometh=esp3/esp3a/" means ESP 3DES without/with Authentication. "ometh=espa/espaa" means ESP AES without/with Authentication.
sch	It means Index(1-15) in Schedule Setup. sch=1,3,5,7 Set schedule 1->3->5->7
rcallb	It means Require Remote to Callback. "rcallb=on/off" means to enable/disable Set Require Remote to Callback.

ikeid	It means IKE Local ID. "ikeid=vigor" means Set Local ID = vigor.
For Dial-In Settings	
itype	It means Allowed Dial-In Type. Available settings include: "itype=t" means PPTP. "itype=s" means IPSec. "itype=L1"means L2TP (None). "itype=L1" means L2TP(Nice to Have). "itype=l2" means L2TP(Must).
peer	It means specify Peer VPN Server IP for Remote VPN Gateway. Type "203.12.23.48" means to allow VPN dial-in with IP address of 203.12.23.48. Type "off" means any remote IP is allowed to dial in.
peerid	It means the peer ID for Remote VPN Gateway. Type "draytek" means the word is used as local ID.
iname	It means Dial-in Username. "iname=admin" means to set username as "admin".
ipwd	It means Dial-in Password. "ipwd=1234" means to set password as "1234".
ivj	It means VJ Compression. "ivj=on/off" means to enable /disable VJ Compression.
ikey	It means IKE Pre-Shared Key. "ikey=abcd" means to set IKE Pre-Shared Key = abcd.
imeth	It means IPSec Security Method "imeth=h" means "Allow AH". "imeth=d" means "Allow DES". "imeth=3" means "Allow 3DES". "imeth=a" means "Allow AES.
For TCP/IP Settings	
mywip	It means My WAN IP. "mywip=1.2.3.4" means to set My WAN IP as "1.2.3.4".
rgip	It means Remote Gateway IP. "rgip=1.2.3.4" means to set Remote Gateway IP as "1.2.3.4".
rnip	It means Remote Network IP. "rnip=1.2.3.0" means to set Remote Network IP as "1.2.3.0".
rnmask	It means Remote Network Mask. "rnmask=255.255.255.0" means to set Remote Network Mask as "255.255.255.0".
rip	It means RIP Direction. "rip=d" means to set RIP Direction as "Disable". "rip=t" means to set RIP Direction as "TX". "rip=r" means to set RIP Direction as "RX". "rip=b" means to set RIP Direction as "Both".
mode	It means the option of "From first subnet to remote network, you have to do". "mode=r" means to set Route mode. "mode=n" means to set NAT mode.
droute	It means to Change default route to this VPN tunnel (Only single

	WAN supports this).
	droute=on/off means to enable/disable the function.

Example

```
> vpn option 1 idle=250
% Change Log..

% Idle Timeout = 250
```

Telnet Command: vpn mroute

This command allows users to list, add or delete static routes for a certain LAN to LAN VPN profile.

Syntax

vpn mroute *<index>* **list**

vpn mroute *<index>* **add** *<network ip>/<mask>*

vpn mroute *<index>* **del** *<network ip>/<mask>*

Syntax Description

Parameter	Description
list	It means to display all of the route settings.
add	It means to add a new route.
del	It means to delete specified route.
<index>	It means the index number of the profile. Available index numbers: 1 ~ 32
<network ip>/<mask>	Type the IP address with the network mask address.

Example

```
> vpn mroute 1 add 192.168.5.0/24
% 192.168.5.0/24
% Add new route 192.168.5.0/24 to profile 1
```

Telnet Command: vpn list

This command allows users to view LAN to LAN VPN profiles.

Syntax

vpn list *<index>* **all**

vpn list *<index>***com**

vpn list*<index>***out**

vpn list *<index>* **in**

vpn list*<index>***net**

Syntax Description

Parameter	Description

all	It means to list configuration of the specified profile.
com	It means to list common settings of the specified profile.
out	It means to list dial-out settings of the specified profile.
in	It means to list dial-in settings of the specified profile.
net	It means to list Network Settings of the specified profile.
<index>	It means the index number of the profile. Available index numbers: 1 ~ 32

