DrayTek

Vigor2120 Series
Broadband Firewall Router

Your reliable networking solutions partner

User's Guide

V1.1

Vigor2120 Series
Broadband Firewall Router

User's Guide

Version: 1.1

Firmware Version: V3.7.5.4

(For future update, please visit DrayTek web site)

Date: March 31, 2015

Intellectual Property Rights (IPR) Information

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

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

Safety Instructions and Approval

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

DrayTek

European Community Declarations

Manufacturer: DrayTek Corp.
Address: No. 26, Fu Shing Road, Hukou Township, Hsinchu Industrial Park, Hsinchu County, Taiwan 303
Product: Vigor2120 Series Router

DrayTek Corp. declares that Vigor2120 Series of routers are in compliance with the following essential requirements and other relevant provisions of R&TTE 1999/5/EC, ErP 2009/125/EC and RoHS 2011/65/EU.

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

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

This product is designed for 2.4GHz/5GHz WLAN network throughout the EC region.

Regulatory Information

Federal Communication Commission Interference Statement

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

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

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

(1) This device may not cause harmful interference, and

(2) This device may accept any interference received, including interference that may cause undesired operation.

The antenna/transmitter should be kept at least 20 cm away from human body.

More update, please visit www.draytek.com.

Table of Contents

DrayTek

Vigor2120 Series User's Guide

4

Advanced Configuration...101

1 Introduction

> **Note: 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.**

Vigor2120 Series is a broadband router which 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 2 VPN tunnels.

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

In addition, Vigor2120 Series supports USB interface for connecting USB printer to share printing function or 3G/4G USB modem for network connection.

Vigor2120 Series provides two-level management to simplify the configuration of network connection. The user mode allows user accessing into WEB interface via simple configuration. However, if users want to have advanced configurations, they can access into WEB interface through admin mode.

Dray Tek
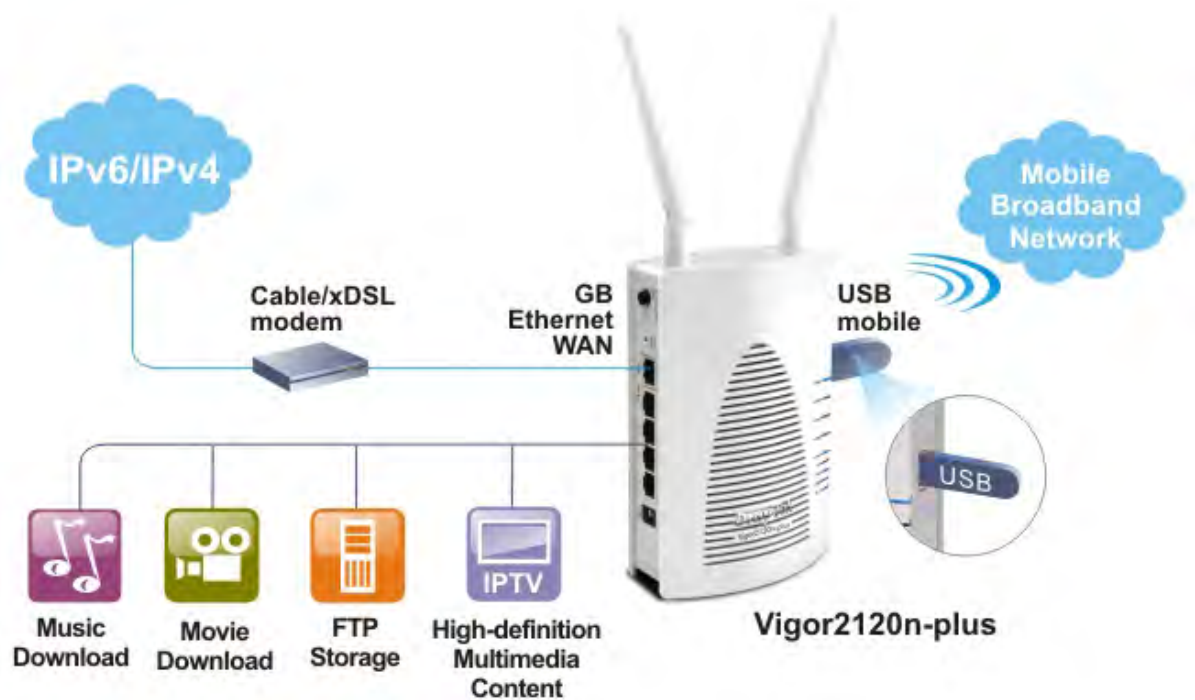
1.1 Web Configuration Buttons Explanation

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

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

Note: For the other buttons shown on the web pages, please refer to Chapter 3, 4 for detailed explanation.
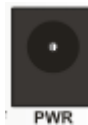
1.2 LED Indicators and Connectors

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

1.2.1 For Vigor2120
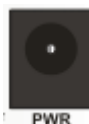
LED	Status	Explanation
ACT	Off	The system is not ready or is failed.
	Blinking	The system is ready and can work normally.
USB	On	A USB device is connected and active.
	Blinking	The data is transmitting.
VPN	On	The VPN tunnel is active.
WCF	On	The profile(s) of CSM (Content Security Management) for Web Content Filter application can be enabled from **Firewall >>General Setup**. (Such profile must be established under **CSM** menu)
LAN 1 - 4	On	A normal connection is through its corresponding port.
	Off	LAN is disconnected.
WAN	On	The WAN port is connected.
	Blinking	It will blink while transmitting data.

Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router. Press the button and keep for more than 6 seconds. Then the router will restart with the factory default configuration.
WAN	Connector for accessing the Internet.
LAN 1- 4	Connecters for local network devices (LAN).
PWR	PWR: Connecter for a power adapter.
USB	Connecter for a USB device (for 3G USB Modem or printer or storage disk).
ON/OFF	ON/OFF: Power switch.

1.2.2 For Vigor2120n-plus
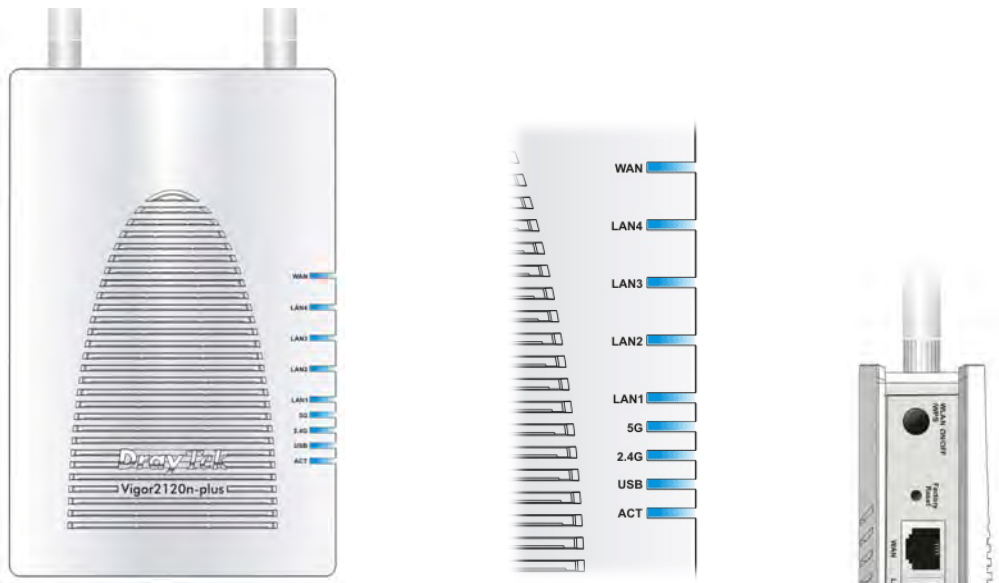
LED	Status	Explanation
ACT	Off	The system is not ready or is failed.
	Blinking	The system is ready and can work normally.
USB	On	A USB device is connected and active.
	Blinking	The data is transmitting.
2.4G	On	Wireless function is ready.
	Off	Wireless function is not ready.
	Blinking	Data is transmitting (sending/receiving).
5G	On	Wireless function is ready.
	Off	Wireless function is not ready.
	Blinking	Data is transmitting (sending/receiving).
LAN 1 - 4	On	A normal connection is through its corresponding port.
	Off	LAN is disconnected.
WAN	On	The WAN port is connected.
	Blinking	It will blink while transmitting data.

Interface	Description
WLAN ON/OFF WPS	WLAN On - Press the button and release it within 2 seconds. When the wireless function is ready, the 2.4G/5G blue LED on front panel will be on.
	WLAN Off - Press the button and release it within 2 seconds to turn off the WLAN function. When the wireless function is not ready, 2.4G/5G blue LED on front panel will be off.
	WPS - When WPS function is enabled by web user interface, press this button for more than 2 seconds. The router will wait for any wireless client connecting to it through WPS.
Factory Reset	Restore the default settings. Usage: Turn on the router. Press the button and keep for more than 6 seconds. Then the router will restart with the factory default configuration.
WAN	Connector for accessing the Internet.
LAN 1- 4	Connecters for local network devices (LAN).
PWR	PWR: Connecter for a power adapter.
USB	Connecter for a USB device (for 3G USB Modem or printer or storage disk).
ON/OFF	ON/OFF: Power switch.

Dray Tek

1.3 Hardware Installation

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

1. Connect the cable Modem/DSL Modem/Media Converter to any WAN port of router with Ethernet cable (RJ-45).

2. Connect one end of an Ethernet cable (RJ-45) to one of the **LAN** ports of the router and the other end of the cable (RJ-45) into the Ethernet port on your computer.

3. Connect one end of the power adapter to the router's power port on the rear panel, and the other side into a wall outlet.

4. Power on the device by pressing down the power switch on the rear panel.

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

   (For the hardware connection, we take *"n"* model as an example.)
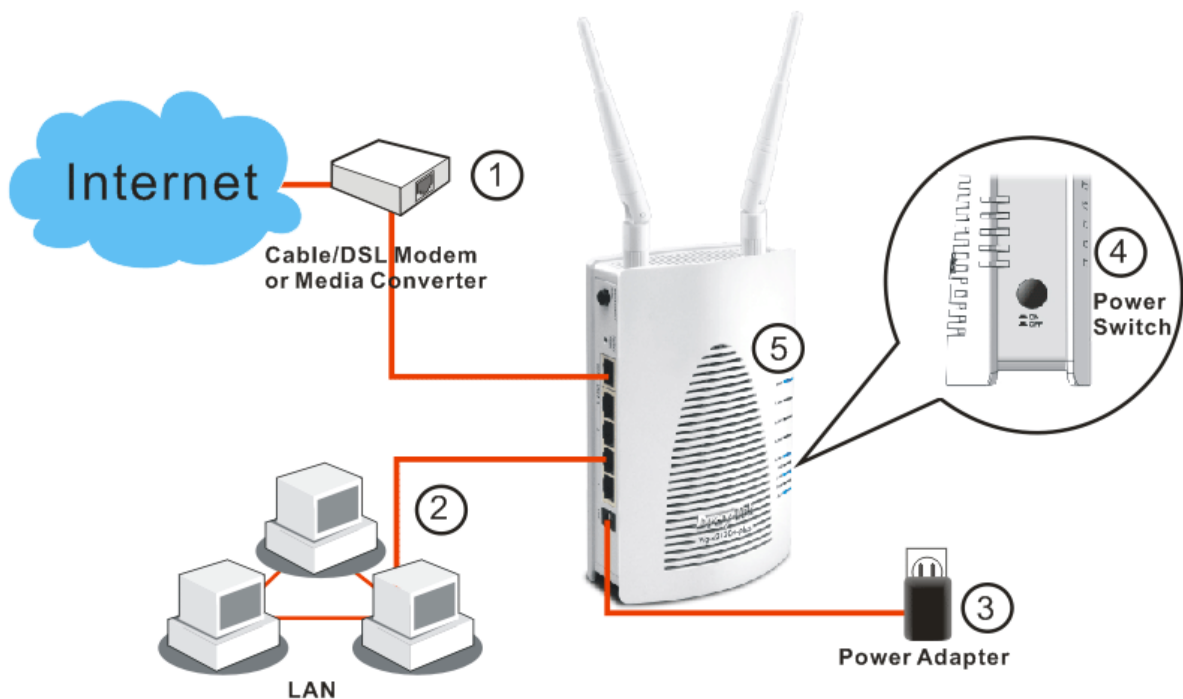
1.4 Printer Installation

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 XP/2000. For Windows 98/SE/Vista, 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**.
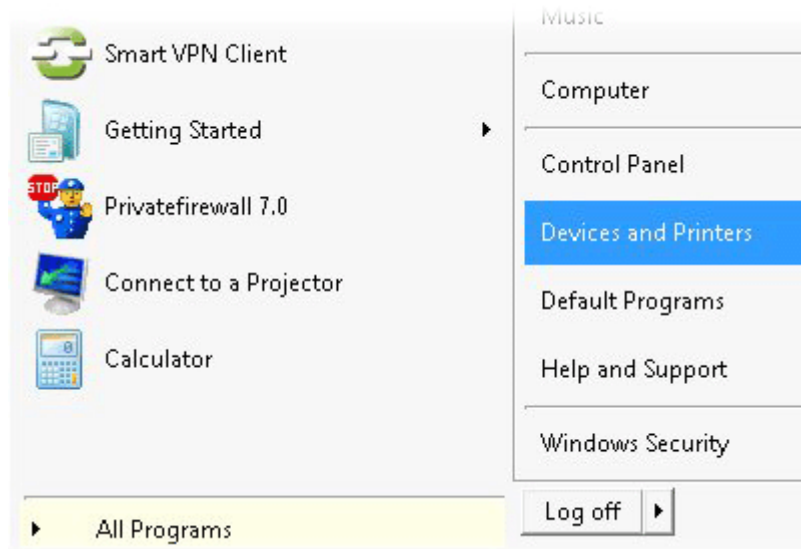
3. Click **Add a printer**.
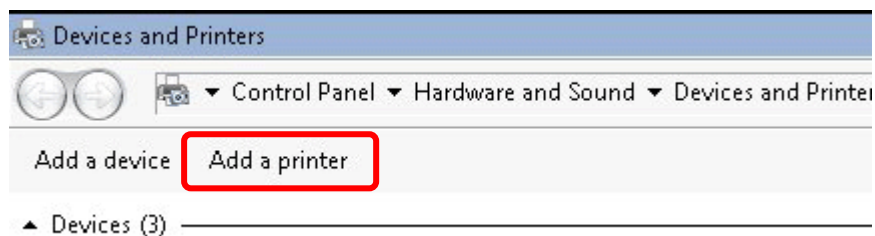
4. A dialog will appear. Click **Add a local printer** and click **Next**.
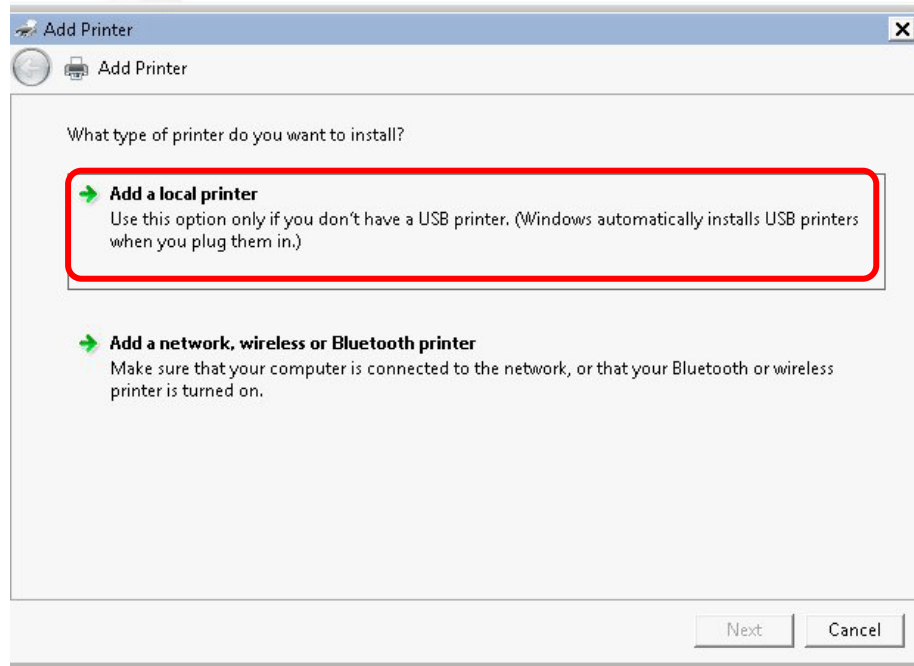
5. In this dialog, choose **Create a new port.** In the field of **Type of port,** use the drop down list to select **Standard TCP/IP Port**. Then, click **Next**.
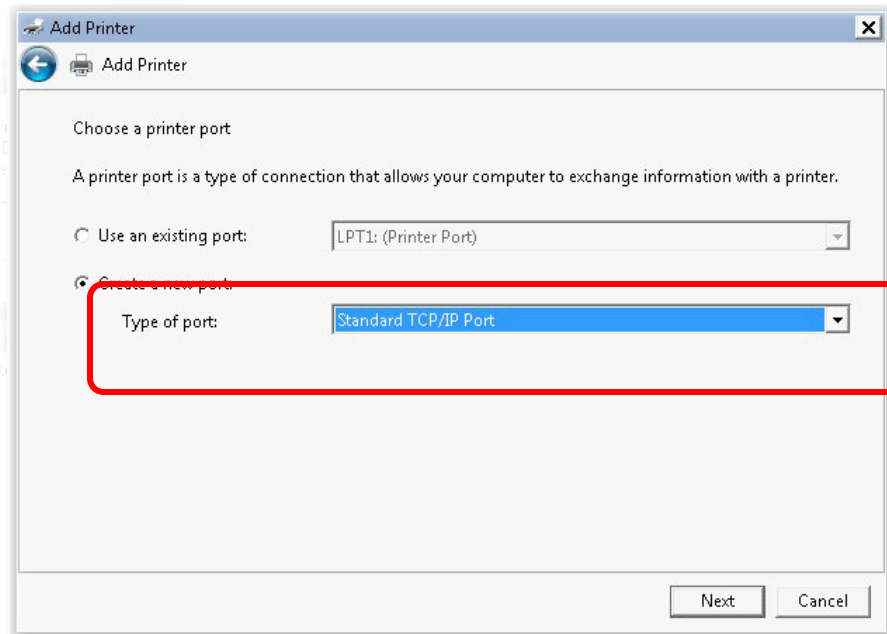
6. In the following dialog, type **192.168.1.1** (router's LAN IP) in the field of **Hostname or IP Address** and type **192.168.1.1** as the **Port name**. Then, click **Next**.

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

DrayTek

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**.
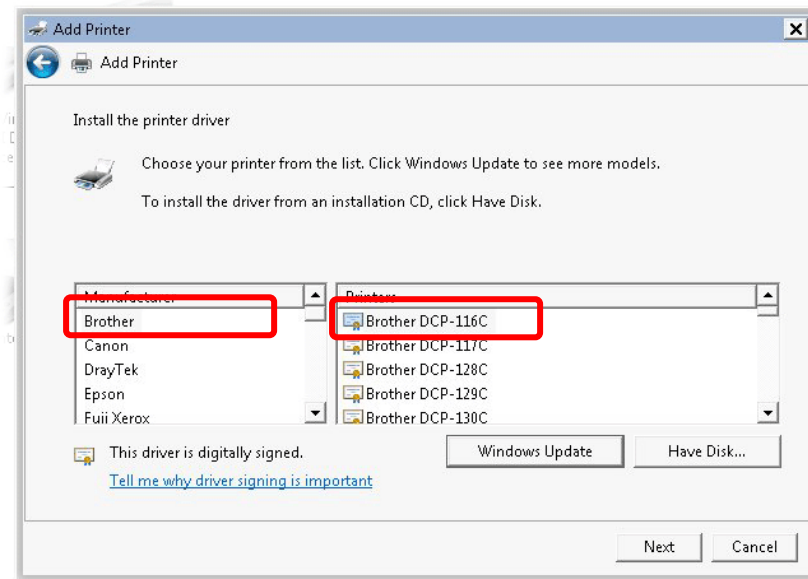
9. Type a name for the chosen printer. Click **Next.**
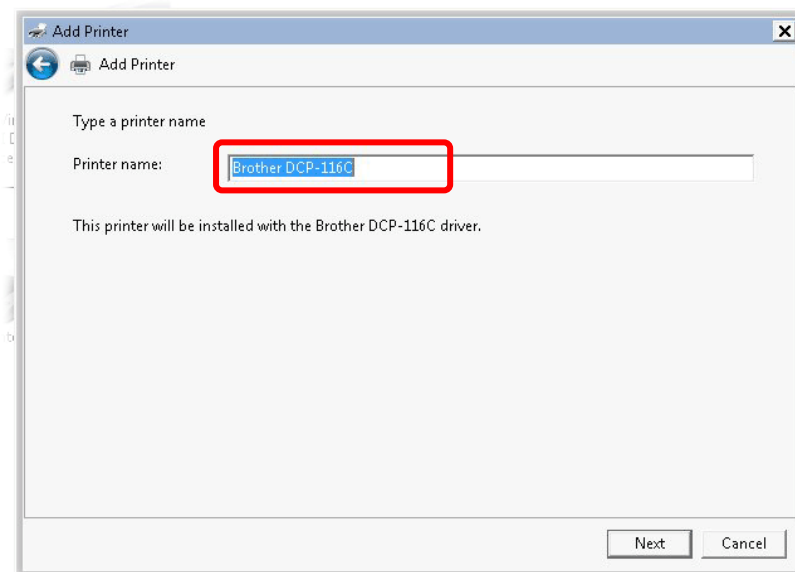
10. Choose **Do not share this printe**r and click **Next**.
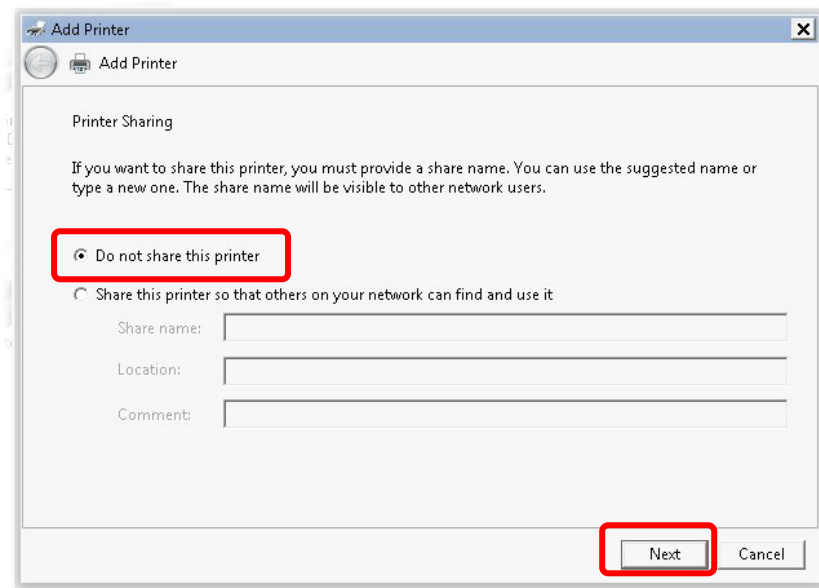
11. Then, in the following dialog, click **Finish**.
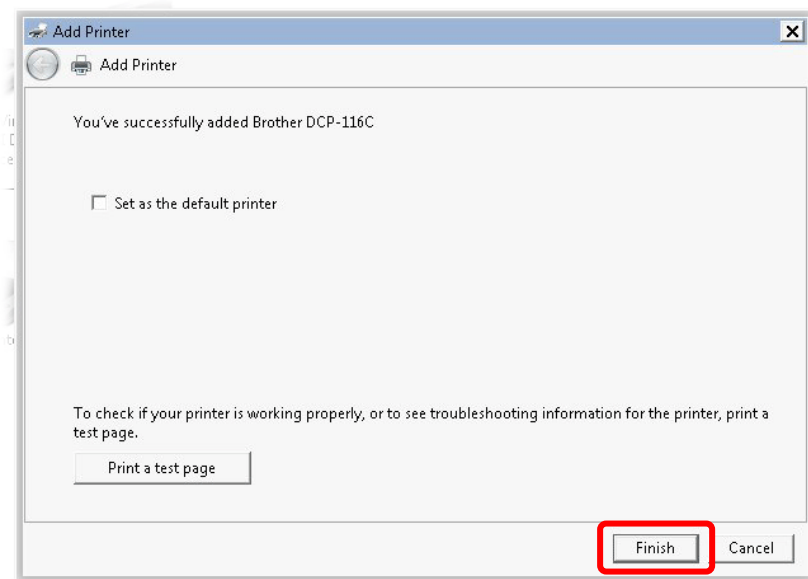
12. The new printer has been added and displayed under **Printers and Faxes**. Click the new printer icon and click **Printer server properties**.
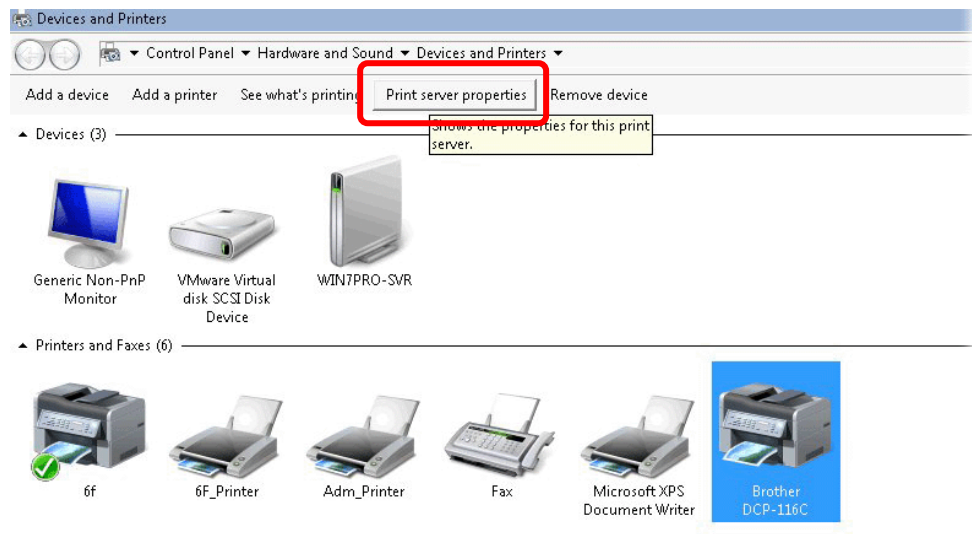
13. Edit the property of the new printer you have added by clicking **Configure Port**.
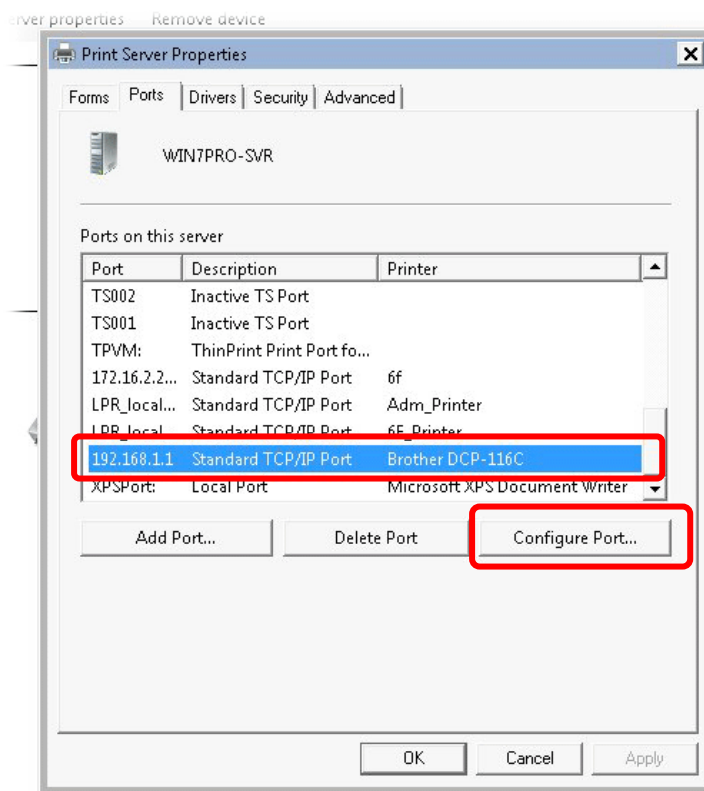
14. Select "**LPR**" on Protocol, type **p1** (number 1) as **Queue Name**. Then click **OK**. Next please refer to the red rectangle for choosing the correct protocol and LPR name.
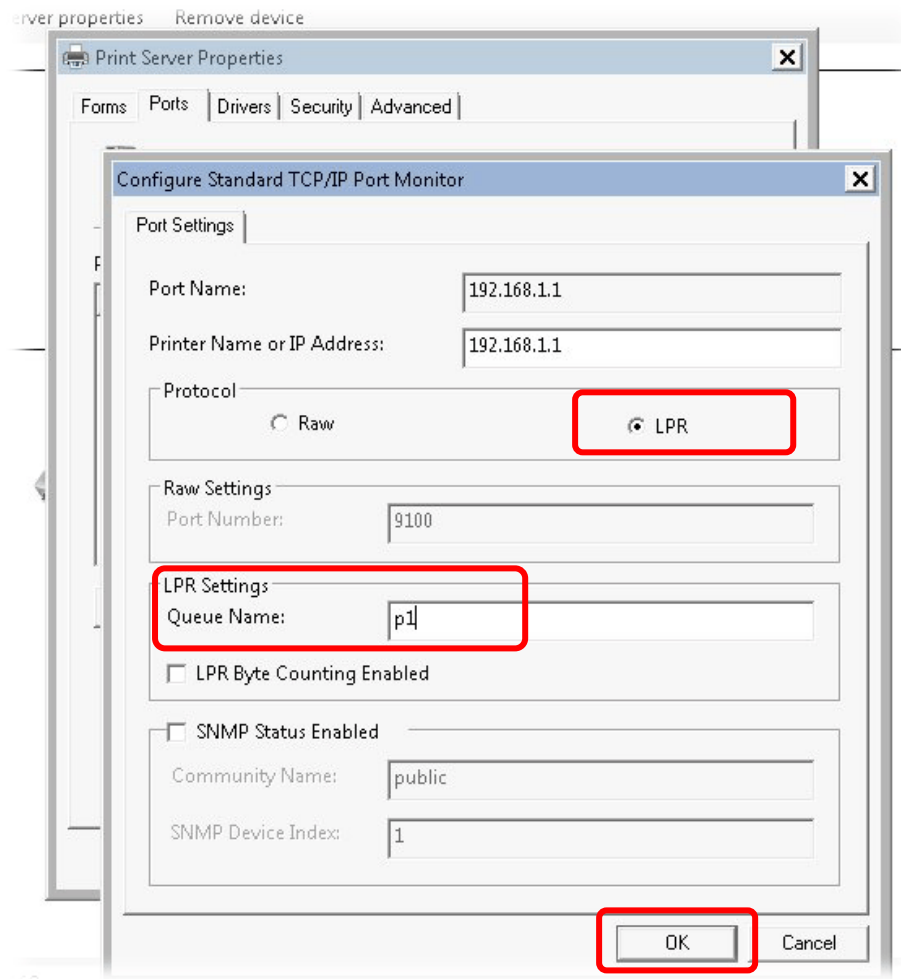
The printer can be used for printing now. Most of the printers with different manufacturers are compatible with vigor router.

Dray Tek

Note 1: Some printers with the fax/scanning or other additional functions are not supported. If you do not know whether your printer is supported or not, please visit www.draytek.com to find out the printer list. Open **Support >FAQ/Application Notes**; find out the link of **USB>>Printer Server** and click it.
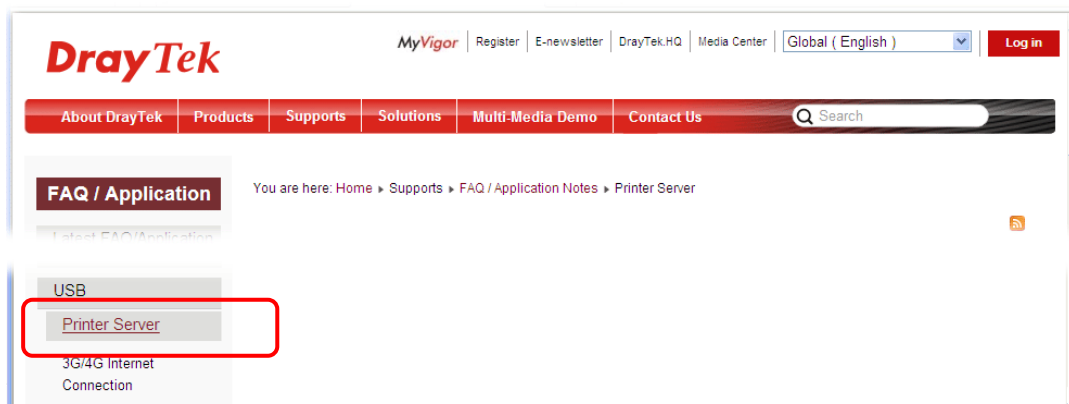
Then, click the **What types of printers are compatible with Vigor router**? link.
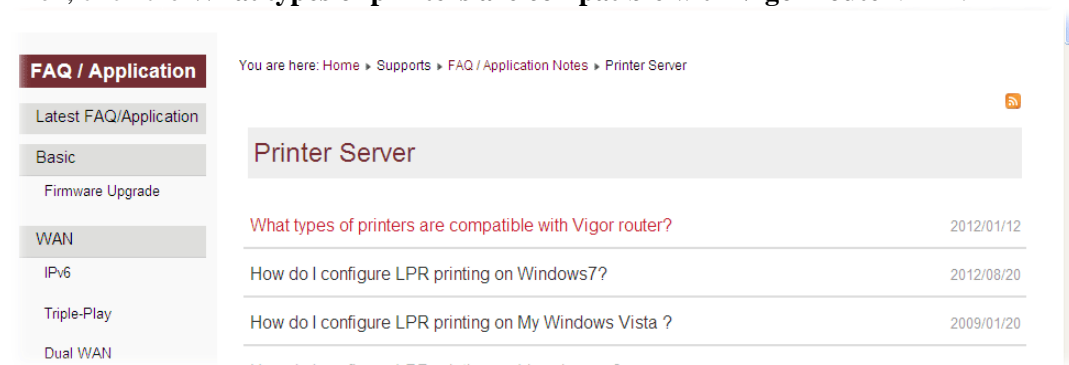
Note 2: Vigor router supports printing request from computers via LAN ports but not WAN port.

1.5 Accessing Web Page

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

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

2. Open a web browser on your PC and type **http://192.168.1.1.** The following window will be open to ask for username and password.
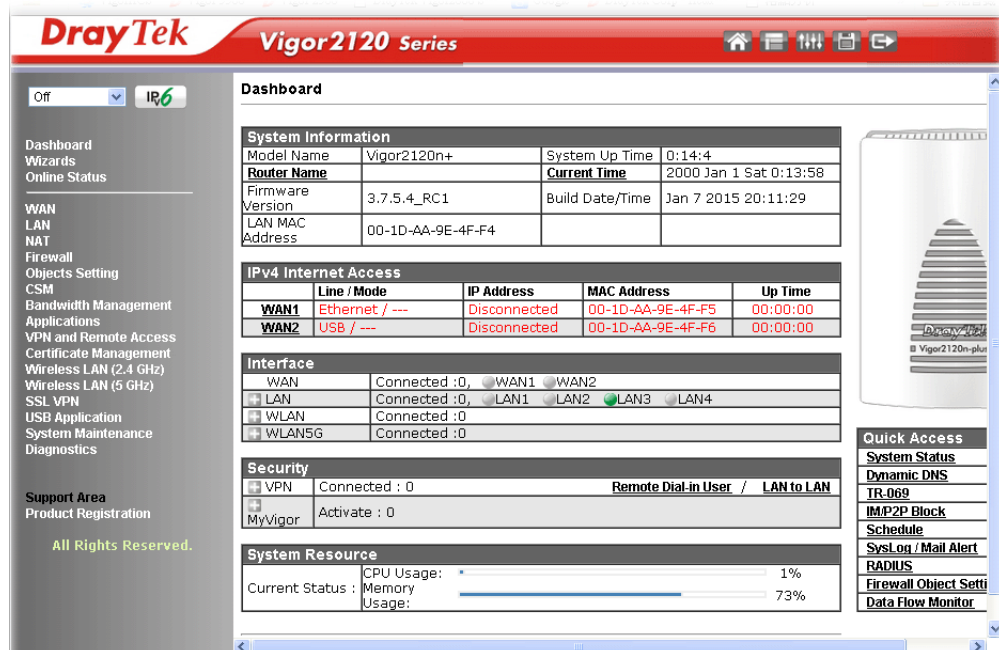
3. Please type "admin/admin" as the Username/Password and click **Login**.

    > **Notice:** 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.

> **Note:** 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.
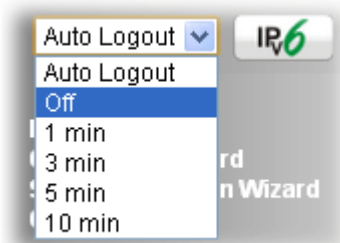
1.6 Changing Password

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**. Then click **OK** to continue.

> **Note:** 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.

> **Note:** Even the password has been changed, the Username for logging to the web user interface is still "admin".

1.7 Introducing 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.
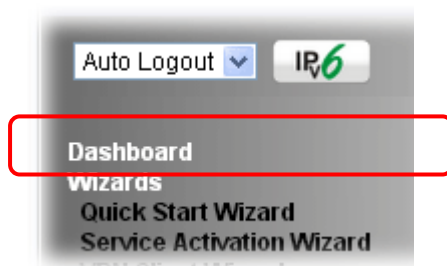
A web page with default selections will be displayed on the screen. Refer to the following figure:
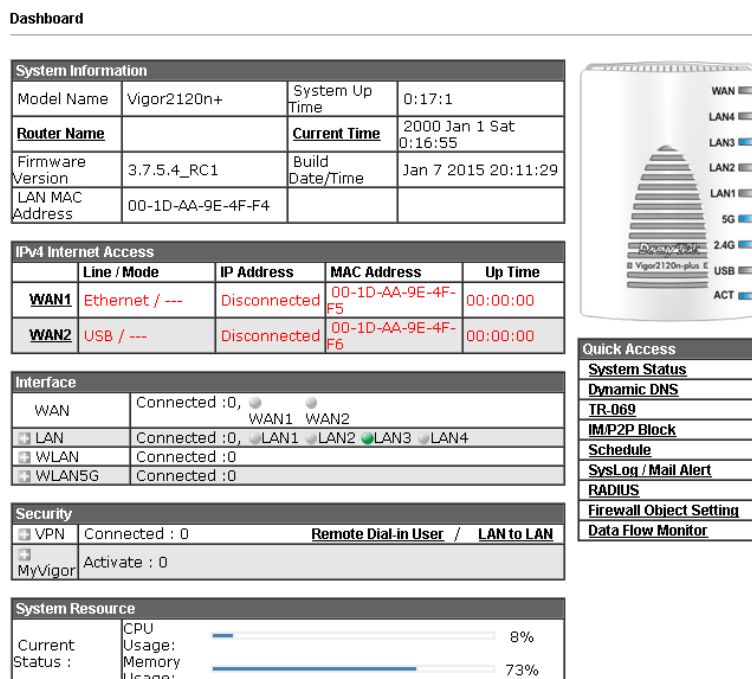
1.7.1 Virtual Panel

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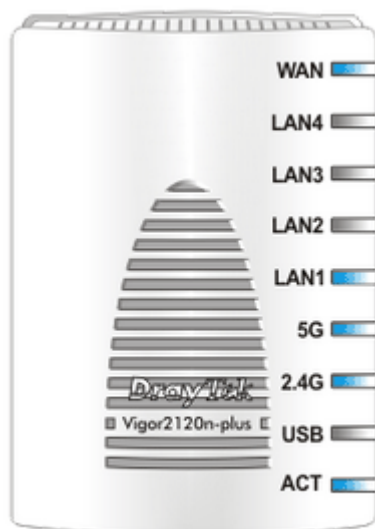
For detailed information about the LED display, refer to **1.2 LED Indicators and Connectors**.

1.7.2 Name with a Link

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

1.7.3 Quick Access for Common Used Menu

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

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

The function links of System Status, Dynamic DDNS, TR-069, IM/P2P Block, Schedule, Syslog/Mail Alert, RADIUS, Firewall Object Setting and Data Flow Monitor are displayed here. Move your mouse cursor on any one of the links and click on it. The corresponding setting page will be open immediately.

In addition, quick access for VPN security settings such as **Remote Dial-in User** and **LAN to LAN** are located on the bottom of this page. Scroll down the page to find them and use them if required.

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

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

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

1.7.4 GUI Map

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

1.7.5 Web Console

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

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

```
192.168.1.1/doc/console.htm - 楓樹瀏覽器

192.168.1.1/doc/console.htm

Type ? for command help
> ?

% Valid commands are:
bpa         csm          ddns        dos        exit         internet
ip          ip6          ipf         log        mngt         msubnet
object      port         portmaptime prn        qos          quit
show        srv          switch      sys        testmail     upnp
usb         vigbrg       vlan        vpn        wan          wptl
wol
> █
```
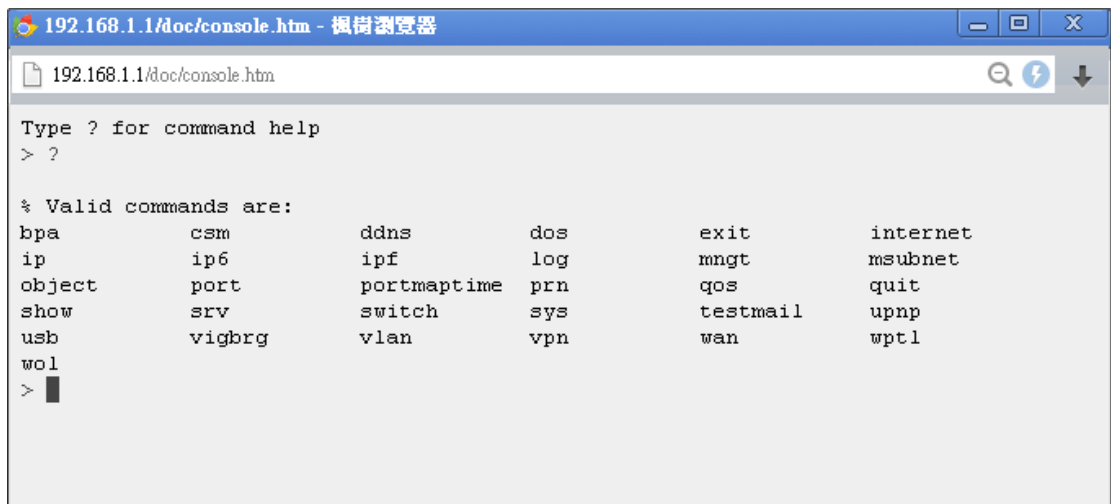
1.7.6 Config Backup

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

Simply click the icon on the top of the main screen and a pop up dialog will appear.
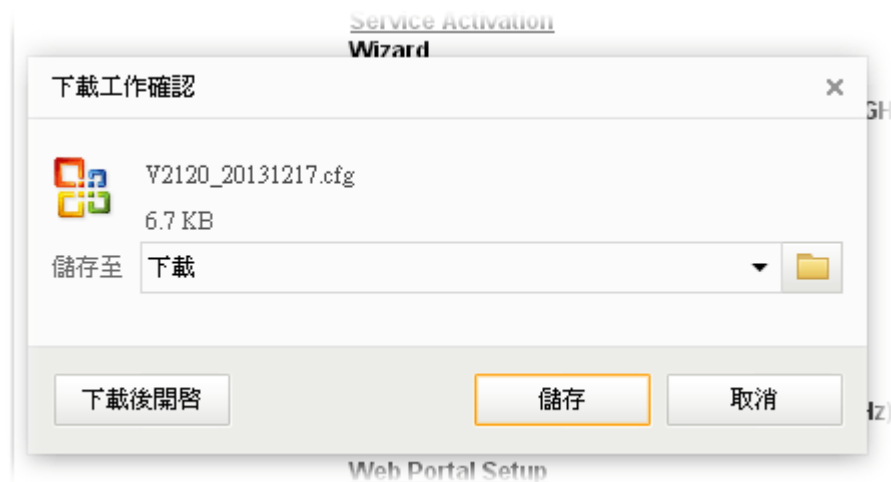
Click **Save** to store the setting.