Example

```
> vpn list 32 all
% Common Settings

% Profile Name          : ???
% Profile Status        : Disable
% Netbios Naming Packet  : Pass
% Call Direction        : Both
% Idle Timeout          : 300
% PING to keep alive    : off


% Dial-out Settings

% Type of Server        : PPTP
% Link Type:            : 64k bps
% Username              : ???
% Password              :
% PPP Authentication    : PAP/CHAP
% VJ Compression        : on
% Pre-Shared Key        :
% IPSec Security Method : AH
% Schedule              : 0,0,0,0
% Remote Callback       : off
% Provide ISDN Number   : off
% IKE phase 1 mode      : Main mode
% IKE Local ID          :



% Dial-In Settings

--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
> vpn list 1 com
% Common Settings

% Profile Name          : ???
% Profile Status        : Disable
% Netbios Naming Packet : Pass
% Call Direction        : Both
% Idle Timeout          : 300
% PING to keep alive    : off
>
```

Telnet Command: vpn remote

This command allows users to enable or disable *PPTP/IPSec/L2TP* VPN service.

Syntax

vpn remote *[PPTP/IPSec/L2TP] [on/off]*

Syntax Description

Parameter	Description
PPTP/IPSec/L2TP	There are four types to be selected.
on/off	on - enable VPN remote setting. off - disable VPN remote setting.

Example

```
> vpn remote PPTP on
Set PPTP VPN Service : On

Please restart the router!!
```

Telnet Command: vpn NetBios

This command allows users to enable or disable NetBios for Remote Access User Accounts or LAN-to-LAN Profile.

Syntax

vpn NetBios set *<H2I/L2I> <index> <Block/Pass>*

Syntax Description

Parameter	Description
<H2I/L2I>	H2I means Remote Access User Accounts. L2I means LAN-to-LAN Profile. Specify which one will be applied by NetBios.
<index>	The index number of the profile.
<Block/Pass>	**Pass** - Have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. **Block** - When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, set it block data transmission of Netbios Naming Packet inside the tunnel.

Example

```
> vpn NetBios set H2l 1 Pass
% Remote Dial In Profile Index [1] :
% NetBios Block/Pass: [PASS]
```

Telnet Command: vpn mss

This command allows users to configure the maximum segment size (MSS) for different TCP types.

Syntax

vpn mss show

vpn mss default

vpn mss set *<connection type> <TCP maximum segment size range>*

Syntax Description

Parameter	Description
show	It means to display current setting status.
default	TCP maximum segment size for all the VPN connection will be set as 1360 bytes.
set	Use it to specify the connection type and value of MSS.
<connection type>	1~4 represent various type. 1 - PPTP 2 - L2TP 3 - IPSec 4 - L2TP over IPSec
<TCP maximum segment size range>	Each type has different segment size range. PPTP - 1 ~ 1412 L2TP - 1 ~ 1408 IPSec - 1 ~ 1381 L2TP over IPSec - 1 ~ 1361

Example

```
>vpn mss set 1 1400
% VPN TCP maximum segment size (MSS) :
  PPTP  = 1400
  L2TP  = 1360
  IPSec = 1360
  L2TP over IPSec  = 1360
>vpn mss show
 VPN TCP maximum segment size (MSS) :
 PPTP  = 1400
 L2TP  = 1360
 IPSec = 1360
 L2TP over IPSec  = 1360
```

Telnet Command: vpn ike

This command is used to display IKE memory status and leakage list.

Syntax

vpn ike -q

Example

```
> vpn ike -q
IKE Memory Status and Leakage List

# of free L-Buffer=95, minimum=94, leak=1
# of free M-Buffer=529, minimum=529 leak=3
```

```
# of free S-Buffer=1199, minimum=1198, leak=1
# of free Msgid-Buffer=1024, minimum=1024
```

Telnet Command: vpn Multicast

This command allows users to pass or block the multi-cast packet via VPN.

Syntax

vpn Multicast set *<H2l/L2l> <index> <Block/Pass>*

Syntax Description

Parameter	Description
<H2l/L2l>	H2l means Host to LAN (Remote Access User Accounts). L2l means LAN-to-LAN Profile.
<index>	The index number of the profile.
<Block/Pass>	Set Block/Pass the Multicast Packets. The default is Block.

Example

```
> vpn Multicast set L2l 1 Pass
% Lan to Lan Profile Index [1] :
% Status Block/Pass: [PASS]
```

Telnet Command: vpn pass2nd

This command allows users to determine if the packets coming from the second subnet passing through current used VPN tunnel.