1.7.7 Logout

Click this icon to exit the web user interface.

DrayTek

1.8 Online Status

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

1.8.1 Physical Connection for IPv4 Protocol

1.8.2 Physical Connection for IPv6 Protocol

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/WAN2	**Enable – Yes** in red means such interface is available but not enabled. **Yes** in green means such interface is enabled.

Item	Description
	Line – Displays the physical connection (Ethernet, or USB) of this interface.
	Name – Display the name of the router.
	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.
WAN IPv6 Status	**Enable – No** in red means such interface is available but not enabled. **Yes** in green means such interface is enabled. No in red means such interface is not available.
	Mode - Displays the type of WAN connection (e.g., TSPC).
	Up Time - Displays the total uptime of the interface.
	IP - Displays the IP address of the WAN interface.
	Gateway IP - Displays the IP address of the default gateway.

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

Dray Tek

1.8.3 Virtual WAN

Such page displays the virtual WAN connection information.

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

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

1.9 Saving Configuration

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

Admin mode
Status: Settings Saved

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

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

This page is left blank.

2 # Quick Setup

There are several setup wizards offered for you to configure the router simply and quickly.

- **Quick Start Wizard** – used for building network connection, Internet access.
- **Service Activation Wizard** – used for activating the web content filter service.
- **VPN Client Wizard** – used for establishing VPN tunnel; the router is treated as a VPN client.
- **VPN Server Wizard** – used for establishing VPN tunnel; the router is treated as a VPN server.

2.1 Quick Start Wizard

The **Quick Start Wizard** is designed for you to easily set up your router for Internet access. Open **Wizards>>Quick Start Wizard**.
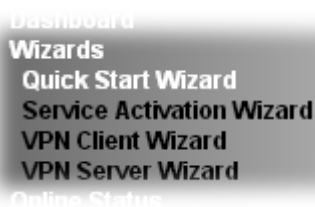
It can help you to deploy and use the router easily and quickly. The first screen of **Quick Start Wizard** is entering login password. After typing the password, please click **Next**.

On the next page as shown below, please select the WAN interface that you use. If Ethernet interface is used, please choose WAN1; if 3G USB modem is used, please choose WAN2. Then click **Next** for next step.

Quick Start Wizard

WAN Interface

WAN Interface: WAN1

Display Name:

Physical Mode: Ethernet

Physical Type: Auto negotiation

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

WAN1 and WAN2 will bring up different configuration page. Refer to the following for detailed information.

DrayTek

2.1.1 For WAN1 (Ethernet)

WAN1 is dedicated to physical mode in Ethernet. If you choose WAN1, please specify physical type. Then, click **Next**.

Quick Start Wizard

WAN Interface

WAN Interface:	WAN1
Display Name:	
Physical Mode:	Ethernet
Physical Type:	Auto negotiation

< Back   Next >   Finish   Cancel

2.1.1.1 PPPoE

1. Open **Wizards>>Quick Start Wizard**. Finish the password settings and click **Next**.

2. Choose **WAN1** as the WAN Interface and click the **Next** button.

3. The following page will be open for you to specify Internet Access Type. Click **PPPoE** as the Internet Access Type. Then click **Next** to continue.

Quick Start Wizard

Connect to Internet

WAN 1
Select one of the following Internet Access types provided by your ISP.
- PPPoE
- PPTP
- L2TP
- Static IP
- DHCP

< Back   Next >   Finish   Cancel

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

Quick Start Wizard

PPPoE Client Mode

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

Service Name (Optional)	
Username	77484247@hinet.net
Password	●●●●●●●●
Confirm Password	●●●●●●●●

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

Available settings are explained as follows:

Item	Description
Service Name	Type the service information for identifying ISP.
Username	Assign a specific valid user name provided by the ISP.
Password	Assign a valid password provided by the ISP.
Confirm Password	Retype the password.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

5. A summary page will be displayed as follows.

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN1
Physical Mode:	Ethernet
Internet Access:	PPPoE

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

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

DrayTek

6. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear.

Quick Start Wizard Setup OK!

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

2.1.1.2 PPTP/L2TP

1. Open **Wizards>>Quick Start Wizard**. Finish the password settings and click **Next**.

2. Choose **WAN1** as the WAN Interface and click the **Next** button.

3. The following page will be open for you to specify Internet Access Type. Click **PPTP/L2TP** as the Internet Access Type. Then click **Next** to continue.

Quick Start Wizard

Connect to Internet

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

- ○ PPPoE
- ● PPTP
- ○ L2TP
- ○ Static IP
- ○ DHCP

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

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

Quick Start Wizard

PPTP Client Mode

WAN 1
Enter the username, password, WAN IP configuration and PPTP server IP provided by your ISP.

Username	774494727
Password	••••••••
Confirm Password	••••••••
WAN IP Configuration	
○ Obtain an IP address automatically	
● Specify an IP address	
IP Address	172.16.3.136
Subnet Mask	255.255.255.0
Gateway	172.16.3.1
Primary DNS	undefined
Second DNS	undefined
PPTP Server	

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

Available settings are explained as follows:

Item	Description
User Name	Assign a specific valid user name provided by the ISP.
Password	Assign a valid password provided by the ISP.
Confirm Password	Retype the password.

WAN IP Configuration	**Obtain an IP address automatically** – the router will get an IP address automatically from DHCP server.
	Specify an IP address – you have to type relational settings manually.
	IP Address - Type the IP address.
	Subnet Mask –Type the subnet mask.
	Gateway – Type the IP address of the gateway.
	Primary DNS –Type in the primary IP address for the router.
	Second DNS –Type in secondary IP address for necessity in the future.
PPTP Server / L2TP Server	Type the IP address of the server.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

5. A summary page will be displayed as follows.

Quick Start Wizard

Please confirm your settings:

WAN Interface: WAN1
Physical Mode: Ethernet
Internet Access: PPTP

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

< Back   Next >   Finish   Cancel

6. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear.

Quick Start Wizard Setup OK!

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

2.1.1.3 Static IP

1.   Open **Wizards>>Quick Start Wizard**. Finish the password settings and click **Next**.

2.   Choose **WAN1** as the WAN Interface and click the **Next** button.

3.   The following page will be open for you to specify Internet Access Type. Click **Static IP**
     as the Internet Access Type. Then click **Next** to continue.

Quick Start Wizard

Connect to Internet

> **WAN 1**
> Select one of the following Internet Access types provided by your ISP.
>
> ○ PPPoE
> ○ PPTP
> ○ L2TP
> ◉ Static IP
> ○ DHCP

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

4.   Please type in the IP address information originally provided by your ISP. Then click
     Next for viewing summary of such connection..

Quick Start Wizard

Static IP Client Mode

> **WAN 1**
> Enter the Static IP configuration provided by your ISP.
>
> | | | |
> |---|---|---|
> | WAN IP | 172.16.3.130 | |
> | Subnet Mask | 255.255.255.0 | |
> | Gateway | 172.16.3.1 | |
> | Primary DNS | 8.8.8.8 | |
> | Secondary DNS | undefined | (optional) |

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

Available settings are explained as follows:

Item	Description
WAN IP	Type the IP address.
Subnet Mask	Type the subnet mask.
Gateway	Type the IP address of gateway.
Primary DNS	Type in the primary IP address for the router.

Secondary DNS	Type in secondary IP address for necessity in the future.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

5. A summary page will be displayed as follows.

Quick Start Wizard

Please confirm your settings:

WAN Interface: WAN1
Physical Mode: Ethernet
Internet Access: Static IP

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

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

6. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear.

Quick Start Wizard Setup OK!

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

2.1.1.4 DHCP

1. Open **Wizards>>Quick Start Wizard**. Finish the password settings and click **Next**.

2. Choose **WAN1** as the WAN Interface and click the **Next** button.

3. The following page will be open for you to specify Internet Access Type. Click **DHCP** as the Internet Access Type. Then click **Next** to continue.

Quick Start Wizard

Connect to Internet

> **WAN 1**
> Select one of the following Internet Access types provided by your ISP.
>
> ○ PPPoE
> ○ PPTP
> ○ L2TP
> ○ Static IP
> ◉ DHCP

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

4. Click **DHCP** as the Internet Access type. Simply click **Next** to continue. Then click **Next** for viewing summary of such connection.

Quick Start Wizard

DHCP Client Mode

> **WAN 1**
> If your ISP requires you to enter a specific host name or specific MAC address, please enter it in.
>
> Host Name   Vigor   (optional)
> MAC   00 -1D -AA -9C -F7 -35 (optional)

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

Available settings are explained as follows:

Item	Description
Host Name	Type the name of the host. **Note:** The maximum length of the host name you can set is 39 characters.
MAC	Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to

DrayTek

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

5. A summary page will be displayed as follows.

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN1
Physical Mode:	Ethernet
Internet Access:	DHCP

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

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

6. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear.

Quick Start Wizard Setup OK!

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

2.1.2 For WAN2 (USB)

WAN2 is dedicated to physical mode in USB.

1. Open **Wizards>>Quick Start Wizard**. Finish the password settings and click **Next**

2. Choose **WAN2** as the WAN Interface and click the **Next** button.

3. In the following page, fill in the information for 3G/4G USB Modem.

Available settings are explained as follows:

Item	Description
Internet Access	Choose a protocol for accessing the Internet.
3G/4G USB Modem (PPP mode)	**SIM Pin code** –Type PIN code of the SIM card that will be used to access Internet. The maximum length of the pin code you can set is 15 characters.
	Modem Initial String – Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP. The maximum length

38   **Dray Tek**

	of the string you can set is 47 characters.
	APN Name – APN means Access Point Name which is provided and required by some ISPs. Type the name and click **Apply**.
4G USB Modem (DHCP mode)	**SIM Pin code** –Type PIN code of the SIM card that will be used to access Internet.
	Network Mode – Force Vigor router to connect Internet with the mode specified here. If you choose 4G/3G/2G as network mode, the router will choose a suitable one according to the actual wireless signal automatically.
	APN Name – APN means Access Point Name which is provided and required by some ISPs.

4.   Then, click **Next** for viewing summary of such connection.

Quick Start Wizard

Please confirm your settings:

WAN Interface: WAN2
Physical Mode: USB
Internet Access: PPP

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

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

5.   Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear.

Quick Start Wizard Setup OK!

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

2.2 Service Activation Wizard

Service Activation Wizard can guide you to activate WCF service (Web Content Filter) with a quick and easy way. **For the Service Activation Wizard is only available for admin operation, therefore, please type "admin/admin" on Username/Password while Logging into the web user interface.**

Service Activation Wizard is a tool which allows you to use trial version of WCF directly without accessing into the server (**MyVigor**) located on http://myvigor.draytek.com. For using Web Content Filter Profile, please refer to later section **Web Content Filter Profile** for detailed information.

Now, follow the steps listed below to activate WCF feature for your router.

Note: Such function is available only for **Admin Mode**.

1. Open **Wizards>>Service Activation Wizard**.
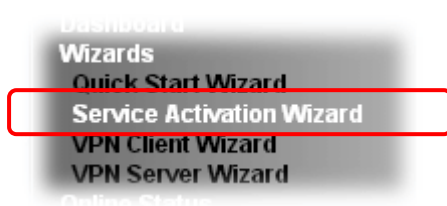
2. The screen of **Service Activation Wizard** will be shown as follows. Choose the one you need and click **Next**. In this case, we choose to activate free trail edition.

Free trial edition: it offers a period of trial for you to get acquainted with WCF function.

3. In the following page, you can activate the Web content filter services at the same time or individually. When you finish the selection, please click **Next**.

Commtouch is the web content filter based on Commtouch operated in the worldwide. There is a 30-day trial period. After trial, you can purchase DrayTek's prepared Commtouch GlobalView WCF package from retailing outlets.

BPjM is WCF for German Speaking users. The fragFINN is whitelist for German Speaking users. The BPjM is ideal for your family to provide more Internet security for youngsters.

Web Content Filter (fragFINN) service had not been supported since January 1, 2015.

4. Setting confirmation page will be displayed as follows, please click **Next**.

5. Wait for a moment till the following page appears.

Service Activation Wizard

Connection Succeeded!

Please check the following item(s) to enable services on your router.

☑ Enable Web Content Filter

Next > [Finish]

When such page appears, you can enable or disable these services for your necessity. Then, click **Finish.**

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

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

Service Activation Wizard

Server Enabled!

DrayTek Service Activation

Service Name	Start Date	Expire Date	Status
Web Content filter	2013-02-18	2013-03-21	Commtouch

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.

When all the trial editions for various web content filters had been enabled, the configuration page of Service Activation Wizard will be invalid as shown below.

Service Activation Wizard

Select the service type that you want to activate

This wizard is used for activating
- N/A

Please choose the edition you need.

◉ Free trial edition

https://myvigor.draytek.com/

Next > [Finish] [Cancel]

DrayTek

2.3 VPN Client Wizard

Such wizard is used to configure VPN settings for VPN client. Such wizard will guide to set the LAN-to-LAN profile for VPN dial out connection (from server to client) step by step.

1. Open **VPN and Remote Access>>VPN Client Wizard**. The following page will appear.

Available settings are explained as follows:

Item	Description
LAN-to-LAN Client Mode Selection	Choose the client mode.
	Route Mode/NAT Mode – If the remote network only allows you to dial in with single IP, please choose this mode, otherwise please choose Route Mode.
Please choose a LAN-to-LAN Profile	There are 32 VPN profiles for users to set.

```
[Index] [Status] [Name]
1         x       ???
2         x       ???
3         x       ???
4         x       ???
5         x       ???
6         x       ???
7         x       ???
8         x       ???
9         x       ???
10        x       ???
11        x       ???
12        x       ???
13        x       ???
14        x       ???
15        x       ???
16        x       ???
17        x       ???
18        x       ???
19        x       ???
20        x       ???
21        x       ???
22        x       ???
23        x       ???
24        x       ???
25        x       ???
26        x       ???
27        x       ???
28        x       ???
29        x       ???
```

2. When you finish the mode and profile selection, please click **Next** to open the following page.

VPN and Remote Access >> VPN Client Wizard

VPN Connection Setting

Security ranking (1 is the highest; 5 is the lowest)

1. L2TP over IPsec
2. IPsec
3. PPTP (Encryption)
4. L2TP
5. PPTP (None Encryption)

Throughput ranking (1 is the highest; 5 is the lowest)

1. PPTP (None Encryption)
2. L2TP
3. IPsec
4. L2TP over IPsec
5. PPTP (Encryption)

Select VPN Type: PPTP (Encryption)

PPTP (None Encryption)
PPTP (Encryption)
IPsec
L2TP
L2TP over IPsec (Nice to Have)
L2TP over IPsec (Must)

< Back   Next >   Finish   Cancel

In this page, you have to select suitable VPN type for the VPN client profile. There are six types provided here. Different type will lead to different configuration page. After making the choices for the client profile, please click **Next**. You will see different configurations based on the selection(s) you made.

DrayTek

Note: The following descriptions for VPN Type are based on the **Route Mode** specified in **LAN-to-LAN Client Mode Selection.**

- When you choose **PPTP** (**None Encryption)** or **PPTP** (**Encryption),** you will see the following graphic:

VPN and Remote Access >> VPN Client Wizard

VPN Client PPTP Encryption Settings

Profile Name	???
☐ Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	draytek.com
Username	marketing
Password	••••••
Remote Network IP	192.168.1.6
Remote Network Mask	255.255.255.0

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

- When you choose **IPsec,** you will see the following graphic:

VPN Client Wizard

VPN Client IPsec Settings

Profile Name	???
☐ Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
IKE Authentication Method	
◉ Pre-Shared Key	
Confirm Pre-Shared Key	
◯ Digital Signature (X.509)	
Peer ID	None
Local ID	
◉ Alternative Subject Name First	
◯ Subject Name First	
Local Certificate	None
IPsec Security Method	
◉ Medium (AH)	
◯ High (ESP)	DES without Authentication
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

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

- When you choose **L2TP**, you will see the following graphic:

VPN Client Wizard

VPN Client L2TP Settings

Profile Name	???
☐ Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
Username	???
Password	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

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

- When you choose **L2TP over IPsec (Nice to Have)** or **L2TP over IPsec (Must),** you will see the following graphic:

VPN Client Wizard

VPN Client L2TP over IPsec (Nice to Have) Settings

Profile Name	???
☐ Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
IKE Authentication Method	
⊙ Pre-Shared Key	
Confirm Pre-Shared Key	
○ Digital Signature (X.509)	
Peer ID	None
Local ID	
⊙ Alternative Subject Name First	
○ Subject Name First	
Local Certificate	None
IPsec Security Method	
⊙ Medium (AH)	
○ High (ESP)	DES without Authentication
Username	???
Password	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

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

DrayTek

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such profile. The length of the file is limited to 10 characters.
Always On	Check to enable router always keep VPN connection.
Server IP/Host Name for VPN	Type the IP address of the server or type the host name for such VPN profile.
IKE Authentication Method	IKE Authentication Method usually applies to those are remote dial-in user or node (LAN to LAN) which uses dynamic IP address and IPsec-related VPN connections such as L2TP over IPsec and IPsec tunnel. **Pre-Shared Key-** Specify a key for IKE authentication. **Confirm Pre-Shared Key-**Confirm the pre-shared key. **Digital Signature (X.509) -** Click **Digital Signature** to invoke this function. ● **Peer ID** – Choose the peer ID selection from the drop down list. ● **Local ID** – Choose **Alternative Subject Name First** or **Subject Name First**. ● **Local Certificate** – Use the drop down list to choose one of the certificates for using. You have to configure one certificate at least previously in **Certificate Management >> Local Certificate.** Otherwise, the setting you choose here will not be effective.
IPsec Security Method	**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.
User Name	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above. The length of the user name is limited to 11 characters.
Password	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 11 characters.
Remote Network IP	Please type one LAN IP address (according to the real location of the remote host) for building VPN connection.
Remote Network Mask	Please type the network mask (according to the real location of the remote host) for building VPN connection.

3. After finishing the configuration, please click **Next.** The confirmation page will be shown as follows. If there is no problem, you can click one of the radio buttons listed on the page and click **Finish** to execute the next action.

VPN Client Wizard

Please confirm your settings

```
LAN-to-LAN Index:            3
Profile Name:                VPN_Jim
VPN Connection Type:         L2TP over IPsec (Nice to Have)
Always on:                   No
Server IP/Host Name:         172.16.3.8
IKE Authentication Method:   Pre-Shared Key
IPsec Security Method:       AH-SHA1
Remote Network IP:           172.16.3.99
Remote Network Mask:         255.255.255.0
```

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and proceed to the following action:

- ⊙ Go to the VPN Connection Management.
- ○ Do another VPN Client Wizard setup.
- ○ View more detailed configurations.

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

Available settings are explained as follows:

Item	Description
Go to the VPN Connection Management	Click this radio button to access **VPN and Remote Access>>Connection Management** for viewing VPN Connection status.
Do another VPN Server Wizard Setup	Click this radio button to set another profile of VPN Server through VPN Server Wizard.
View more detailed configuration	Click this radio button to access **VPN and Remote Access>>LAN to LAN** for viewing detailed configuration.

DrayTek

2.4 VPN Server Wizard

Such wizard is used to configure VPN settings for VPN server. Such wizard will guide to set the LAN-to-LAN profile for VPN dial in connection (from client to server) step by step.

1. Open **VPN and Remote Access>>VPN Server Wizard**. The following page will appear.

VPN Server Wizard

Choose VPN Establishment Environment

VPN Server Mode Selection:	Remote Dial-in User (Teleworker ▼
Please choose a LAN-to-LAN Profile:	1　　　x　　　??? ▼
Please choose a Dial-in User Accounts:	8　　　x　　　??? ▼
Allowed Dial-in Type:	
	☑ PPTP
	☑ IPsec
	☑ L2TP with IPsec Policy None ▼
	☑ SSL Tunnel
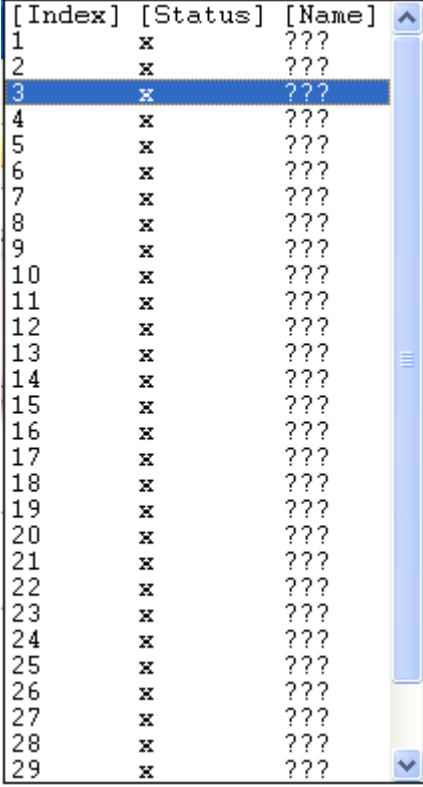
`< Back` `Next >` `Finish` `Cancel`

Available settings are explained as follows:

Item	Description
VPN Server Mode Selection	Choose the direction for the VPN server. **Site to Site VPN** – To set a LAN-to-LAN profile automatically, please choose Site to Site VPN. **Remote Dial-in User** –You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in via VPN connection. Site to Site VPN (LAN-to-LAN) ▼ Site to Site VPN (LAN-to-LAN) Remote Dial-in User (Teleworker)
Please choose a LAN-to-LAN Profile	This item is available when you choose **Site to Site VPN** (LAN-to-LAN) as VPN server mode. There are 32 VPN profiles for users to set.

```
[Index] [Status] [Name] ▲
1          x        ???
2          x        ???
3          x        ???
4          x        ???
5          x        ???
6          x        ???
7          x        ???
8          x        ???
9          x        ???
10         x        ???
11         x        ???
12         x        ???
13         x        ???
14         x        ???
15         x        ???
16         x        ???
17         x        ???
18         x        ???
19         x        ???
20         x        ???
21         x        ???
22         x        ???
23         x        ???
24         x        ???
25         x        ???
26         x        ???
27         x        ???
28         x        ???
29         x        ??? ▼
```

Please choose a Dial-in User Accounts	This item is available when you choose Remote Dial-in User (Teleworker) as VPN server mode. There are 32 VPN tunnels for users to set.
Allowed Dial-in Type	This item is available after you choose any one of dial-in user account profiles. Next, you have to select suitable dial-in type for the VPN server profile. There are several types provided here (similar to VPN Client Wizard). ☑ PPTP ☑ IPsec ☑ L2TP with IPsec Policy　[None ▼]　None / Nice to Have / Must ☑ SSL Tunnel Different Dial-in Type will lead to different configuration page. In addition, adjustable items for each dial-in type will be changed according to the VPN Server Mode (**Site to Site VPN** and **Remote Dial-in User**) selected.

2. After making the choices for the server profile, please click **Next**. You will see different configurations based on the selection you made.

    Here we take the examples of choosing **Site-to-Site VPN** as the **VPN Server Mode**.

● When you check **PPTP**, you will see the following graphic:

VPN Server Wizard

VPN Authentication Setting

Profile Name	
PPTP / L2TP / L2TP over IPsec / SSL Tunnel Authentication	
Username	???
Password	
Peer IP/VPN Client IP	
Site to Site Information	
Remote Network IP	
Remote Network Mask	

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

● When you check **PPTP & IPsec & L2TP** (three types) or **PPTP & IPsec** (two types) or **L2TP with Policy** (**Nice to Have/Must**), you will see the following graphic:

VPN Server Wizard

VPN Authentication Setting

Profile Name	???
PPTP / L2TP / L2TP over IPsec / SSL Tunnel Authentication	
Username	???
Password	
IPsec / L2TP over IPsec Authentication	
☑ Pre-Shared Key	
Confirm Pre-Shared Key	
☐ Digital Signature (X.509)	
Peer ID	None
Local ID	
◉ Alternative Subject Name First	
○ Subject Name First	
Peer IP/VPN Client IP	
Peer ID	
Site to Site Information	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

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

● When you check **IPsec**, you will see the following graphic:

VPN Server Wizard

VPN Authentication Setting

Profile Name	???
IPsec / L2TP over IPsec Authentication	
☑ Pre-Shared Key	
Confirm Pre-Shared Key	
☐ Digital Signature (X.509)	
Peer ID	None
Local ID	
⦿ Alternative Subject Name First	
○ Subject Name First	
Peer IP/VPN Client IP	
Peer ID	
Site to Site Information	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

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

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such profile. The length of the file is limited to 10 characters.
User Name	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 11 characters.
Password	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 11 characters.
Pre-Shared Key	For IPsec/L2TP IPsec authentication, you have to type a pre-shared key. The length of the name is limited to 64 characters.
Confirm Pre-Shared Key	Type the pre-shared key again for confirmation.
Digital Signature (X.509)	Check the box of Digital Signature to invoke this function. **Peer ID** – Choose the peer ID selection from the drop down list. **Local ID** – Choose **Alternative Subject Name First** or **Subject Name First**.
Peer IP/VPN Client IP	Type the WAN IP address or VPN client IP address for the remote client.
Peer ID	Type the ID name for the remote client. The length of the name is limited to 47 characters.

Dray Tek

Remote Network IP	Please type one LAN IP address (according to the real location of the remote host) for building VPN connection.
Remote Network Mask	Please type the network mask (according to the real location of the remote host) for building VPN connection.

3. After finishing the configuration, please click **Next.** The confirmation page will be shown as follows. If there is no problem, you can click one of the radio buttons listed on the page and click **Finish** to execute the next action.

Available settings are explained as follows:

Item	Description
Go to the VPN Connection Management	Click this radio button to access **VPN and Remote Access>>Connection Management** for viewing VPN Connection status.
Do another VPN Server Wizard Setup	Click this radio button to set another profile of VPN Server through VPN Server Wizard.
View more detailed configuration	Click this radio button to access **VPN and Remote Access>>LAN to LAN** for viewing detailed configuration.

2.5 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.
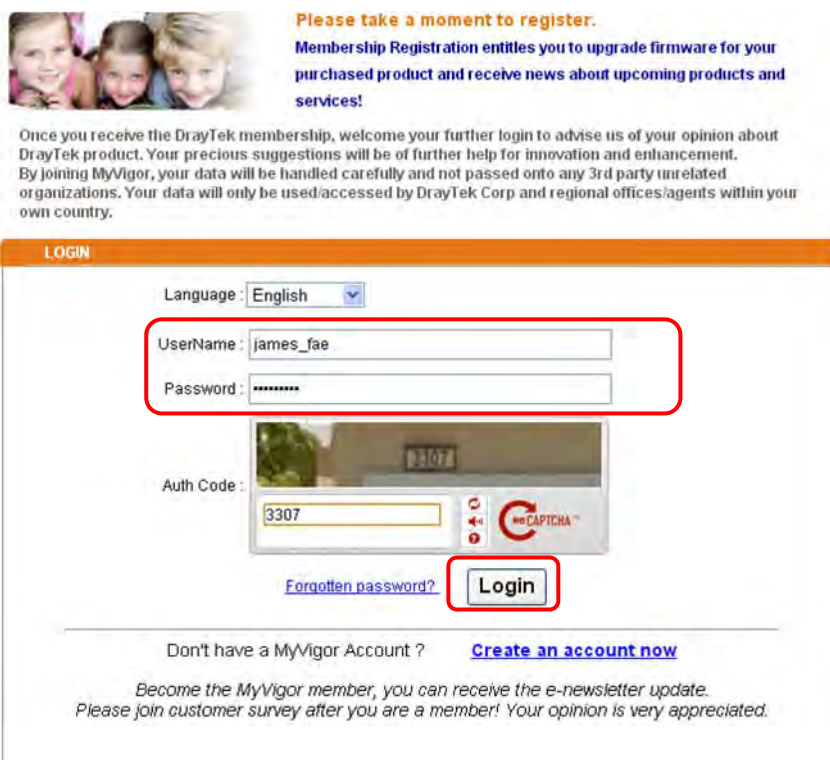
2   Click **Support Area>>Production Registration** from the home page.

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

> **Notice:** If you haven't an accessing account, please refer to section 3.5 Creating an Account for MyVigor on this Guide 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. From this page, please click **Add** or **Product Registration**.

5   When the following page appears, please type in Nickname (for the router) and choose the right registration date from the popup calendar (it appears when you click on the box of Registration Date). After adding the basic information for the router, please click **Submit**.

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

Your device has been successfully added to the database.

OK

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

DrayTek

Tutorials and Applications

3.1 How to configure settings for IPv6 Service in Vigor2120

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

- **Dual Stack**

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

- **Tunnel**

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

- **Translation**

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

Before configuring the settings on Vigor2120, you need to know which connection type that your IPv6 service used.

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

I. Configuring the WAN Settings

For the IPv6 WAN settings for Vigor2120, there are five connection types to be chosen: PPP, TSPC, AICCU, DHCPv6 Client and Static IPv6.

1. Access into the web user interface of Vigor2120. Open **WAN**>> **Internet Access**. Choose one of the WAN interfaces as the one supporting IPv6 service. Then, click the IPv6 button of the selected WAN.

> **Note:** Only one WAN interface support IPv6 service at one time. In this example, WAN1 is chosen as the one supporting IPv6 service.

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

Internet Access >> IPv6

IPv6 Mode

Internet Access Mode

Connection Type   Offline

Offline
PPP
TSPC
AICCU
DHCPv6 Client
Static IPv6
6in4 Static Tunnel
6rd

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

● **PPP – Dual Stack application, IPv4 and IPv6 services can be utilized at the same time**

Choose PPP and type the information for PPPoE of IPv4.

Internet Access >> PPPoE

PPPoE Client Mode

PPPoE Setup		PPP/MP Setup	
PPPoE Link	◉ Enable ○ Disable	PPP Authentication	PAP or CHAP
ISP Access Setup		Idle Timeout	-1 second(s)
ISP Name	Hinet	**IP Address Assignment Method (IPCP)** [WAN IP Alias]	
Username	73168525@hinet.net	Fixed IP	○ Yes ◉ No (Dynamic IP)
Password	••••••	Fixed IP Address	
Index(1-15) in **Schedule** Setup:			
=> [ ] , [ ] , [ ] , [ ]		◉ Default MAC Address	
		○ Specify a MAC Address	
WAN Connection Detection		MAC Address:	
Mode	ARP Detect	00 ·1D ·AA :9C ·F7 ·35	
Ping IP			
TTL:			
PPPoE Pass-through			
☐ For Wired LAN			
☐ For Wireless LAN			

[OK]

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

Internet Access >> IPv6

IPv6 Mode

Internet Access Mode

Connection Type   PPP

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

[OK]

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

Vigor2120 Series User's Guide

● **TSPC – Tunnel application, both IPv6 hosts communicate through IPv4 network**

Choose **TSPC** and type the information for TSPC service.

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

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

Internet Access >> IPv6

IPv6 Mode

Internet Access Mode

Connection Type	TSPC

TSPC Configuration

Username	cacahsu
Password	••••••••
Confirm Password	••••••••
Tunnel Broker	broker.freenet6.net

OK

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

Online Status

Physical Connection			System Uptime: 0:2:3
	IPv4	IPv6	

LAN Status
IP Address
2001:5C0:1502:D00:21D:AAFF:FEA6:2568/64 (Global)
FE80::21D:AAFF:FEA6:2568/64 (Link)

TX Packets	RX Packets	TX Bytes	RX Bytes
88	121	15596	10249

WAN2 IPv6 Status

Enable	Mode	Up Time	
Yes	TSPC	0:01:40	

IP		Gateway IP	

2001:5C0:1400:B::10B9/128 (Global)   ---
FE80::722C:3559/128 (Link)

TX Packets	RX Packets	TX Bytes	RX Bytes
127	89	9219	15866

Dray Tek

● **AICCU – Tunnel application**

Choose AICCU and type the information for AICCU of IPv6.

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

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

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

Vigor2120 Series User's Guide

● **DHCPv6 Client**

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

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

- **Static IPv6**

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

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

II. Configuring the LAN Settings

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

1. Access into the web user interface of Vigor2120. Open **LAN**>> **General Setup**. Click the **IPv6** button to display the following page.

   > **Note**: Only the subnet of **LAN1** supports IPv6 feature.

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

3. In the field of **DHCPv6 Server**, when DHCPv6 service is enabled, you can assign available IPv6 address for the client manually.

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

III. Confirming IPv6 Service Run Successfully

1. Make sure you have get the correct IPv6 IP address. Get into MS-DOS interface and type the command of "ipconfig". Refer to the following figure.
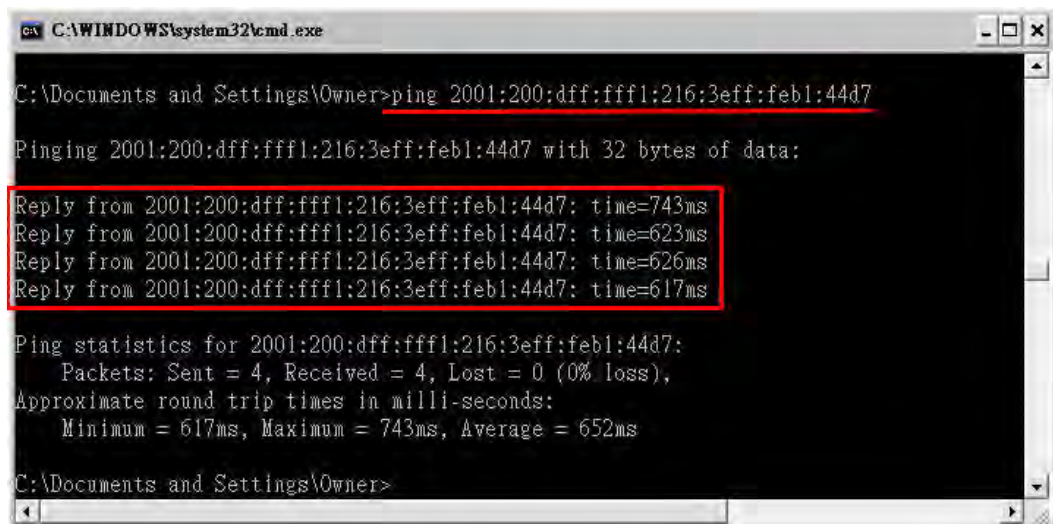
From the above figure we can see IPv6 IP address has been captured by the system.

2. Use the Ping command to ping any IPv6 address indicating an IPv6 website. For example, www.kame.net is a website supporting IPv4 IP and IPv6 IP services. Its IPv6 address is seen with a format of 2001:200:dff:fff1:216:3eff:feb1:44d7.

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

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

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

DrayTek

3.2 How can I get the files from USB storage device connecting to Vigor router?

Files on USB storage device can be reviewed by opening **USB Applicaiton>>File Explorer.** If it is necessary for you to delete, copy files on the device or write, paste files to the devcie, it must be done through or FTP server.

1. Plug the USB device to the USB port on the router. Make sure **Disk Connected** appears on the **Connection Status** as the figure shown below:

2. Setup a user account for the FTP service by using **USB Application >>USB User Management.** Click **Enable** to enable FTP/Samba User account. Here we add a new account "user1" and assign authorities "Read", "Write" and "List" to it.

3. Click **OK** to save the configuration.

4. Make sure the FTP service is running properly. Please open a browser and type *ftp://192.168.1.1*. Use the account "**user1**" to login.

5. When the following screen appears, it means the FTP service is running properly.

6. Return to **USB Application >> USB Disk Status**. The information for FTP server will be shown as below.

Now, users in LAN of Vigor2120 can access into the USB storage device by typing ftp://192.168.1.1 on any browser. They can add or remove files / directories, depending on the Access Rule for FTP account settings in **USB Application >>USB User Management.**

3.3 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.

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.

Dray Tek

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.

DrayTek

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

VPN and Remote Access >> Connection Management

Dial-out Tool   Refresh Seconds : 5 ▼   Refresh

(V2920) 172.16.2.145   ▼   Dial

VPN Connection Status
Current Page: 1   Page No.   Go >>

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate (Bps)	Rx Pkts	Rx Rate (Bps)	UpTime	
1 (VPN Client)	IPSec Tunnel DES-SHA1 Auth	218.242.133.91	172.17.1.0/24	8	3	132	36	0:6:41	Drop

xxxxxxxx : Data is encrypted.
xxxxxxxx : Data isn't encrypted.

3.4 How to Optimize the Bandwidth through QoS Technology

Have you ever gotten any problems in uploading/downloading files (Voice, video or email/data only) with the narrow/districted bandwidth you may share from the common Internet connection line? The advanced bandwidth management technology-QoS (Quality of Service) helps you to well allocate the bandwidth upon your demand of Voice, Video, or Data transferring. Let's see how to get the optimum bandwidth per your request by using DrayTek Vigor router as below.

Scenario: The Internet connection you got from ISP line is 2MB/512Kb. There are VoIP telephony network, IPTV set top box and data server at your home. Assume you want to allocate 30% of the bandwidth you got to VoIP demand, 50% for IPTV, 15% for mail/data, 5% for others. Let's see how easily it is to do the setting as below:

1. Open **Bandwidth Management>> Quality of Service**.

2. You will get the following page. Click the **Edit** link for **Class 1**.

3. In the following page, type a name (e.g., VoIP) for such class and click **Add**.

4. Check the box of **ACT**. Click **Edit** to specify the local address.

Bandwidth Management >> Quality of Service

Rule Edit

☑ ACT	
Ethernet Type	⦿ IPv4 ○ IPv6
Local Address	Any [Edit]
Remote Address	Any [Edit]
DiffServ CodePoint	ANY ▾
Service Type	---Predefined--- ▾

Note: Please choose/setup the Service Type first.

[OK] [Cancel]

5.   In the pop-up window, choose **Range Address** as the **Address Type** and type the start IP address and end IP address in relational fields. Click **OK** to save the settings and exit the window.

Ethernet Type: IPv4

Address Type	Range Address ▾
Start IP Address	172.16.1.240
End IP Address	172.16.1.241
Subnet Mask	0.0.0.0

[OK] [Close]

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

Bandwidth Management >> Quality of Service

Rule Edit

☑ ACT	
Ethernet Type	⦿ IPv4 ○ IPv6
Local Address	172.16.1.240~172.16.1.241 [Edit]
Remote Address	Any [Edit]
DiffServ CodePoint	ANY ▾
Service Type	---Predefined--- ▾

Note: Please choose/setup the Service Type first.

[OK] [Cancel]

7. The class rule for VoIP has been set. Click **OK** to return to previous page.

Bandwidth Management >> Quality of Service

Class Index #1

Name: VoIP   ☐ Tag packets as: Default ▾

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 ○	Active	172.16.1.240 ~ 172.16.1.241	Any	ANY	ANY

[Add] [Edit] [Delete]

[OK] [Cancel]

8. Do the same steps to add class rules for IPTV and Data/Email with IP addresses as shown below.

Bandwidth Management >> Quality of Service

Class Index #2

Name: IPTV   ☐ Tag packets as: Default ▾

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 ○	Active	172.16.1.242 ~ 172.16.1.249	Any	ANY	ANY

[Add] [Edit] [Delete]

[OK] [Cancel]

and

Bandwidth Management >> Quality of Service

Class Index #3

Name: Data/Email   ☐ Tag packets as: Default ▾

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 ○	Active	Any	Any	IP precedence 2	ANY

[Add] [Edit] [Delete]

[OK] [Cancel]

DrayTek

9. Assuming you get 2MB/512Kb Internet line. You can click the **Setup** link of WAN1 to set up the bandwidth for different groups among VoIP, IPTV and Data/Email.

Bandwidth Management >> Quality of Service

General Setup | Set to Factory Default |

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
Backup WAN	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setup

Class Rule

Index	Name	Rule	Service Type
Class 1	VoIP	Edit	
Class 2	IPTV	Edit	Edit
Class 3	Data/Email	Edit	

10. In the Setup page, check the box of **Enable the QoS Control**. Type 30, 50 and 15 in the boxes for VoIP, IPTV and Data/Email respectively. Check the box of **Enable UDP Bandwidth Control**.

Bandwidth Management >> Quality of Service

General Setup
☑ **Enable the QoS Control** OUT ▼

	WAN Inbound Bandwidth	100	○ Kbps ⊙ Mbps
	WAN Outbound Bandwidth	100	○ Kbps ⊙ Mbps

Index	Class Name	Reserved_bandwidth Ratio
Class 1	VoIP	30 %
Class 2	IPTV	50 %
Class 3	Data/Email	15 %
	Others	5 %

☑ Enable UDP Bandwidth Control   Limited_bandwidth Ratio 25 %
☐ Outbound TCP ACK Prioritize

[OK] [Clear] [Cancel]

> **Note:** 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.

11. Click **OK** to save the settings. The class rules for WAN1 are defined as shown below.

Bandwidth Management >> Quality of Service

General Setup | **Set to Factory Default** |

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Enable	100000Kbps/100000Kbps	Outbound	30%	50%	15%	5%	Active	**Status**	**Setup**
Backup WAN	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	**Setup**

Class Rule

Index	Name	Rule	Service Type
Class 1	VoIP	**Edit**	
Class 2	IPTV	**Edit**	**Edit**
Class 3	Data/Email	**Edit**	

DrayTek

3.5 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.

3.5.1 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.

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

Once you receive the DrayTek membership, welcome your further login to advise us of your opinion about DrayTek product. Your precious suggestions will be of further help for innovation and enhancement.
By joining MyVigor, your data will be handled carefully and not passed onto any 3rd party unrelated organizations. Your data will only be used/accessed by DrayTek Corp and regional offices/agents within your own country.

LOGIN

Language : English

UserName :

Password :

Auth Code : 3307

3307

Forgotten password? **Login**

Don't have a MyVigor Account ? **Create an account now**

Become the MyVigor member, you can receive the e-newsletter update.
Please join customer survey after you are a member! Your opinion is very appreciated.

3. Click the link of **Create an account now**.
4. Check to confirm that you accept the Agreement and click **Accept**.

Register
Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 Completion

================================ MyVigor Agreement ================================

1. Agreement
Draytek provides MyVigor(myvigor.draytek.com) service according to this agreement. When you use MyVigor service, it means that you have read, understand and agree to accept the items listed in this agreement. Draytek can modify or change the content of the items without any reasons. It is suggested for you to notice the medications or changes at any time. If you still use MyVigor service after knowing the modifications and changes of this service, it means you have read, understand and agree to accept the modifications and changes. If you do not agree the content of this agreement, please stop using MyVigor service.