Syntax

vpn pass2nd*[on]*

vpn pass2nd *[off]*

Syntax Description

Parameter	Description
on/off	on - the packets can pass through NAT. off - the packets cannot pass through NAT.

Example

```
> vpn pass2nd on
% 2nd subnet is allowed to pass VPN tunnel!
```

Telnet Command: vpn pass2nat

This command allows users to determine if the packets passing through by NAT or not when the VPN tunnel disconnects.

Syntax

vpn pass2nat *[on]*

vpn pass2nat *[off]*

Syntax Description

Parameter	Description
on/off	on - the packets can pass through NAT. off - the packets cannot pass through NAT.

Example

```
> vpn pass2nat on
% Packets would go through by NAT when VPN disconnect!!
```

Telnet Command: wan ppp_mru

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

Syntax

wan ppp_mru *<WAN interface number> <MRU size >*

Syntax Description

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

Example

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

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

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

Telnet Command: wan mtu / mtu2

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

Syntax

wan mtu *[value]*

wan mtu2 *[value]*

Syntax Description

Parameter	Description
value	It means the number of MTU for PPP. The available range is from 1000 to 1500.

	For Static IP/DHCP, the maximum number will be 1500.
	For PPPoE, the maximum number will be 1492.
	For PPTP/L2TP, the maximum number will be 1460.

Example

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

Telnet Command: wan DF_check

This command allows you to enable or disable the function of DF (Don't fragment)

Syntax

wan DF_check *[on]*

wan DF_check *[off]*

Syntax Description

Parameter	Description
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.

Syntax

wan forward *[on]*

wan forward *[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 modem

This command, wan modem, allows you to configure 3G/4G USB Modem (PPP mode) of WAN5.

Syntax

wan modem *[init/init2/dial/pin][string]*

wan modem paponly *[on/off]*

wan modem backup_wait *[value]*

wan modem pipe *[Int][Din][Dout]*

wan modem wakeup *[on/off/value]*

wan modem vid *[id]*

wan modem pid *[id]*

wan modem status

Syntax Description

Parameter	Description
init	Set initial modem AT command (default value is "AT&FE0V1X1&D2&C1S0=0").
Init2	Set the second initial modem AT command.
dial	Set dial modem AT command (default value is "ATDT*99#").
pin	Set PIN code for SIM card. "0":disable
paponly	It means PAP Only. Set the PPP authentication of the USB WAN. on: None. off: PAP or CHAP.
backup_wait	Set waiting time after boot if USB WAN is in backup mode. This waiting time is reserved for the dial of main WANs so that the backup USB WAN will not go up first. Available setting is from 1 to 255. Unit is second.
pipe	It is for RD debug only. Please don't use it without our advice.
wakeup [on/off]	It is for RD debug only. Please don't use it without our advice.
vid	Set VID of VID/PID match to bind the USB modem to specify WAN interface. By default, this match is not set (0x0/0x0) and the router specifies WAN interface by USB port.
pid	Set PID of VID/PID match to bind the USB modem to specify WAN interface. By default, this match is not set (0x0/0x0) and the router specifies WAN interface by USB port.
status	Display current status of USB modem.

Example

```
> wan modem pin 0000
> wan modem status
 Modem Link Speed=0
 Current Signal Strength=0
 Last Fail Message:
 Current Connect Stage:
```

Telnet Command: wan detect

This command allows you to Ping a specified IP to detect the WAN connection (static IP or PPPoE mode).

Syntax

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.

Syntax

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 WAN interface as the member of load balance.
off	It means to cancel WAN interface as the member of load balance.

Example

```
> wan lb status
 WAN1: on
 WAN2: on
 WAN3: on
 WAN4: on
 WAN5: on
 WAN6: on
 WAN7: 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.

Syntax

wan mvlan *[pvc_no/status/save/enable/disable] [on/off/clear/tag tag_no] [service type/vlan priority] [px …][Keep Tag]*

Syntax Description

Parameter	Description
pvc_no	It means index number of PVC. There are 10 PVC, 0(Channel-1) to 9(Channel-9) allowed to be configured. However, only 2 to 9 are available for configuration.
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.
Keep Tag	It means Multi-VLAN packets will keep their VLAN headers to LAN.

Example

PVC 7 will map to LAN port 2/3/4 in bridge mode; service type is Normal. No tag added.