2. Registration
To use this service, you have to agree the following conditions:
  (a) Provide your complete and correct information according to the registration steps of this service.
  (b) If you provide any incorrect or fake information here. DrayTek has the right to pause or terminate

☑ I have read and understand the above Agreement. (Use the scroll bar to view the entire agreement)

<< Back   Accept >>

Dray Tek

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

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

7. Now you have created an account successfully. Click START.

8. Check to see the confirmation *email* with the title of **New Account Confirmation Letter from <u>myvigor.draytek.com</u>**.
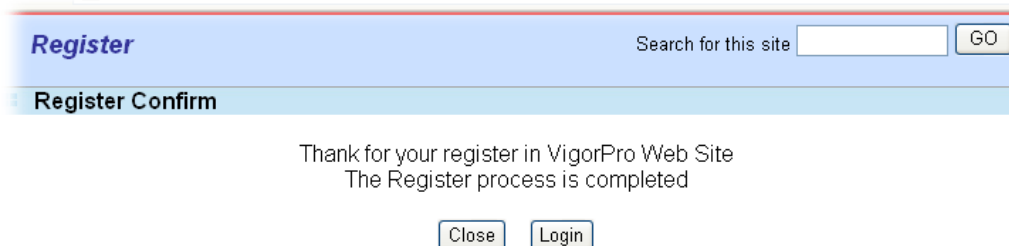
***** This is an automated message from myvigor.draytek.com. *****

Thank you **(Mary)** for creating an account.
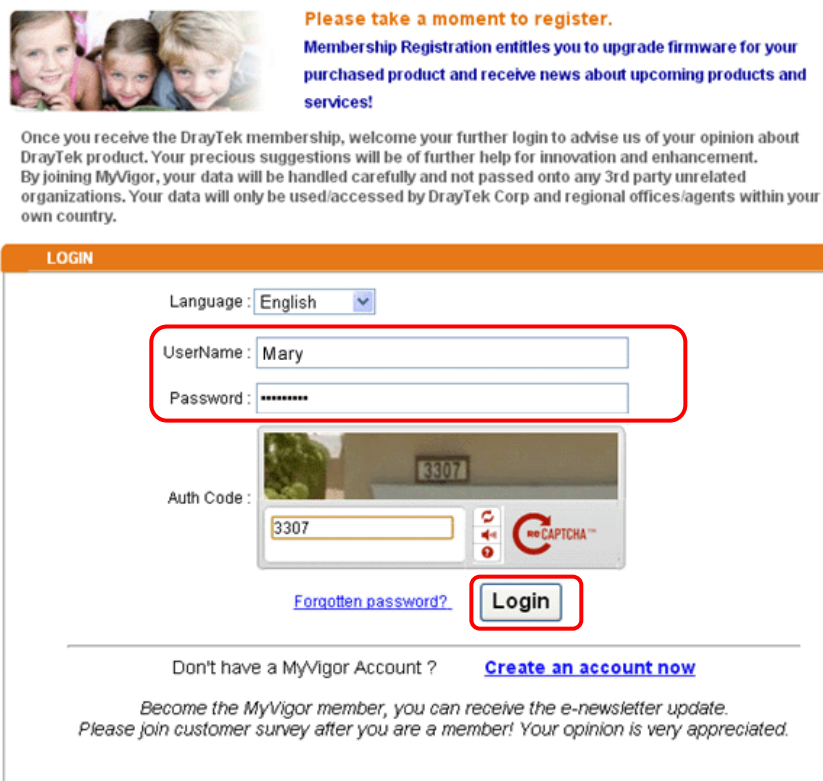
Please click on the activation link below to activate your account

Link : Activate my Account

9. 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**.

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

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

3.5.2 Create an Account via MyVigor Web Site

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

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

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

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

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

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

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

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

Please click on the activation link below to activate your account

Link : <u>Activate my Account</u>

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

Register   Search for this site

Register Confirm

The Confirm message of New Owner(Mary) maybe timeout
Please try again or contact to draytek.com

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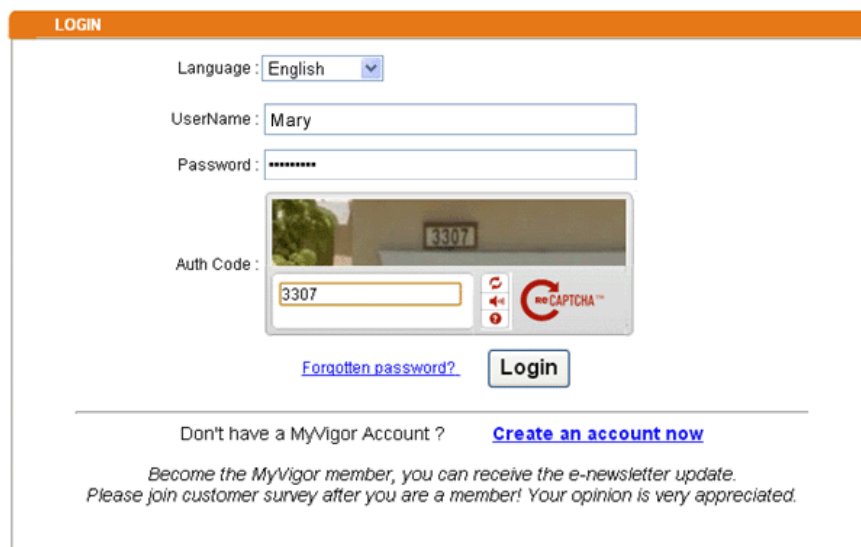
8. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**. Then type the code in the box of Auth Code according to the value displayed on the right side of it.

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

Once you receive the DrayTek membership, welcome your further login to advise us of your opinion about DrayTek product. Your precious suggestions will be of further help for innovation and enhancement. By joining MyVigor, your data will be handled carefully and not passed onto any 3rd party unrelated organizations. Your data will only be used/accessed by DrayTek Corp and regional offices/agents within your own country.

LOGIN

Language : [English ▼]
UserName : Mary
Password : ••••••••
Auth Code : 3307
[3307]

Forgotten password?   [Login]

Don't have a MyVigor Account ?   **Create an account now**

Become the MyVigor member, you can receive the e-newsletter update. Please join customer survey after you are a member! Your opinion is very appreciated.

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

3.6 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection

Follow the steps listed below:

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

2. Configure relational objects first. Open **Object Settings>>SMS/Mail Server Object** to get the following page.

Object Settings >> SMS / Mail Service Object

SMS Provider	Mail Server		Set to Factory Default
Index	**Profile Name**		**SMS Provider**
1.			kotsms.com.tw (TW)
2.			kotsms.com.tw (TW)
3.			kotsms.com.tw (TW)
4.			kotsms.com.tw (TW)
5.			kotsms.com.tw (TW)
6.			kotsms.com.tw (TW)
7.			kotsms.com.tw (TW)
8.			kotsms.com.tw (TW)
9.	Custom 1		
10.	Custom 2		

Index 1 to Index 8 allows you to choose the built-in SMS service provider. If the SMS service provider is not on the list, you can configure Index 9 and Index 10 to add the new service provider to Vigor router.

3. Choose any index number (e.g., Index 1 in this case) to configure the SMS Provider setting. In the following page, type the username and password and set the quota that the router can send the message out.

Object Settings >> SMS / Mail Service Object

Profile Index: 1

Profile Name	Local number
Service Provider	kotsms.com.tw (TW)
Username	abc5026
Password	•••
Quota	3
Sending Interval	3 (seconds)

[OK] [Clear] [Cancel]

DrayTek

4. After finished the settings, click **OK** to return to previous page. Now you have finished the configuration of the SMS Provider profile setting.

Object Settings >> SMS / Mail Service Object

SMS Provider	Mail Server		Set to Factory Default	
Index	**Profile Name**	**SMS Provider**
1.	Local number	kotsms.com.tw (TW)
2.		kotsms.com.tw (TW)
3.		kotsms.com.tw (TW)
4.		kotsms.com.tw (TW)
5.		kotsms.com.tw (TW)
6.		kotsms.com.tw (TW)
7.		kotsms.com.tw (TW)
8.		kotsms.com.tw (TW)
9.	Custom 1	
10.	Custom 2	

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.

Object Settings >> Notification Object

Profile Index: 1

Profile Name	WAN_Notify	
Category	**Status**	
WAN	☑ Disconnected	☑ Reconnected
VPN Tunnel	☐ Disconnected	☐ Reconnected

[OK] [Clear] [Cancel]

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).

Application >> SMS / Mail Alert Service

SMS Provider		Mail Server			Set to Factory Default
Index	SMS Provider	Recipient	Notify Profile	Schedule(1-15)	
1 ☑	1 - Local number	0912345678	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		

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.

DrayTek

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.

Object Settings >> 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	3
Sending Interval	3 (seconds)

OK   Clear   Cancel

3.7 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.
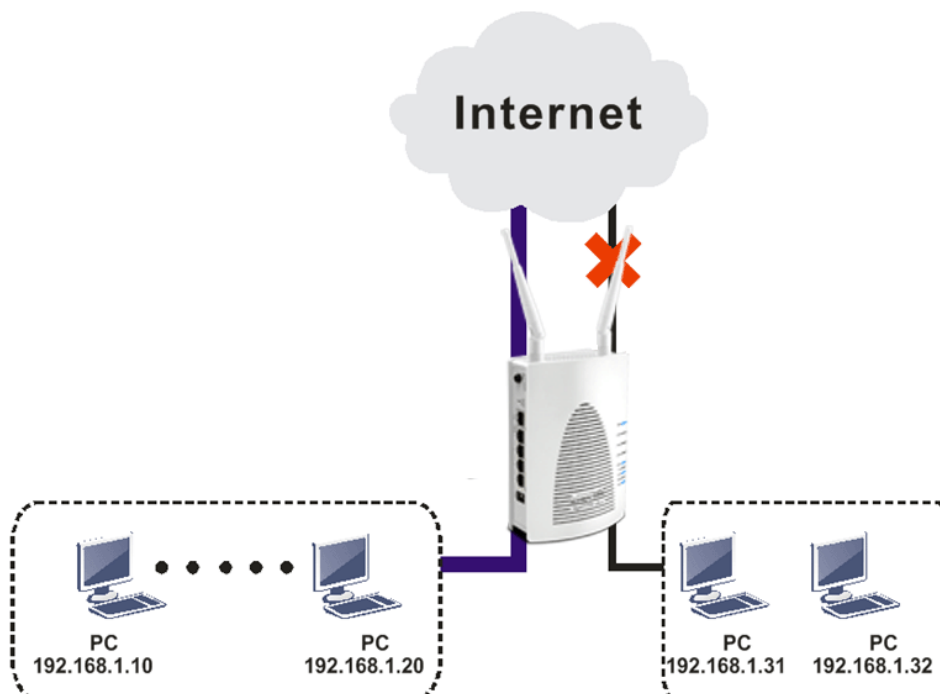
The way we can use is to set two rules under **Firewall**. For **Rule 1** of **Set 2** under **Firewall>>Filter Setup** is used as the default setting, we have to create a new rule starting from Filter Rule 2 of Set 2.

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.

DrayTek

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

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

4. Next, set another rule. Just open **Firewall>>Filter Setup**. Click the **Set 2** link and choose the **Filter Rule 3** button.

5. Check the box of **Check to enable the Filter Rule**. Type the comments (e.g., **open_ip**). Click the **Edit** button for **Source IP**.

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.

DrayTek

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

9. 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.

3.8 How to Block Facebook Service Accessed by the Users via Web Content Filter / URL Content Filter

There are two ways to block the facebook service, Web Content Filter and URL Content Filter.

Web Content Filter,

Benefits: Easily and quickly implement the category/website that you want to block.

Note: License is required.

URL Content Filter,

Benefits: Free, flexible for customize webpage.

Note: Manual setting (e.g., one keyword for one website.)

I. Via Web Content Filter

1.   Make sure the Web Content Filter (powered by Commtouch) license is valid.

2. Open **CSM >> Web Content Filter Profile** to create a WCF profile. Check **Social Networking** with Action**, Block**.

3. Enable 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.

DrayTek

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.

Objects Setting >> Keyword Object Setup

Profile Index : 2

Name	facebook-apps
Contents	apps.facebook

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

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

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

[OK]   [Clear]   [Cancel]

3. Open **CSM>>URL Content Filter Profile**. Click an index number to open the setting page.

4. Configure the settings as the following figure.

CSM >> URL Content Filter Profile

Profile Index: 2

Profile Name:	face.apps
Priority:	Either : URL Access Control First Log: None

1.URL Access Control

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

Action: Group/Object Selections

Block   facebook..   [Edit]

2.Web Feature

☐ Enable Restrict Web Feature

Action:

Pass   ☐ Cookie ☐ Proxy ☐ Upload **File Extension Profile:** None

[OK]   [Clear]   [Cancel]

5. When you finished the above steps, 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.

3.9 How to use SmartMonitor with Vigor2120 series

For the models that support SmartMonitor, you can connect the device installed with SmartMonitor to the monitor port of Vigor router, then all the traffic in other LAN port will forward to the monitor port. But, there is no hardware monitor port for Vigor2120 series. Therefore we need to configure mirror port setting in the web user interface of Vigor2120 for using SmartMonitor.

1. Please go to **LAN > LAN Port Mirror** to setup the mirror port.

LAN >> LAN Port Mirror

LAN Port Mirror

Port Mirror:
⊙Enable ○Disable
Mirror port:
⊙P2   ○P3   ○P4
Mirrored port:
☑P1   ☐P2   ☑P3   ☑P4

Note :The selected mirror port will only serve debug purposes and should not be used as a part of the LAN.

OK

2. Please enable the Port Mirror function first.

3. Select the Mirror port and Mirrored port, the traffics of mirrored ports will be forwarded to mirror port. For example, if we select **P2** as mirror port and mirrored ports are P1, P3 and P4, then P1, P3 and P4 will forward the traffic to P2.

When the LAN Port Mirror is configured correctly, just connect the PC installed with SmartMonitor to the mirror port.

Note: Please pay attention that the mirror port will fail to get IP from Vigor2120. It means that any computer connects to mirror port can not access Vigor2120 or Internet, and only can be used as a "monitor" device.

Advanced Configuration

This chapter will guide users to execute advanced (full) configuration through admin mode operation.

1. Open a web browser on your PC and type **http://192.168.1.1.** The window will ask for typing username and password.

2. Please type "admin/admin" on Username/Password for administration operation.

Now, the **Main Screen** will appear. Be aware that "Admin mode" will be displayed on the bottom left side.

4.1 WAN

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

4.1.1 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 USB Modem

For 3G mobile communication through Access Point is popular more and more, Vigor2120 adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor2120, it can support HSDPA/ UMTS/EDGE/ GPRS/ GSM and the future 3G standard (HSUPA, etc). Vigor2120n-plus with 3G USB Modem allows you to receive 3G 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 four LAN ports on the router to access Internet. Also, they can access Internet via 802.11n wireless function of Vigor2120n-plus, and enjoy the powerful firewall, bandwidth management, VPN features of Vigor2120n-plus series.

After connecting into the router, 3G USB Modem will be regarded as the third WAN port. However, the original WAN1 and WAN2 still can be used and Load-Balance can be done in the router. Besides, 3G USB Modem in WAN3 also can be used as backup device. Therefore,

DrayTek

when WAN1 and WAN2 are not available, the router will use 3.5G for supporting automatically. The supported 3G USB Modem will be listed on DrayTek web site. Please visit www.draytek.com for more detailed information.

Below shows the menu items for **WAN**.

4.1.2 General Setup

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

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

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 WAN2 or choose **Auto negotiation** for determined by the system.

	Auto negotiation
	Auto negotiation
	10M half duplex
	10M full duplex
	100M half duplex
	100M full duplex
	1000M full duplex
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	Display that WAN2 will be activated as Backup interface.

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

4.1.3 Internet Access

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

Available settings are explained as follows:

Item	Description
Index	Display the WAN interface.
Display Name	It shows the name of the WAN1/WAN2 that entered in general setup.
Physical Mode	It shows the physical connection for WAN1(Ethernet) /WAN2(USB) according to the real network connection.
Access Mode	Use the drop down list to choose a proper access mode. Then, click **Details Page** for accessing the settings 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 Pag**e will be changed slightly based on physical mode specified on **WAN>>General Setup**.
IPv6	This button will open different web page (based on Physical Mode) to setup IPv6 Internet Access Mode for WAN interface. If IPv6 service is active on this WAN interface, the color of "IPv6" will become green.

4.1.3.1 Details Page for PPPoE in WAN1

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

Internet Access >> PPPoE

PPPoE Client Mode

PPPoE Setup		PPP/MP Setup	
PPPoE Link	○ Enable ◉ Disable	PPP Authentication	PAP or CHAP ▾
ISP Access Setup		Idle Timeout	-1 second(s)
ISP Name	[ ]	**IP Address Assignment Method (IPCP)** [WAN IP Alias]	
Username	[ ]	Fixed IP	○ Yes ◉ No (Dynamic IP)
Password	[ ]	Fixed IP Address	[ ]
Index(1-15) in **Schedule** Setup:			
=> [ ] , [ ] , [ ] , [ ]		◉ Default MAC Address	
		○ Specify a MAC Address	
WAN Connection Detection		MAC Address:	
Mode	ARP Detect ▾	00 · 1D · AA · 9C · F7 · 35	
Ping IP	[ ]		
TTL:			
MTU	1492 (Max:1492)		
PPPoE Pass-through			
☐ For Wired LAN			
☐ For Wireless LAN			

[OK]

Available settings are explained as follows:

Item	Description
PPPoE Link	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. **Index (1-15) in Schedule Setup -** You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application >> Schedule** web page and you can use the number that you have set in that web page.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. **Mode** – Choose **ARP Detect** or **Ping Detect** for the system

	to execute for WAN detection.
	Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.
	TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.
MTU	It means Max Transmit Unit for packet. The default setting is 1492.
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.
	For Wireless LAN – If you check this box, PCs on the same wireless network can use another set of PPPoE session (different with the Host PC) to access into Internet.
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.
	WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Type the additional WAN IP address and check the Enable box. Then click **OK** to exit the dialog.

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

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

4.1.3.2 Details Page for Static or Dynamic IP in WAN1

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.

DrayTek
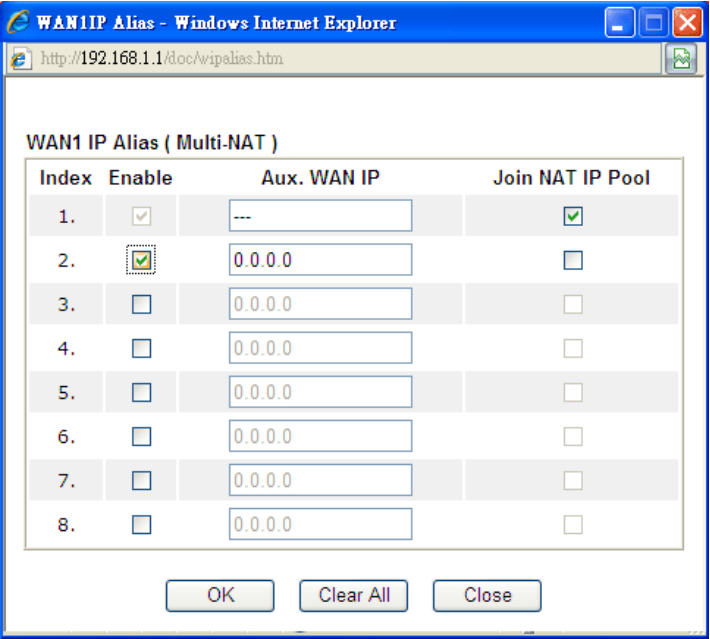
Static or Dynamic IP

Access Control		WAN IP Network Settings [WAN IP Alias]
Broadband Access	⦿ Enable ○ Disable	○ Obtain an IP address automatically (DHCP Client)

Access Control
Broadband Access   ⦿ Enable   ○ Disable

Keep WAN Connection
☐ Enable PING to keep alive
  PING to the IP   0.0.0.0
  PING Interval   0   minute(s)

WAN Connection Detection
  Mode   ARP Detect ▾
  Ping IP
  TTL:

MTU   1492   (Max:1500)

RIP Protocol
☐ Enable RIP

WAN IP Network Settings [WAN IP Alias]
  ○ Obtain an IP address automatically (DHCP Client)
    Router Name   Vigor   *
    Domain Name   *
    * : Required for some ISPs
DHCP Client Identifier for some ISP
  ☐ Enable
    Username
    Password
  ⦿ Specify an IP address
    IP Address   172.16.3.130
    Subnet Mask   255.255.255.0
    Gateway IP Address 172.16.3.1

  ⦿ Default MAC Address
  ○ Specify a MAC Address
    MAC Address:
    00 ·1D ·AA :9C ·F7 ·35

DNS Server IP Address
  Primary IP Address   8.8.8.8
  Secondary IP Address 8.8.4.4

[OK]

Available settings are explained as follows:

Item	Description
Broadband Access	Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.
Keep WAN Connection	Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time. Check **Enable PING to keep alive** box to activate this function. **PING to the IP** - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive. **PING Interval** - Enter the interval for the system to execute the PING operation.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. **Mode** – Choose **ARP Detect** or **Ping Detect** for the system to execute for WAN detection. **Ping IP** – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. **TTL (Time to Live)** – Displays value for your reference. TTL value is set by telnet command.

MTU	It means Max Transmit Unit for packet.
RIP Protocol	Routing Information Protocol is abbreviated as RIP（RFC1058）specifying how routers exchange routing tables information. Click **Enable RIP** for activating this function.
WAN IP Network Settings	This group allows you to obtain an IP address automatically and allows you type in IP address manually. **WAN IP Alias** - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. **Obtain an IP address automatically** – Click this button to obtain the IP address automatically if you want to use **Dynamic IP** mode. - **Router Name**: Type in the router name provided by ISP. - **Domain Name**: Type in the domain name that you have assigned. **DHCP Client Identifier for some ISP** - **Enable:** Check the box to specify username and password as the DHCP client identifier for some ISP. - **Username:** Type a name as username. The maximum length of the user name you can set is 63 characters. - **Password:** Type a password. The maximum length of the password you can set is 62 characters. **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. **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.
DNS Server IP Address	Type in the primary IP address for the router if you want to use **Static IP** mode. If necessary, type in secondary IP address for necessity in the future.

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

4.1.3.3 Details Page for PPTP/L2TP in WAN1

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

Internet Access >> PPTP/L2TP

PPTP/L2TP Client Mode

PPTP/L2TP Setup	PPP Setup
PPTP/L2TP Link ○ Enable PPTP ○ Enable L2TP ● Disable Server Address [ ] Specify Gateway IP Address [172.16.3.1] **ISP Access Setup** Username [ ] Password [ ] Index(1-15) in **Schedule** Setup: => [ ], [ ], [ ], [ ] **MTU** [1460] (Max:1460)	PPP Authentication [PAP or CHAP ▼] Idle Timeout [-1] second(s) **IP Address Assignment Method (IPCP)** Fixed IP ○ Yes ● No (Dynamic IP) Fixed IP Address [ ] **WAN IP Network Settings** ○ Obtain an IP address automatically ● Specify an IP address IP Address [172.16.3.130] Subnet Mask [255.255.255.0]

[OK]

Available settings are explained as follows:

Item	Description
PPTP/L2TP Link	**Enable PPTP-** Click this radio button to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface. **Enable L2TP** - Click this radio button to enable a L2TP client to establish a tunnel to a DSL modem on the WAN interface. **Disable** – Click this radio button to close the connection through PPTP or L2TP. **Server Address** - Specify the IP address of the PPTP/L2TP server if you enable PPTP/L2TP client mode.

Dray Tek

	Specify Gateway IP Address – Specify the gateway IP address for DHCP server.
ISP Access Setup	**Username** -Type in the username provided by ISP in this field. The maximum length of the user name you can set is 63 characters.
	Password -Type in the password provided by ISP in this field. The maximum length of the password you can set is 62 characters.
	Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application >> Schedule** web page and you can use the number that you have set in that web page.
MTU	It means Max Transmit Unit for packet.
PPP 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)	**Fixed IP** - Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Click **Yes** to use this function and type in a fixed IP address in the box.
	Fixed IP Address -Type a fixed IP address.
WAN IP Network Settings	**Obtain an IP address automatically** – Click this button to obtain the IP address automatically.
	Specify an IP address – Click this radio button to specify some data.
	● **IP Address** – Type the IP address.
	● **Subnet Mask** – Type the subnet mask.

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

4.1.3.4 Details Page for 3G/4G USB Modem (PPP mode) in WAN2

To use **3G/4G USB Modem (PPP mode)** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **3G/4G USB Modem (PPP mode)** for WAN2. The following web page will be shown.

Available settings are explained as follows:

Item	Description
3G /4G USB Modem (PPP mode)	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.
SIM PIN code	Type PIN code of the SIM card that will be used to access Internet. The maximum length of the PIN code you can set is 15 characters.
Modem Initial String	Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP. The maximum length of the string you can set is 47 characters.

APN Name	APN means Access Point Name which is provided and required by some ISPs. Type the name and click **Apply**. The maximum length of the name you can set is 43 characters.
Modem Initial String2	The initial string 1 is shared with APN. In some cases, user may need another initial AT command to restrict 3G band or do any special settings. The maximum length of the string you can set is 47 characters.
Modem Dial String	Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP. The maximum length of the string you can set is 31 characters.
Service Name	Enter the description of the specific network service.
PPP Username	Type the PPP username (optional). The maximum length of the name you can set is 63 characters.
PPP Password	Type the PPP password (optional). The maximum length of the password you can set is 62 characters.
PPP Authentication	Select **PAP only** or **PAP or CHAP** for PPP.
Index (1-15) in Schedule Setup	You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application >> Schedule** web page and you can use the number that you have set in that web page
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. **Mode** – Choose **ARP Detect** or **Ping Detect** for the system to execute for WAN detection. **Ping IP** – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. **TTL (Time to Live)** – Displays value for your reference. TTL value is set by telnet command.

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

4.1.3.5 Details Page for 3G/4G USB Modem (DHCP mode) in WAN2

To use **3G/4G USB Modem (DHCP mode)** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **3G/4G USB Modem (DHCP mode)** for WAN2. The following web page will be shown.

Available settings are explained as follows:

Item	Description
3G/4G USB Modem (DHCP mode)	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.
SIM PIN code	Type PIN code of the SIM card that will be used to access Internet. The maximum length of the PIN code you can set is 15 characters.
Network Mode	Force Vigor router to connect Internet with the mode specified here. If you choose 4G/3G/2G as network mode, the router will choose a suitable one according to the actual wireless signal automatically.
APN Name	APN means Access Point Name which is provided and required by some ISPs. Type the name and click **Apply**. The maximum length of the name you can set is 43 characters.
MTU	It means Max Transmit Unit for packet. The default setting is 1380.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. **Mode** – Choose **ARP Detect** or **Ping Detect** for the system

	to execute for WAN detection.
	Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.
	TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.

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

4.1.3.6 Details Page for IPv6 – Offline in WAN1/WAN2

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

4.1.3.7 Details Page for IPv6 – PPP in WAN1/WAN2

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.

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

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

4.1.3.8 Details Page for IPv6 – TSPC in WAN1/WAN2

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.

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

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

DrayTek

4.1.3.9 Details Page for IPv6 – AICCU in WAN1/WAN2

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.
Confirm Password	Type the password again to make the confirmation.
Tunnel Broker	Type the address for the tunnel broker IP, FQDN or an optional port number.
Subnet Prefix	Type the subnet prefix address obtained from service provider. The maximum length of the prefix you can set is 128 characters.

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

4.1.3.10 Details Page for IPv6 – DHCPv6 Client in WAN1

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

Available settings are explained as follows:

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

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

4.1.3.11 Details Page for IPv6 – Static IPv6 in WAN1

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

Internet Access >> IPv6

IPv6 Mode

Internet Access Mode

Connection Type   [Static IPv6 ▼]

Static IPv6 Address Configuration

IPv6 Address   / Prefix Length

[   ] / [   ] [Add] [Delete]

Current IPv6 Address Table

Index IPv6 Address/Prefix Length   Scope

[OK]

Available settings are explained as follows:

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

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

4.1.3.12 Details Page for IPv6 – 6in4 Static Tunnel in WAN1

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.

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

4.1.3.13 Details Page for IPv6 – 6rd in WAN1

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

Available settings are explained as follows:

Item	Description
6rd Mode	**Auto 6rd** – Retrieve 6rd prefix automatically from 6rd service provider. The IPv4 WAN must be set as "DHCP". **Static 6rd -** Set 6rd options manually.
IPv4 Border Relay	Type the IPv4 addresses of the 6rd Border Relay for a given 6rd domain.
IPv4 Mask Length	Type a number of high-order bits that are identical across all CE IPv4 addresses within a given 6rd domain. It may be any value between 0 and 32.
6rd Prefix	Type the 6rd IPv6 address.
6rd Prefix Length	Type the IPv6 prefix length for the 6rd IPv6 prefix in number of bits.

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

Dray Tek

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

4.1.4 Multi-VLAN

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

General

This page shows the basic configurations used by every channel.

WAN >> Multi-VLAN

Multi-VLAN

General				
Channel	Enable	WAN Type	VLAN Tag	Port-based Bridge
1	Yes	Ethernet(WAN1)	None	
3. WAN3	No	Ethernet(WAN1)	None	☐ Enable ☐ P1 ☐ P2 ☐ P3 ☐ P4
4. WAN4	No	Ethernet(WAN1)	None	☐ Enable ☐ P1 ☐ P2 ☐ P3 ☐ P4
5. WAN5	No	Ethernet(WAN1)	None	☐ Enable ☐ P1 ☐ P2 ☐ P3 ☐ P4
6.	No	Ethernet(WAN1)	None	☐ Enable ☐ P1 ☐ P2 ☐ P3 ☐ P4
7.	No	Ethernet(WAN1)	None	☐ Enable ☐ P1 ☐ P2 ☐ P3 ☐ P4
8.	No	Ethernet(WAN1)	None	☐ Enable ☐ P1 ☐ P2 ☐ P3 ☐ P4

[OK]   [Cancel]

Available settings are explained as follows:

Item	Description
Channel	Display the number of each channel. Channel 1 is used by the Internet Access web user interface and can not be configured here. Channels 3 ~ 8 are configurable.
Enable	Display whether the settings in this channel are enabled (Yes) or not (No).
WAN Type	Displays the physical medium that the channel will use.
VLAN Tag	Displays the VLAN tag value that will be used for the packets traveling on this channel.
Port-based Bridge	The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value. **Enable** - Check this box to enable the port-based bridge function on this channel. **P1 ~ P4** – Check the box(es) to build bridge connection on LAN.

Click any index (6~ 8) to get the following web page:

Dray Tek

Multi-VLAN Channel 6: ⊙ **Enable** ○ **Disable**
WAN Type : Ethernet(WAN1) ▾

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

Bridge mode
☑ Enable
  Physical Members
  ☐ P1 ☐ P2 ☐ P3 ☐ P4
Note: P1 is reserved for NAT use, and cannot be configured for bridge mode.

[OK]   [Cancel]

Available settings are explained as follows:

Item	Description
Multi-VLAN Channel (6~8)	**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.
Bridge mode	**Enable –** Click it to enable Bridge mode for such channel. **Physical Members –** Group the physical ports by checking the corresponding check box(es) for applying the bridge connection.

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

WAN >> Multi-VLAN >> Channel 5

Multi-VLAN Channel 5: ⦿ Enable ○ Disable
WAN Type :   Ethernet(WAN1) ▾

General Settings
  VLAN Header
  VLAN Tag: [0]
  Priority: [0 ▾]
Note: Tag value must be set between 1~4095 and unique for each channel.
       Only one channel can be untagged (equal to 0) at a time.

☐ Open Port-based Bridge Connection for this Channel
Physical Members
☐ P1 ☐ P2 ☐ P3 ☐ P4
Note: P1 is reserved for NAT use, and cannot be configured for bridge mode.
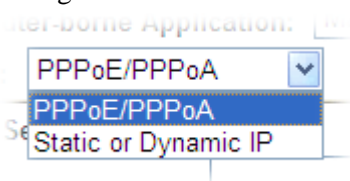
☐ Open WAN Interface for this Channel
  WAN Application: [Management ▾]
  WAN Setup: [Static or Dynamic IP ▾]

ISP Access Setup		WAN IP Network Settings	
ISP Name	[ ]	○ Obtain an IP address automatically	
Username	[ ]	Router Name	[Vigor] *
Password	[ ]	Domain Name	[ ] *
PPP Authentication	[PAP or CHAP ▾]	*: Required for some ISPs	
☑ Always On		⦿ Specify an IP address	
Idle Timeout	[-1] second(s)	IP Address	[ ]
IP Address From ISP		Subnet Mask	[ ]
Fixed IP ○ Yes ⦿ No (Dynamic IP)		Gateway IP Address	[ ]
Fixed IP Address	[ ]	DNS Server IP Address	
		Primary IP Address	[8.8.8.8]
		Secondary IP Address	[8.8.4.4]

[OK]   [Cancel]

Available settings are explained as follows:

Item	Description
Multi-VLAN Channel (3~5)	**Enable** – Click it to enable the configuration of this channel. **Disable** – Click it to disable the configuration of this channel.
WAN Type	The connections and interfaces created in every channel may select a specific WAN type to be built upon. In the Multi-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 Port-based Bridge Connection for this Channel	The settings here will create a bridge between the LAN ports selected and the WAN. The WAN interface of the bridge connection will be built upon the WAN type selected using the VLAN tag configured.
	Physical Members – Group the physical ports by checking the corresponding check box(es) for applying the port-based bridge connection.
Open WAN Interface for this Channel	Check the box to enable relating function.
	WAN for Router-borne Application - Management can be specified for general management (Web configuration/telnet/TR069). If you choose Management, the configuration for this VLAN will be effective for Web configuration/telnet/TR069.
	IPTV - The IPTV configuration will allow the WAN interface to send IGMP packets to IPTV servers.
	WAN Setup – Choose **PPPoE/PPPoA** or **Static or Dynamic IP** to determine what WAN settings must be configured.
ISP Access Setup, IP Address From ISP, WAN IP Network Settings, DNS Server IP Address	For other settings, refer to **Details Page for PPPoE / Static or Dynamic IP in WAN1.**

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

4.2 LAN

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

4.2.1 Basics of LAN

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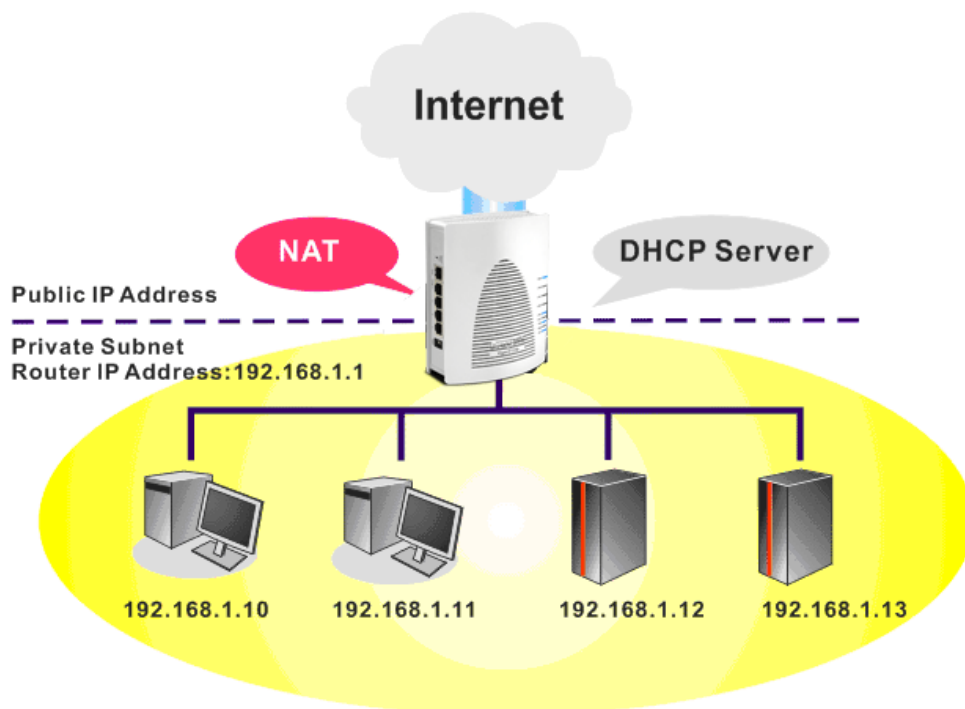
In some special case, you may have a public IP subnet from your ISP such as 220.135.240.0/24. This means that you can set up a public subnet or call second subnet that each host is equipped with a public IP address. As a part of the public subnet, the Vigor router will serve for IP routing to help hosts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

DrayTek
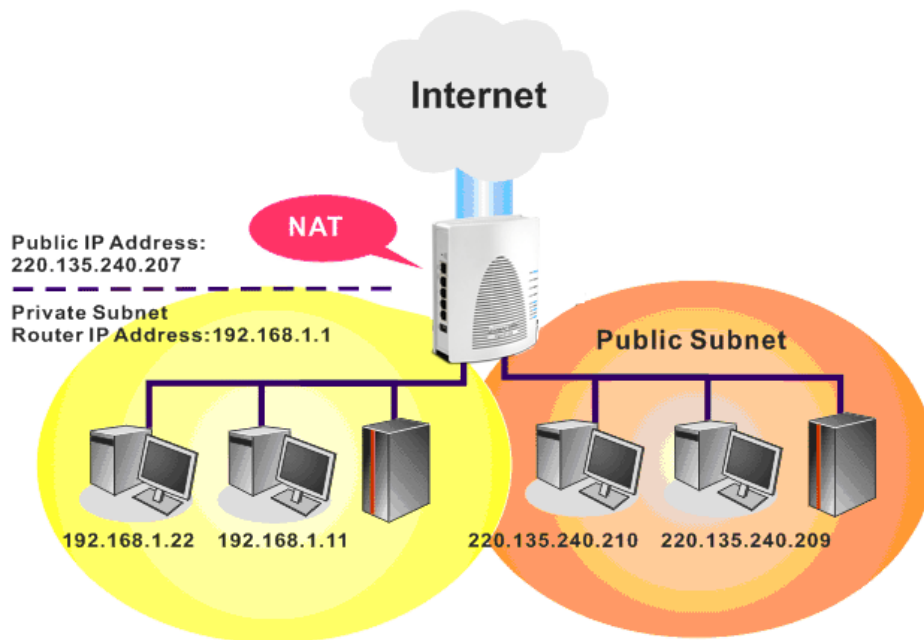
What is Routing Information Protocol (RIP)

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.

4.2.2 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 two subnets provided by the router which allow users to divide groups into different subnets (LAN1 – LAN2). 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 can be operated under **NAT** or **Route** mode. IP Routed Subnet can be operated under Route mode.

LAN >> General Setup

General Setup

Index	Status	DHCP	IP Address		
LAN 1	V	V	192.168.1.1	Details Page	IPv6
LAN 2	☐	☑	192.168.2.1	Details Page	
IP Routed Subnet	☐	☑	192.168.0.1	Details Page	

[Advanced] You can configure DHCP options here.

Inter-LAN Routing

Subnet	LAN 1	LAN 2
LAN 1	☑	☐
LAN 2	☐	☑

Note: LAN 2 is available when VLAN is enabled.

[OK]

Each item is explained as follows:

Item	Description
General Setup	Allow to configure settings for each subnet respectively.
	Index - Display all of the LAN items.
	Status- Basically, LAN1 status is enabled in default. LAN2, LAN3, LAN3 and IP Routed Subnet can be observed by checking the box of **Status**.
	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.

Dray Tek

Advanced	When the router receives the DHCP request from LAN client, the router will assign an IP with the DHCP packets adding option number and data information.
	
	LAN >> General Setup
	
	DHCP Server Options Status
	Options List
	Enable Interface Option Type Data
	
	Enable: ☑
	Interface: All LAN1 LAN2 IP Routed Subnet
	               ☐ ☑ ☐ ☐
	Option Number: [ ]
	DataType: ⊙ ASCII Character (EX :Option:18, Data:/path)
	          ○ Hexadecimal Digit (EX: Option:18, Data:2f70617468)
	          ○ Address List (EX :Option:44, Data:172.16.2.10,172.16.2.20…)
	Data: [ ]
	        [Add] [Update] [Delete]
	
	Enable – Check the box to enable the function of DHCP Option. Each DHCP option is composed by an option number with data. For example,
	
	  Option number:100
	  Data: abcd
	
	When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets.
	
	Interface – Choose the interface for applying such option.
	
	Option Number – Type a number for such function.
	
	DataType – Choose the type (ASCII or Hex or Address) for the data to be stored.
	
	Data – Type the content of the data to be processed by the function of DHCP option.

Inter-LAN Routing	Check the box to link two or more different subnets (LAN and LAN).

DrayTek

4.2.2.1 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	⊙ Enable Server ○ Disable Server
IP Address 192.168.1.1	☐ Enable Relay Agent
Subnet Mask 255.255.255.0	Start IP Address 192.168.1.10
	IP Pool Counts 200
RIP Protocol Control Disable ▾	Gateway IP Address 192.168.1.1
	Lease Time 86400 (s)
	☑ Retrieve IPs from inactive clients periodically
	DNS Server IP Address
	Primary IP Address
	Secondary IP Address

OK

Available settings are explained as follows:

Item	Description
Network Configuration	**For NAT Usage,** ● **IP Address** - Type in private IP address for connecting to a local private network (Default: 192.168.1.1). ● **Subnet Mask -** Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24) **RIP Protocol Control,** ● **Disable** deactivates the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default) ● **Enable** activates the RIP 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. **Enable Server -** Let the router assign IP address to every host in the LAN. **Disable Server –** Let you manually assign IP address to

every host in the LAN.

Enable Relay Agent – Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.

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

Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.

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

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

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

Retrieve IPs from inactive clients periodically - Whenever a DHCP client requests an IP address from the LAN DHCP server, the server will give out an IP to this client for a certain amount of time (e.g., 1 day). However, even if this client only uses the IP for say 5 minutes, the server still "reserves" 1 day for that client. Because a DHCP server only has a limited number of IPs to lease to its DHCP clients, soon enough all the IPs will be used out and then no one will be able to get any IPs from this server anymore. Therefore, this feature is used to get the IP back from inactive clients (i.e. doesn't use the IP but the server still reserves the IP for him).

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

Primary IP Address -You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field.

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

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

Dray Tek

Online Status

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

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

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

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

4.2.2.2 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 **RADVD**(stateless) and the other is **DHCPv6 Server** (Stateful).

Available settings are explained as follows:

Item	Description
Router Advertisement Server	**Enable** – Click it to enable router advertisement server. The router advertisement daemon sends Router Advertisement messages, specified by RFC 2461, to a local Ethernet LAN periodically and when requested by a node sending a Router Solicitation message. These messages are required for IPv6 stateless auto-configuration.
	Disable – Click it to disable router advertisement server.
	Advertisement Lifetime - The lifetime associated with the default router in units of seconds. It's used to control the lifetime of the prefix. The maximum value corresponds to 18.2 hours. A lifetime of 0 indicates that the router is not a default router and should not appear on the default router list.
DHCPv6 Server Configuration	**Enable Server** –Click it to enable DHCPv6 server. DHCPv6 Server could assign IPv6 address to PC according to the Start/End IPv6 address configuration.
	Disable Server –Click it to disable DHCPv6 server.
	Start IPv6 Address / **End IPv6 Address** –Type the start and end address for IPv6 server.
DNS Server IPv6 Address	**Primary DNS Sever** – Type the IPv6 address for Primary DNS server.
	Secondary DNS Server –Type another IPv6 address for DNS server if required.
Static IPv6 Address configuration	**IPv6 Address** –Type static IPv6 address for LAN.
	Prefix Length – Type the fixed value for prefix length.
	Add – Click it to add a new entry.
	Delete – Click it to remove an existed entry.
Current IPv6 Address Table	Display current used IPv6 addresses.

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

4.2.3 Static Route

Go to **LAN** 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.

Static Route for IPv4

LAN >> Static Route Setup

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

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

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.
View 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
Index	The number (1 to 10) under Index allows you to open next page to set up static route.
Destination Address	Displays the destination address of the static route.
Status	Displays the status of the static route.

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

LAN >> Static Route Setup

Index No. 1

☐ Enable

Destination IP Address   ???