```
> > wan mvlan 7 on p2 p3 p4

 PVC  Bridge  p1 p2 p3 p4 p5 p6   Service Type    Tag     Priority    Keep Tag

  ----------------------------------------------------------------

   7   ON      0  0  1  1  0  0     Normal      0(OFF)      0         OFF
```

```
>
```

Telnet Command: wan multifno

This command allows you to specify a channel (in Multi-PVC/VLAN) to make bridge connection to a specified WAN interface.

Syntax

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.

Syntax

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
```

Telnet Command: wan detect_mtu

This command allows you to run a WAN MTU Discovery. The user can specify an IPv4 target to ping and find the suitable MTU size of the WAN interface.

Syntax

wan detect_mtu -w *[number]* **-i** *[Host/IP address]* **-s** *[base_size]* **-d** *[decrease_size]* *(-c [count])*

Syntax Description

Parameter	Description
-w [number]	Specify the WAN interface. Value: Type the number of WAN interface. 1: WAN1; 2:WAN2….and etc.
-I [Host/IP address]	Specify the IPv4 target to detect. If can be an IPv4 address or domain name. Host/IP address: Type the IP address/domain name of the target.
-s [base_size]	Set the MTU size base for Discovery. base_size: Available setting is 1000 ~ 1500.
-d [decrease size]	Set the MTU size to decrease between detections. decrease size: Available setting is 1 ~ 100.
-c [count]	Set the maximum times of ping failure during a Discovery. count: Available settings are 1 ~ 10. Default value is 3.

Example

```
> wan detect_mtu -w 2 -i 8.8.8.8 -s 1500 -d 30 -c 10
 detecting  mtu size:1500!!!

 mtu size:1470!!!
```

Telnet Command: wan detect_mtu6

This command allows you to run a WAN MTU Discovery. The user can specify an IPv6 target to ping and find the suitable MTU size of the WAN interface.

Syntax

wan detect_mtu6 -w *[number]* **-i** *[IPv6 address]* **-s** *[base_size]*

Syntax Description

Parameter	Description
-w [number]	Specify the WAN interface number: Type the number of WAN interface. 1: WAN1; 2:WAN2….and etc.

-I [IPv6 address]	Specify the IPv6 target to detect. It must be an IPv6 IP address.
	IPv6 address: Type the IPv6 address of the target.
-s [base_size]	Specify the size of MTU.
	base_size: Available setting is 1000 ~ 1500.

Example

```
> wan detect_mtu6 –w 2 –i 2404:6800:4008:c06::5e –s 1500
>
```

Telnet Command: wol

This command allows Administrator to set the white list of WAN IP addresses/Subnets, that the magic packet from these IP addresses/Subnets will be eligible to pass through NAT and wake up the LAN client. You also need to set NAT rule for LAN client.

Syntax

wol up *[MAC Address]/[IP Address]*

wol fromWan *[on/off/any]*

wol fromWan_Setting *[idx][ip address][mask]*

Syntax Description

Parameter	Description
MAC Address	It means the MAC address of the host.
IP address	It means the LAN IP address of the host. If you want to wake up LAN host by using IP address, be sure that that IP address has been bound with the MAC address (IP BindMAC).
on/off/any	It means to enable or disable the function of WOL from WAN.
	on: enable
	off: disable
	any: It means any source IP address can pass through NAT and wake up the LAN client.
	This command will allow the user to choose whether WoL packets can be passed from the Internet to the LAN network from a specific WAN interface.
[idx][ip address] [mask]	It means the index number (from 1 to 4).
	These commands will allow the user to configure the LAN clients that the user may wake up from the Internet through the use of the WoL packet.
	ip address - It means the WAN IP address.
	mask - It means the mask of the IP address.

Example

```
> wol fromWan on
> wol fromWan_Setting 1 192.168.1.45 255.255.255.0
>
```

Telnet Command: user

The command is used to create new user account profiles.