Subnet Mask

Gateway IP Address

Network Interface   LAN1 ▾

                     LAN1

[OK] [Cancel]   LAN2

                     WAN1

                     WAN2

Available settings are explained as follows:

Item	Description
Enable	Check 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 IP address as the gateway for such route.
Network Interface	Use the drop down list to specify an interface for such static route.

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

Static Route for IPv6

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

LAN >> Static Route Setup

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

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

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

Each item is explained as follows:

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

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

LAN >> Static Route Setup

Index No. 1

☑ Enable

Destination IPv6 Address / Prefix Len   :: / 0

Gateway IPv6 Address

Network Interface   LAN

[OK]   [Cancel]   [Delete]

Available settings are explained as follows:

Item	Description
Enable	Check it to enable this profile.

DrayTek

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. LAN ▼ LAN WAN1

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

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

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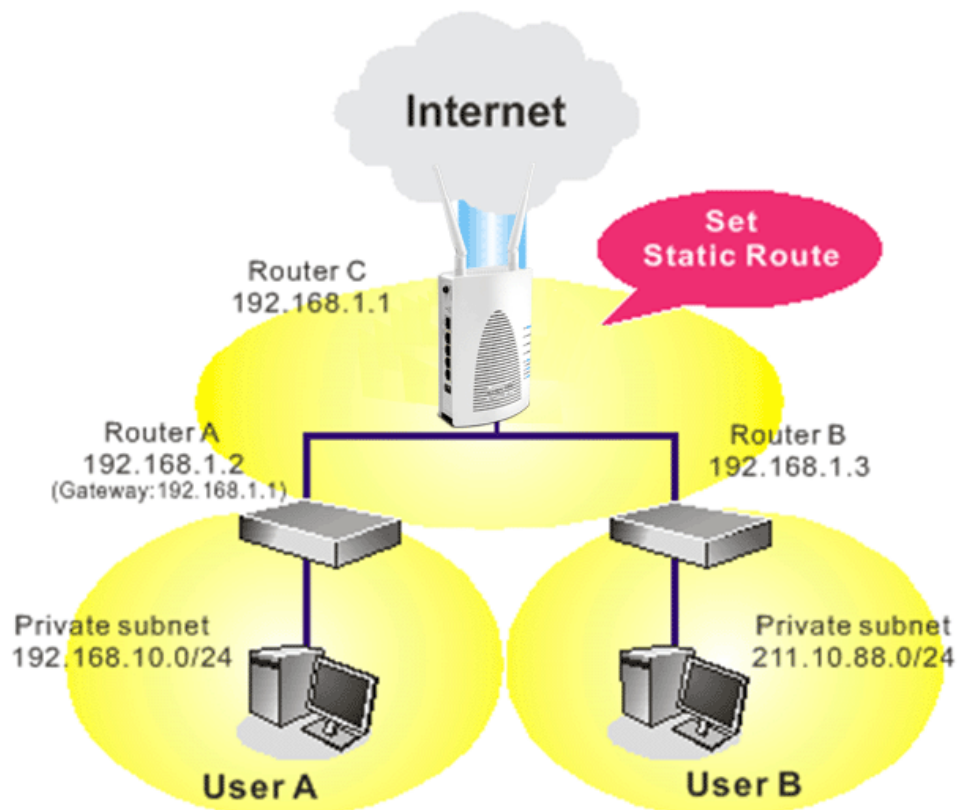
1. Go to **LAN** page and click **General Setup**, select 1st Subnet as the **RIP Protocol Control.** Then click the **OK** button.

> **Note:** There are two reasons that we have to apply RIP Protocol Control on 1st Subnet. The first is that the LAN interface can exchange RIP packets with the neighboring 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**.

LAN >> Static Route Setup

Index No. 1

☑ Enable

Destination IP Address	192.168.1.10
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.2
Network Interface	LAN1

[OK] [Cancel] [Delete]

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**.

LAN >> Static Route Setup

Index No. 2

☑ Enable

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

[OK] [Cancel] [Delete]

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

Diagnostics >> View Routing Table

| Current Running Routing Table | IPv6 Routing Table | | Refresh | |

```
Key: C - connected, S - static, R - RIP, * - default, ~ - private
S~      192.168.10.0/ 255.255.255.0    via 192.168.1.2      LAN1
C~      192.168.1.0/ 255.255.255.0     directly connected   LAN1
S~      211.100.88.0/ 255.255.255.0    via 192.168.1.3      LAN1
```

4.2.4 VLAN

With the 4-port Gigabit switch on the LAN side, Vigor router provides extremely high speed connectivity for the highest speed local data transfer of any server or local PCs. On the Wireless-equipped model (Vigor2120n-plus), each of the wireless SSIDs can also be grouped within one of the VLANs.

Tagged VLAN

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

Port-Based VLAN

Relative to tag-based VLAN which groups clients with an identifier, port-based VLAN uses physical ports (P1 ~ P4) to separate the clients into different VLAN group.

Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. The multi-subnet can let a small businesses have much better isolation for multi-occupancy applications. Go to **LAN** page and select **VLAN**. The following page will appear. Click **Enable** to invoke VLAN function.

LAN >> VLAN Configuration

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

Available settings are explained as follows:

Item	Description
Enable	Click it to enable VLAN configuration.
LAN	**P1 – P4** – Check the LAN port(s) to be grouped under the selected VLAN.
Wireless LAN (2.4GHz)	**SSID1 – SSID4 –** Check the SSID boxes to group them under the selected VLAN.
Wireless LAN (5GHz)	**SSID1 – SSID4 –** Check the SSID boxes to group them under the selected VLAN.
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.

DrayTek

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.
	Priority – Type the packet priority number for such VLAN. The range is from 0 to 7.

> **Note:** Leave one VLAN untagged at least to prevent from not connecting to Vigor router due to unexpected error.

To add or remove a VLAN, please refer to the following example.

1. If, VLAN 0 is consisted of hosts linked to P1 and P2 and VLAN 1 is consisted of hosts linked to P3 and P4. VLAN0 and VLAN1 are configured with different subnets.

2. After checking the box to enable VLAN function, you will check the table according to the needs as shown below. Click **OK** to save the settings.

LAN >> VLAN Configuration

VLAN Configuration

☑Enable

	LAN				Wireless LAN(2.4GHz)				Wireless LAN(5GHz)				Subnet	VLAN Tag		
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	SSID1	SSID2	SSID3	SSID4		Enable	VID	Priority
VLAN0	☑	☑	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	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 ▾

1. For each VLAN row, if enable is checked for the VLAN Tag then the corresponding VID will be applied to wired LAN traffic.
2. Wireless LAN traffic is always untagged, but will still be a member of the VLAN group selected.
3. Each VID must be unique.

[OK] [Clear] [Cancel]

3. To remove VLAN, uncheck the needed box and click **OK** to save the results.

4.2.5 Bind IP to MAC

This function is used to bind the IP and MAC address in LAN to have a strengthening control in network. When this function is enabled, all the assigned IP and MAC address binding together cannot be changed. If you modified the binding IP or MAC address, it might cause you not access into the Internet.

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

Available settings are explained as follows:

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

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

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

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

4.2.6 LAN Port Mirror

LAN port mirror can be applied for the users in LAN. Generally speaking, this function copies traffic from one or more specific ports to a target port. This mechanism helps manager track the network errors or abnormal packets transmission without interrupting the flow of data access the network. By the way, user can apply this function to monitor all traffics which user needs to check.

There are some advantages supported in this feature. First, it is more economical without other detecting equipments to be set up. Second, it may be able to view traffic on one or more ports within a VLAN at the same time. Third, it can transfer all data traffics to be mirrored to one analyzer connecting to the mirroring port. Last, it is more convenient and easy to configure in user's interface.

LAN >> LAN Port Mirror

LAN Port Mirror

Port Mirror:
⊙ Enable   ○ Disable
Mirror port:
○ P2   ○ P3   ○ P4
Mirrored port:
☐ P1   ☐ P2   ☐ P3   ☐ P4

Note: The selected mirror port will only serve debug purposes and should not be used as a part of the LAN.

[OK]

Available settings are explained as follows:

Item	Description
Port Mirror	Check **Enable** to activate this function. Or, check **Disable** to close this function.
Mirror Port	Select a port to view traffic sent from mirrored ports.
Mirrored port	Select which ports are necessary to be mirrored.

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

Dray Tek

4.2.7 Web Portal Setup

This page allows you to configure a profile with specified URL for accessing into or display a message when a wireless/LAN user connects to Internet through this router. No matter what the purpose of the wireless/LAN client is, he/she will be forced into the URL configured here while trying to access into the Internet or the desired web page through this router. That is, a company which wants to have an advertisement for its products to users can specify the URL in this page to reach its goal.

> For the telnet command usage, please refer to "*Telnet Command: wptl*" in the chapter of Telnet Command Reference.

LAN >> Web Portal Setup

Web Portal Table:

Profile	Status	Interface	
1.	Disable	None	Preview
2.	Disable	None	Preview
3.	Disable	None	Preview
4.	Disable	None	Preview

Note: Internet access must be enabled while webpage redirection is about to enable.

Each item is explained as follows:

Item	Description
Profile	Display the number link which allows you to configure the profile.
Status	Display the content (Disable, URL Redirect or Message) of the profile.
Interface	Display the applied interfaces of the profile.
Preview	Open a preview window according to the configured settings.

To configure the profile, click any index number link to open the following page.

Available settings are explained as follows:

Item	Description
Disable	Click this button to close this function.
URL Redirect	Any user who wants to access into Internet through this router will be redirected to the URL specified here first. It is a useful method for the purpose of advertisement. For example, force the wireless user(s) in hotel to access into the web page that the hotel wants the user(s) to visit.
Message	Type words or sentences here. The message will be displayed on the screen for several seconds when the wireless users access into the web page through the router.
Applied Interfaces	Check the box(es) representing different interfaces to be applied by such profile. The advantage is that each SSID (1/2/3/4) for wireless network can be applied with different web portal separately.

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

4.3 NAT

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

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

The benefit of the NAT includes:

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

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

> **Note:** 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.

Below shows the menu items for NAT.

4.3.1 Port Redirection

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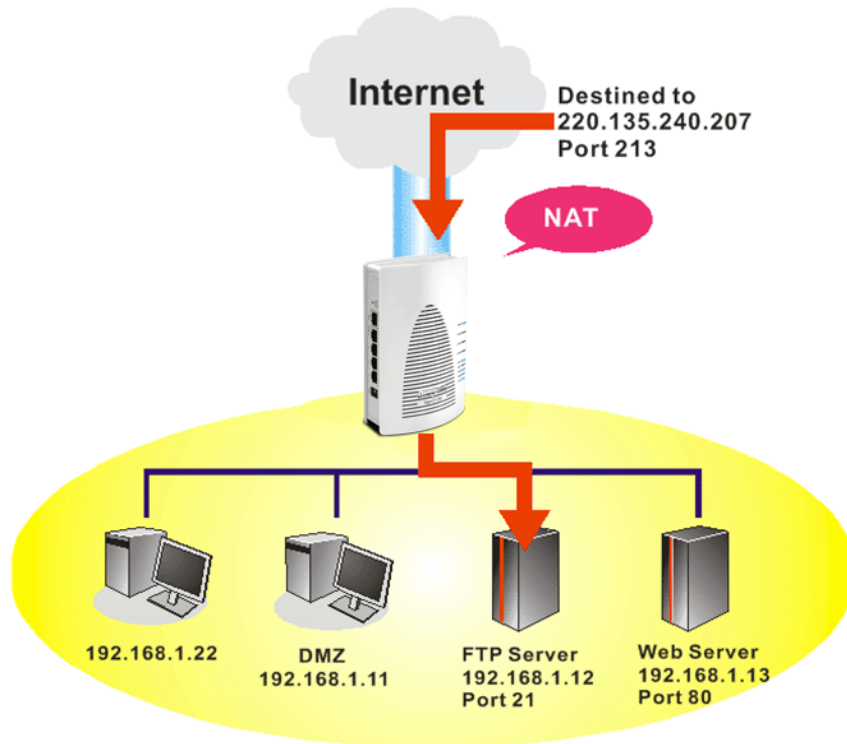
The port redirection can only apply to incoming traffic.

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

NAT >> Port Redirection

Index	Service Name	WAN Interface	Protocol	Public Port	Private IP	Status
1.		All				x
2.		All				x
3.		All				x
4.		All				x
5.		All				x
6.		All				x
7.		All				x
8.		All				x
9.		All				x
10.		All				x

<< 1-10 | 11-20 >>   Next >>

Note: The configured ports in the **Management** and **SSL VPN** webUIs will be used by the router and not be sent to the local computer defined here.

Each item is explained as follows:

Item	Description
Index	Display the number of the profile.
Service Name	Display the description of the specific network service.
WAN Interface	Display the WAN IP address used by the profile.

Protocol	Display the transport layer protocol (TCP or UDP).
Public Port	Display the port number which will be redirected to the specified **Private IP and Port** of the internal host.
Private IP	Display the IP address of the internal host providing the service.
Status	Display if the profile is enabled (v) or not (x).

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

Available settings are explained as follows:

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

Private IP	Specify the private IP address of the internal host providing the service. If you choose Range as the port redirection mode, you will see two boxes on this field. Type a complete IP address in the first box (as the starting point). The second one will be assigned automatically later.
Private Port	Specify the private port number of the service offered by the internal host.

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

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

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

4.3.2 DMZ Host

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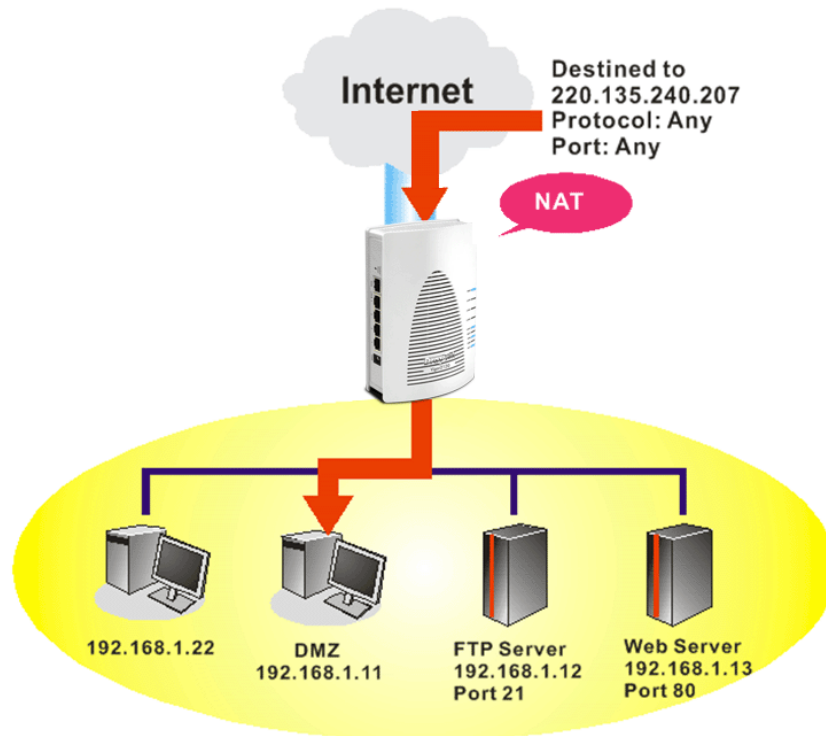
The security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

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

Available settings are explained as follows:

Item	Description
WAN 1 None ▼ None Private IP Active True IP	Choose **Private IP** or **Active True IP** first. **Active True IP** selection is available for WAN1 only.
Private IP	Enter the private IP address of the DMZ host, or click Choose PC to select one.
Choose PC	Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host. 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 following screen. Click **OK** to save the setting. NAT >> DMZ Host Setup **DMZ Host Setup** WAN1 | WAN2 | WAN3 **WAN 1** Private IP ▼ Private IP 192.168.1.49 Choose PC MAC Address of the True IP DMZ Host 00 . 00 . 00 . 00 . 00 . 00 Note: When a True-IP DMZ host is turned on, it will force the router's WAN connection to be always on. OK

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

NAT >> DMZ Host Setup

DMZ Host Setup

	WAN1			
WAN 1				
Index	**Enable**	**Aux. WAN IP**	**Private IP**	
1.	☐	172.16.3.130	0.0.0.0	Choose IP
2.	☐	172.16.3.149	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 PC	Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.
	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 following screen. Click **OK** to save the setting.
	NAT >> DMZ Host Setup
	DMZ Host Setup
	WAN1
	WAN 1
	Index **Enable** **Aux. WAN IP** **Private IP**
	1. ☐ 172.16.3.130 0.0.0.0 Choose IP
	2. ☑ 172.16.3.149 192.168.1.10 Choose IP
	OK Clear

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

4.3.3 Open Ports

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

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

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

Available settings are explained as follows:

Item	Description
Index	Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.
Comment	Specify the name for the defined network service.
WAN Interface	Display the WAN interface used by such index.
Aux. WAN IP	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.
Local IP Address	Display the private IP address of the local host offering the service.
Status	Display the state for the corresponding entry. X or V is to represent the **Inactive** or **Active** state.

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

NAT >> Open Ports >> Edit Open Ports

Index No. 1

☑ Enable Open Ports

Comment	P2261	
WAN Interface	WAN1 ▾	
WAN IP	172.16.3.130 ▾	
Private IP	192.168.1.10	Choose IP

	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	TCP ▾	80	80	2.	----- ▾	0	0
3.	----- ▾	0	0	4.	----- ▾	0	0
5.	----- ▾	0	0	6.	----- ▾	0	0
7.	----- ▾	0	0	8.	----- ▾	0	0
9.	----- ▾	0	0	10.	----- ▾	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.
Private IP	Enter the private IP address of the local host or click **Choose PC** to select one. **Choose PC -** Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select the appropriate IP address of the local host in the list.
Protocol	Specify the transport layer protocol. It could be **TCP**, **UDP**, or **-----** (none) for selection.
Start Port	Specify the starting port number of the service offered by the local host.
End Port	Specify the ending port number of the service offered by the local host.

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

NAT >> Open Ports

Open Ports Setup | Set to Factory Default |

Index	Comment	WAN Interface	Aux. WAN IP	Local IP Address	Status
1.	P2261	WAN1	172.16.3.130	192.168.1.10	v
2.					x
3.					x
4.					x
5.					x
6.					x
7.					v

4.3.4 Address Mapping

Address Mapping is used to map a specified private IP or a range of private IPs of NAT subnet into a specified WAN IP (or WAN IP alias IP). Refer to the following figure.
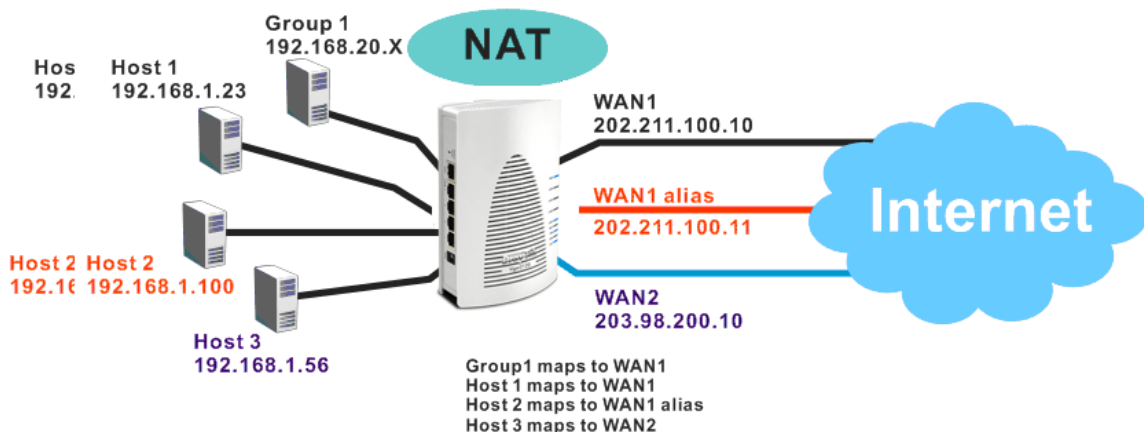
Suppose the WAN settings for a router are configured as follows:

WAN1: 202.211.100.10, WAN1 alias: 202.211.100.11
WAN2: 203.98.200.10

Without address mapping feature, when a NAT host with an IP say "192.168.1.10" sends a packet to the WAN side (or the Internet), the source address of the NAT host will be mapped into either 202.211.100.10 or 203.98.200.10 (which IP or mapping is decided by the internal load balancing algorithm).

With address mapping feature, you can manually configure any host mapping to any WAN interface to fit the request. In the above example, you can configure NAT Host1 to always map to 202.211.100.10 (WAN1); Host2 to always map to 202.211.100.11 (WAN1 alias); Host3 always map to 203.98.200.10 (WAN2) and Group 1 to always map to 202.211.100.10 (WAN1).

NAT >> Address Mapping

Address Mapping Setup | **Set to Factory Default** |

Index	Protocol	Public IP	Private IP	Mask	Status
1.	ALL	---		/32	x
2.	ALL	---		/32	x
3.	ALL	---		/32	x
4.	ALL	---		/32	x
5.	ALL	---		/32	x

Available settings are explained as follows:

Item	Description
Index	Indicate the relative number for the particular entry that you want to configure You should click the appropriate index number to edit or clear the corresponding entry.
Protocol	Display the protocol used for this address mapping.
Public IP	Display the public IP address selected for this entry, e.g., 172.16.3.102.
Private IP	Display the private IP set for this address mapping, e.g., 192.168.1.10.
Mask	Display the subnet mask selected for this address mapping.
Status	Display the status for the entry, enable or disable.

Click the index number link to open the configuration page.

NAT >> Address Mapping

Index No. 1

☐ Enable

Protocol:	ALL ▾
WAN Interface	WAN1 ▾
WAN IP	1-172.16.3.130 ▾
Private IP:	
Subnet Mask:	/32 ▾
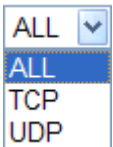
[OK]   [Clear]   [Cancel]

Available settings are explained as follows:

Item	Description
Enable	Check to enable this entry.