Syntax

user set *[-e|-d|-c|-I|-o|-a|-r|-b]*

user edit *[PROFILE_IDX] [-e|-d|-n|-p|-t|-u|-i|-q|-r|-w|-s|-m|-x|-v]*

user account *[USER_NAME] [-t|-d|-q|-r|-w]*

Syntax Description

Parameter	Description
set	It means to configure general setup for the user management.
edit	It means to modify the selected user profile.
account	It means to
User Set	
-e	Enable User management function.
-d	Disable User management function.
-a[Profile idx][User name][IP_Address]	It means to pass an IP Address. *Profile idx*- type the index number of the selected profile. *User name*- type the user name that you want it to pass. *IP_Address*- type the IP address that you want it to pass.
-l all *-l userl* *-l ip*	Show online user. *all* – all of the users will be displayed on the screen. *user name* – type the user name that you want to view on the screen. *ip* – type the IP address that you want to view on the screen.
-o	It means to show user account information. e.g.,*-o*
-c[user name] *-c all*	Clear the user record. *user name* – type the user name that you want to get clear corresponding record. *all* – all of the records will be removed.
-buser [user name] *-b ip [ip address]*	Block specifies user or IP address. *user name* – type the user name that you want to block. *ip address* –- type the IP address that you want to block.
-u user [user name] *-u ip [ip address]*	Unblock specifies user or IP address. *user name* – type the user name that you want to unblock. *ip address* –- type the IP address that you want to unblock.
*-r [user name	all]*	Remove the user record. *user name* – type the name of the user profile. *all* – all of the user profile settings will be removed.
-q	It means to trigger the alert tool to do authentication.
-s	It means to set login service. 0:HTTPS 1:HTTP e.g.,*-s 1*
User edit	
PROFILE_IDX	Type the index number of the profile that you want to edit.
-e	Enable User profile function.
-d	Disable User profile function.
-n	It means to set a user name for a profile. e.g.,*-n fortest*
-p	It means to configure user password.

	e.g., *-p 60fortest*
-t	It means to enable /disable time quota limitation for user profile 0:Disable 1:Enable
-u	It means to enable /disable data quota limitation for user profile 0:Disable 1:Enable
-i	It means to set idle time. e.g., *-i 60*
-q	set time quota It means to set time quota of the user profile. e.g., *-q 200*
-r	It means to set data quota. e.g., *-r 1000*
-w	It means to specify the data quota unit (MB/GB). e.g., -w MB
-s	It means to set schedule index. Available settings are" sch_idx1,sch_idx2,sch_idx3, and sch_idx4.
-m	It means to set the maximum login user number. e.g., *-m 200*
-x	It means to set external server authentication 0: None 1: LDAP 2: Radius 3: TACAS e.g., *-x 2*
-v	It means to view user profile(s).
User account	
USER_NAME	It means to type a name of the user account.
-t	It means to enable /disable time quota limitation for user account. 0:Disable 1:Enable
-d	It means to enable /disable data quota limitation for user account. 0:Disable 1:Enable
-q	It means to set account time quota. e.g., *-q 200*
-r	It means to set account data quota. e.g., *-r 1000*
-w	It means to set data quota unit (MB/GB).

Example

```
> user account admin -d 1
  Enable the [admin] data quota limited
```

Telnet Command: nand bad /nand usage

"NAND usage" is used to display NAND Flash usage; "nand bad" is used to display NAND Flash bad blocks.

Syntax

nand bad

nand usage

Example

```
>nand usage
Show NAND Flash Usage:
Partition    Total         Used          Available      Use%
cfg          4194304       7920          4186384         0%
bin_web      33554432      11869493      21684939        35%
cfg-bak      4194304       7920          4186384         0%
bin_web-bak 33554432       11869493      21684939        35%
> nand bad
Show NAND Flash Bad Blocks:
Block   Address        Partition
1020    0x07f80000     unused
1021    0x07fa0000     unused
1022    0x07fc0000     unused
1023    0x07fe0000     unused
```

Telnet Command: ha set

This command can be used to configure HA settings for Vigor routers.

Syntax

ha set *[-<command> <parameter>| ...]*

Syntax Description

Parameter	Description
[<command> <parameter>|...]	The available commands with parameters are listed below. *[...]* means that you can type in several parameters in one line.
-e <1/0>	1: Enable the function of High Availability (HA). 0: Disable the function of High Availability (HA).
-l <1/0>	1: Enable the function of recording the operation record of HA in Syslog. 0: Disable the function of recording the operation record of HA in Syslog.
-M <1/0>	Specify the Redundancy Method for HA. 1: Active-Standby 0: Hot-Standby
-v <1-255>	Specify the group ID (VHID) 1- 255: Setting range.
-R	Set HA settings to Factory Default.
-p <1-30>	Specify the Priority ID. 1-30: Setting range.
-k <key>	Specify the Authentication Key. Key: Max. 31 Characters.
-u <1/0>	Enable or disable the function of Update DDNS. 1: Enable. When a router changes HA status to primary, it will

	update DDNS automatically. 0: Disable.
-m <interface>	Specify the management interface. Interface: LAN1 ~ LAN8, DMZ.
-s	It means to get the newest status of other router (except the local router).
-y	It means sync local config to other router. Primary can executes this command. Secondary can not execute this commad.
-c <1/0>	Enable or disable the function of Config Sync. 1: Enable. 0: Disable.
-I -[M|H|D] <interval>	Set the Config Sync Interval for HA. Minimum interval is 15 minutes. -M: Minute. Setting range is 0/15/30/45. (e.g., ha set -I -M 30) -H: Hour. Setting range is from 0 to 23. (e.g., ha set -I -H 12) -D: Day. Setting range is from 0 to 30. (e.g., ha set -I -D 15)
-h <Subnet> [<Virtual IP>]	Enable and set virtual IP to the subnet. Subnet: LAN1 to LAN8, DMZ. Virtual IP*:* The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.1.0) For example, to enable a virtual IP to the sunet, simply type: ha set –h LAN1 192.168.1.5
-d <Subnet>	Disable a virtual IP to the subnet. Subnet: LAN1 to LAN8, DMZ. For example, to disable a virtual IP to the subnet, just type: ha set –h LAN1

Example

```
> ha set –h LAN1 192.168.1.5
% Enable Virtual IP on LAN1

% Set Virtual IP 192.168.1.5 OK!!

>
```

Telnet Command: ha show

This command can be used to show the *settings information* about config sync and general setup.

Syntax

ha show –c

ha show –g

Syntax Description

Parameter	Description
-c	Show the settings of config sync.
-g	Show the settings of general setup.

Example

```
> ha show -g
%   High Availability   : Disable
%   Redundancy Method   : Active-Standby
%   Group ID            : 1
```

```
%   Priority ID       : 10
%   Preempt Mode      : Enable
%   Update DDNS       : Disable
%   Management Interface : LAN1
%   Authentication Key  : draytek
%   Syslog            : OFF
%
%   [ Index | Enable | Virtual IP ]
%   LAN1    -       0.0.0.0
%   LAN2    -       0.0.0.0
%   LAN3    -       0.0.0.0
%   LAN4    -       0.0.0.0
%   LAN5    -       0.0.0.0
%   LAN6    -       0.0.0.0
%   LAN7    -       0.0.0.0
%   LAN8    -       0.0.0.0
%   DMZ     -       0.0.0.0

>
```

Telnet Command: ha status

This command is used to display *HA status information*.

Syntax

ha status -a *[Detail Level]*

ha status -m *[Detail Level]*

Syntax Description

Parameter	Description
-a	Show the status for all of the routers in HA group.
-m	Show the status of local router only.
Detail Level	0: Basic information.
	1: Basic information with more data (e.g., firmware version, model, HTTPs port. MAC address and etc).
	2: Basic information with some HA settings.

Example

```
> ha status –m 2
%   [Local Router] DrayTek
%   IPv4              : 192.168.1.1
%   Status            : !
%   High Availability : ! Disable
%   Redundancy Method : Active-Standby
%   Group ID          : 1
%   Priority ID       : 10
%   Preempt Mode      : Enable
%   Update DDNS       : Disable
%   Management Interface : LAN1
%   Authentication Key  : draytek
%   Virtual IP: (Max. 7 Virtual IPs)
%     ! OFF
%   Config Sync       : Disable
%   Config Sync Interval : 0 Day 0 Hour 15 Minute
%   Cached Time       : 0 (s)
> ha status –m 0
```

```
%     [Local Router] DrayTek
%     IPv4                : 192.168.1.1
%     Status              : !
%     State               : Down
%     Stable              : ! No
%     WAN                 : ! All WANs Down - Eth
%     Config Sync Status  : Not Ready
%     Cached Time         : 0 (s)
%
>
```