Protocol	Specify the transport layer protocol. It could be **TCP**, **UDP**, or **ALL** for selection.
	ALL ▼
	ALL
	TCP
	UDP
WAN Interface	Choose the WAN interface for such address mapping profile.
WAN IP	This is the source IP of a packet captured on the WAN side and sent by a NAT host specified in the **Private IP** field. The drop down menu contains WAN interface IPs and WAN IP alias IPs.
Private IP	This is the source IP of a NAT host which wishes to send packets to the WAN side and have source address as configured in the **WAN IP** field.
Subnet Mask	Select a value of subnet mask for private IP address.

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

4.3.5 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.

Dray Tek

NAT >> Port Triggering

Port Triggering | Set to Factory Default |

Index	Comment	Triggering Protocol	Triggering Port	Incoming Protocol	Incoming Port	Status
1.						x
2.						x
3.						x
4.						x
5.						x
6.						x
7.						x
8.						x
9.						x
10.						x

<< 1-10 | 11-20 >>   Next >>

Available settings are explained as follows:

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

Click the index number link to open the configuration page.

NAT >> Port Triggering

No. 1

☑ Enable

Service   User Defined ▾

Comment

Triggering Protocol   TCP ▾

Triggering Port   80

Incoming Protocol   UDP ▾

Incoming Port   1024
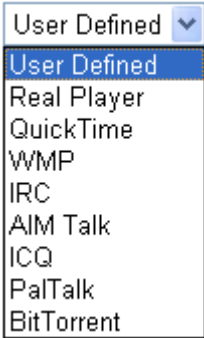
Note: The Triggering Port and Incoming Port should be input like this :
123-456,777-789 (legal),123-456,789 (legal), but 123-456-789 (illegal).

[OK]   [Clear]   [Cancel]

Available settings are explained as follows:

Item	Description
Enable	Check to enable this entry.
Service	Choose the **predefined** service to apply for such trigger profile. User Defined User Defined Real Player QuickTime WMP IRC AIM Talk ICQ PalTalk BitTorrent
Comment	Type the text to memorize the application of this rule.
Triggering Protocol	Select the protocol (TCP, UDP or TCP/UDP) for such triggering profile. --- --- TCP UDP TCP/UDP
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. --- --- TCP UDP TCP/UDP
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.

4.4 Firewall

4.4.1 Basics for Firewall

While the broadband users demand more bandwidth for multimedia, interactive applications, or distance learning, security has been always the most concerned. The firewall of the Vigor 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.
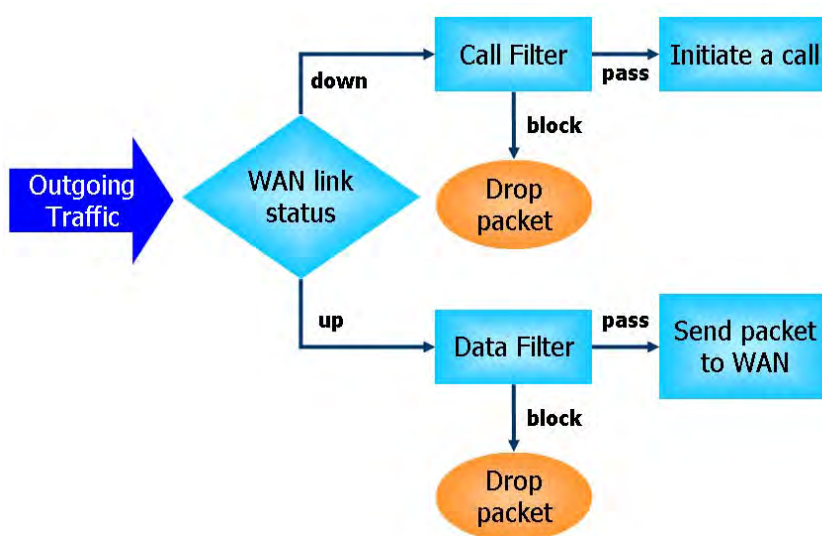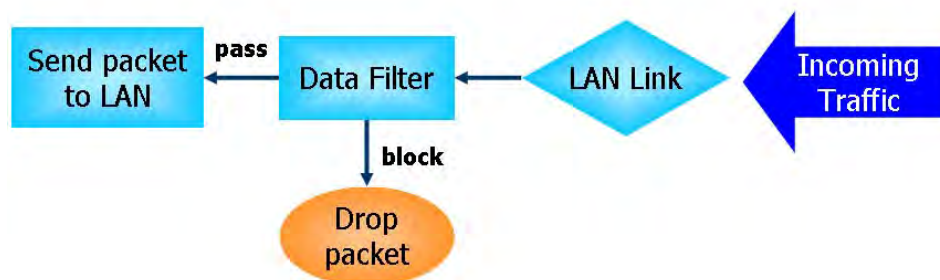
Stateful Packet Inspection (SPI)

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 just examines the header information, but also monitors the state of the connection.

Denial of Service (DoS) Defense

The **DoS Defense** functionality helps you to detect and mitigate the DoS attack. The attacks are usually categorized into two types, the flooding-type attacks and the vulnerability attacks. The flooding-type attacks will attempt to exhaust all your system's resource while the vulnerability attacks will try to paralyze the system by offending the vulnerabilities of the protocol or operation system.

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

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

The below shows the attack types that DoS/DDoS defense function can detect:

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

Below shows the menu items for Firewall.

DrayTek
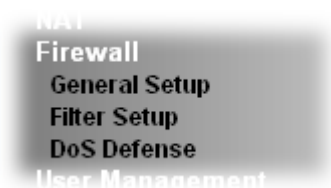
4.4.2 General Setup

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

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

4.4.2.1 General Setup Page

Such page allows you to enable / disable Call Filter and Data Filter, determine general rule for filtering the incoming and outgoing data.

```
Firewall >> General Setup
```

General Setup

| General Setup | Default Rule |

Call Filter   ⦿ Enable   Start Filter Set [Set#1 ▾]
                   ○ Disable
Data Filter   ⦿ Enable   Start Filter Set [Set#2 ▾]
                   ○ Disable

☑ Accept large incoming fragmented UDP or ICMP packets (for some games, ex. CS)
☑ Enable Strict Security Firewall
Block routing packet from WAN
    ☑ IPv4   ☑ IPv6

Note: The packets will be filtered by the following firewall functions sequentially:
1. Data Filter Sets and Rules
2. Block routing packets from WAN
3. Default Rule

[OK]   [Cancel]

Available settings are explained as follows:

Item	Description
Call Filter	Check **Enable** to activate the Call Filter function. Assign a start filter set for the Call Filter.
Data Filter	Check **Enable** to activate the Data Filter function. Assign a start filter set for the Data Filter.
Accept large incoming…	Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor router will reject these fragmented packets to prevent attack unless you enable "**Accept large incoming fragmented UDP or ICMP Packets**". By checking this box, you can play these kinds of on-line games. If security concern is in higher priority, you cannot enable "**Accept large incoming**

	fragmented UDP or ICMP Packets".
Enable Strict Security Firewall	For the sake of security, the router will execute strict security checking for data transmission.
	Such feature is enabled in default. All the packets, while transmitting through Vigor 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/traffics from WAN to LAN are allowed in default.
	IPv6 - 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 - 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.

4.4.2.2 Default Rule Page

Such page allows you to choose filtering profiles including QoS, Policy Route, WCF, APP Enforcement, and URL Content Filter for data transmission via Vigor router.

Firewall >> General Setup

General Setup
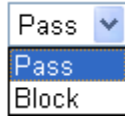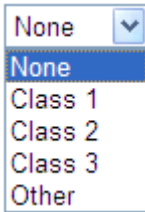
General Setup	Default Rule

Actions for default rule:

Application	Action/Profile	Syslog
Filter	Pass	☐
Sessions Control	29 / 32000	☐
Quality of Service	None	☐
APP Enforcement	None	☐
URL Content Filter	None	☐
Web Content 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. The default setting is 60000.
Quality of Service	Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later.
APP Enforcement	Select an **APP Enforcement** profile for global IM/P2P application blocking. If there is no profile for you to select, please choose **[Create New]** from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the **APP Enforcement** profile selected here. For detailed information, refer to the section of **APP Enforcement** profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
URL Content Filter	Select one of the **URL Content Filter** profile settings (created in **CSM>> URL Content Filter**) for applying with this router. Please set at least one profile for choosing in **CSM>> URL Content Filter** web page first. Or choose **[Create New]** from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for **URL Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
Web Content Filter	Select one of the **Web Content Filter** profile settings (created in **CSM>> Web Content Filter**) for applying with this router. Please set at least one profile for anti-virus in **CSM>> Web Content Filter** web page first. Or choose **[Create New]** from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for **Web Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
Advance Setting	Click **Edit** to open the following window. However, it is

strongly recommended to use the default settings here.

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

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

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

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

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

4.4.3 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

Filter Rule	Active	Comments	Move Up	Move Down
1	☑	Block NetBios		Down
2	☐		UP	Down
3	☐		UP	Down
4	☐		UP	Down
5	☐		UP	Down
6	☐		UP	Down
7	☐		UP	

Next Filter Set None

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.
Move Up/Down	Use **Up** or **Down** link to move the order of the filter rules.
Next Filter Set	Set the link to the next filter set to be executed after the current filter run. Do not make a loop with many filter sets.

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

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 3 Rule 1

☐ Check to enable the Filter Rule
Comments: [_____]
Index(1-15) in Schedule Setup: [____], [____], [____], [____]
Clear sessions when schedule ON: ☐ Enable

Direction: [LAN/RT/VPN -> WAN ▾]
Source IP: [Any_____] [Edit]
Destination IP: [Any_____] [Edit]
Service Type: [Any_____] [Edit]
Fragments: [Don't Care ▾]

Application	Action/Profile	Syslog
Filter:	[Pass Immediately ▾]	☐
Branch to Other Filter Set:	[None ▾]	
Sessions Control	0 / [32000]	☐
MAC Bind IP	[Non-Strict ▾]	☐
Quality of Service	[None ▾]	☐
APP Enforcement:	[None ▾]	☐
URL Content Filter:	[None ▾]	☐
Web Content Filter:	[None ▾]	☐

Advance Setting [Edit]

[OK] [Clear] [Cancel]

Available settings are explained as follows:

Item	Description
Check to enable the Filter Rule	Check this box to enable the filter rule.
Comments	Enter filter set comments/description. Maximum length is 14- character long.
Index(1-15)	Set PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications >> Schedule** setup. The default setting of this field is blank and the function will always work.
Clear sessions when schedule ON	Check this box to clear the sessions when the above schedule profiles are applied.
Direction	Set the direction of packet flow. It is for **Data Filter** only. For the **Call Filter**, this setting is not available since **Call Filter** is only applied to outgoing traffic. [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	Click **Edit** to access into the following dialog to choose the source/destination IP or IP ranges.
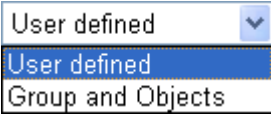
To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose **Group and Objects** as the Address Type.
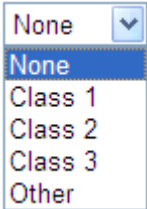
From the **IP Group** drop down list, choose the one that you want to apply. Or use the **IP Object** drop down list to choose the object that you want.

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

To set the service type manually, please choose **User defined** as the Service Type and type them in this dialog. In

	addition, if you want to use the service type from defined groups or objects, please choose **Group and Objects** as the Service Type.
	![User defined dropdown showing "User defined" and "Group and Objects" options] **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.

Dray Tek

MAC Bind IP	**Strict** – Make the MAC address and IP address settings configured in **IP Object** for **Source IP** and **Destination IP** be bound for applying such filter rule. **No-Strict -** no limitation.
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. None ▾ None Class 1 Class 2 Class 3 Other
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.
Advance Setting	Click **Edit** to open the following window. However, it is **strongly recommended** to use the default settings here.

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

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

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

Session timeout – Setting timeout for sessions can make the best utilization of network resources. However, Queue timeout is configured for TCP protocol only; session timeout is configured for the data flow which matched with the firewall rule.

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

	The requested Web page has been blocked by Web Content Filter. Please contact your system administrator for further information. [Powered by Draytek]
	Strict Security Checking - For the sake of security, you might want the router executing strict security checking for data transmission. The router performance will be affected if you invoke strict security checking. *APP Enforcement* – Check this box to execute the critical checking for all the files transferred via IM/P2P.

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

Example

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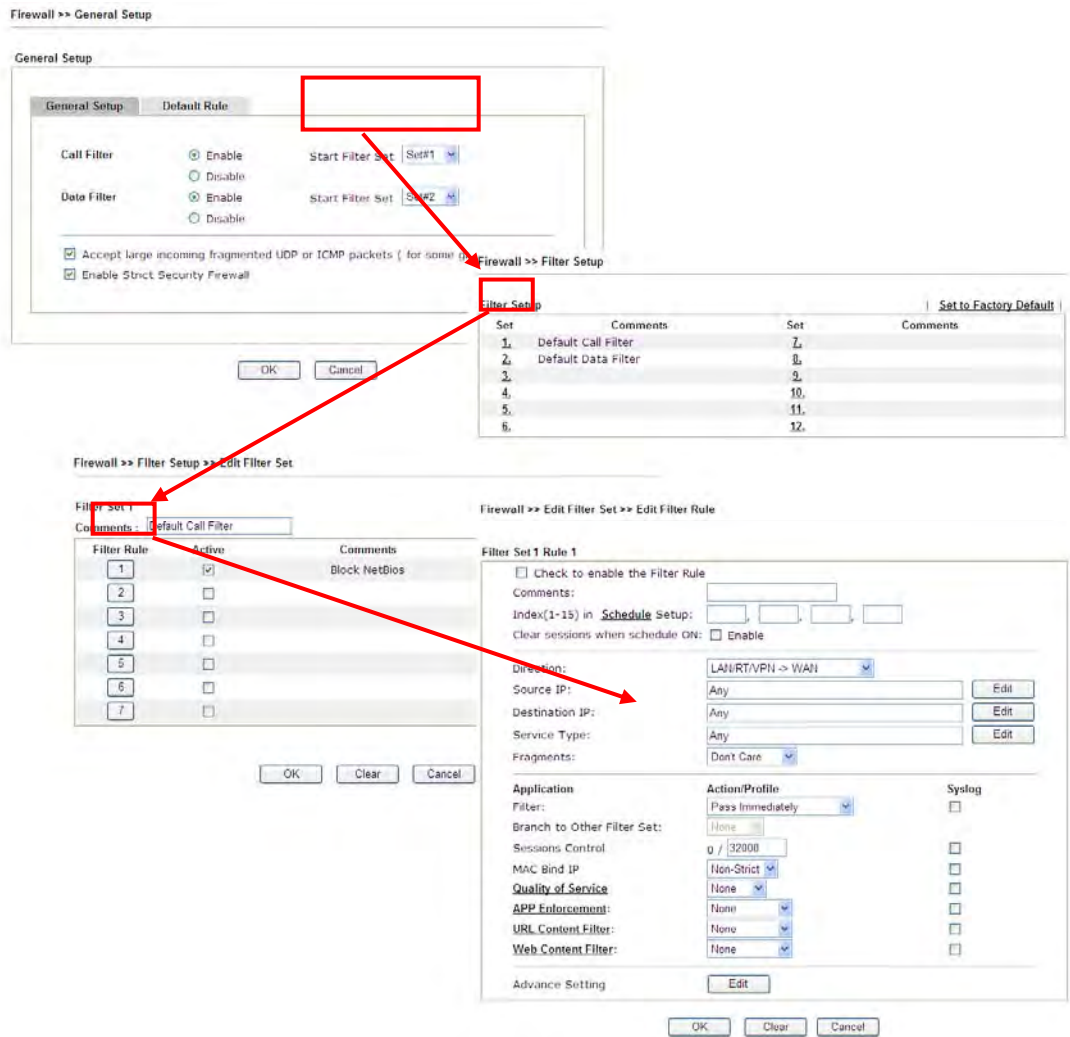
4.4.4 DoS Defense

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

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

Available settings are explained as follows:

Item	Description
Enable Dos Defense	Check the box to activate the DoS Defense Functionality.
Select All	Click this button to select all the items listed below.
Enable SYN flood defense	Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor 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.

Dray Tek

	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 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.

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

4.5 Objects Settings

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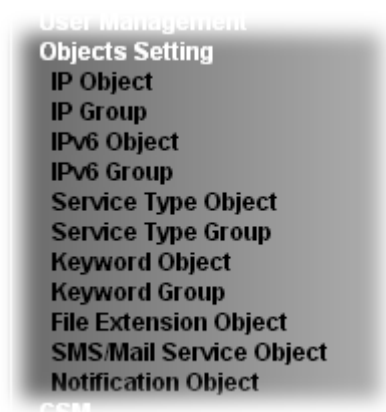
4.5.1 IP Object

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

Available settings are explained as follows:

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

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

1. Click the number (e.g., #1) under Index column for configuration in details.

2. The configuration page will be shown as follows:

Objects Setting >> IP Object

Profile Index : 1

Name:	RD Department
Interface:	Any
Address Type:	Range Address
Mac Address:	00 :00 :00 :00 :00 :00
Start IP Address:	192.168.1.59
End IP Address:	192.168.1.65
Subnet Mask:	0.0.0.0
Invert Selection:	☐

[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. Any Any LAN/RT/VPN WAN 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. Range Address Any Address Single Address Range Address Subnet Address Mac Address
MAC Address	Type the MAC address of the network card which will be controlled.

Dray Tek

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

IP Object Profiles:

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

4.5.2 IP Group

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

Available settings are explained as follows:

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

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

1. Click the number (e.g., #1) under Index column for configuration in details.

2. The configuration page will be shown as follows:

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
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.

4.5.3 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:	
End IP Address:	
Prefix Len:	
Invert Selection:	☐

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. Range Address Any Address Single Address Range Address Subnet Address Mac Address
Mac Address	Type the MAC address of the network card which will be controlled.
Start IP Address	Type the start IP address for Single Address type.
End IP Address	Type the end IP address if the Range Address type is selected.
Prefix Len	Type the number (e.g., 64) for the prefix length of IPv6 address.
Invert Selection	If it is checked, all the IPv6 addresses except the ones listed above will be applied later while it is chosen.

Dray Tek

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

4.5.4 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.

4.5.5 Service Type Object

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

Available settings are explained as follows:

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

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

1. Click the number (e.g., #1) under Index column for configuration in details.

DrayTek

2. The configuration page will be shown as follows:

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile.
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.

4.5.6 Service Type Group

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

Objects Setting >> Service Type Group

Service Type Group Table: | Set to Factory Default |

Group	Name	Group	Name
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 Group column for configuration in details.

2. The configuration page will be shown as follows:

Objects Setting >> Service Type Group Setup

Profile Index : 1

Name: VoIP

Available Service Type Objects   Selected Service Type Objects
1-www
2-SIP

                            >>
                            <<

            OK   Clear   Cancel

Available settings are explained as follows:

DrayTek

Item	Description
Name	Type a name for this profile.
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.

4.5.7 Keyword Object

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

Available settings are explained as follows:

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

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

1. Click the number (e.g., #1) under Index column for configuration in details.

2. The configuration page will be shown as follows:

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. Type a name for this profile, e.g., game.
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.

4.5.8 Keyword Group

This page allows you to bind several keyword objects into one group. The keyword groups set here will be chosen as black /white list in **CSM >>URL /Web Content Filter Profile**.

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.

4.5.9 File Extension Object

This page allows you to set eight profiles which will be applied in **CSM>>URL Content Filter**. All the files with the extension names specified in these profiles will be processed according to the chosen action.

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.

DrayTek

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

1. Click the number (e.g., #1) under Profile column for configuration in details.

2. The configuration page will be shown as follows:

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for this profile. The maximum length of the name you can set is 7 characters.

3. Type a name for such profile and check all the items of file extension that will be processed in the router. Finally, click **OK** to save this profile.

4.5.10 SMS/Mail Service Object

SMS Service Object

This page allows you to set ten profiles which will be applied in **Application>>SMS/Mail Alert Service**.

Object Settings >> SMS / Mail Service Object

Index	Profile Name	SMS Provider
SMS Provider	Mail Server	| Set to Factory Default |
1.		kotsms.com.tw (TW)
2.		kotsms.com.tw (TW)
3.		kotsms.com.tw (TW)
4.		kotsms.com.tw (TW)
5.		kotsms.com.tw (TW)
6.		kotsms.com.tw (TW)
7.		kotsms.com.tw (TW)
8.		kotsms.com.tw (TW)
9.	Custom 1	
10.	Custom 2	

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.

Object Settings >> SMS / Mail Service Object

	SMS Provider	Mail Server		Set to Factory Default
Index	**Profile Name**		**SMS Provider**	
1.			kotsms.com.tw (TW)	
2.			kotsms.com.tw (TW)	
3.			kotsms.com.tw (TW)	
4.			kotsms.com.tw (TW)	
5.			kotsms.com.tw (TW)	
6.			kotsms.com.tw (TW)	
7.			kotsms.com.tw (TW)	
8.			kotsms.com.tw (TW)	
9.	Custom 1			
10.	Custom 2			

You can click the number (e.g., #9) under Index column for configuration in details.

Object Settings >> SMS / Mail Service Object

Profile Index: 9

Profile Name	Custom 1
Service Provider	

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	
Password	
Quota	10
Sending Interval	3 (seconds)

[OK] [Clear] [Cancel]

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:

Object Settings >> SMS / Mail Service Object

Profile Index: 1

Profile Name	Mail_Notify
SMTP Server	192.168.1.98
SMTP Port	465
Sender Address	carrieni@draytek.com
☑ Use SSL	
☑ Authentication	
Username	john
Password	••••
Sending Interval	0 (seconds)

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 enable such function.
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.

Dray Tek

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.	

4.5.11 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.		

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.
Settings	Display the category selected for such profile.

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.	

2. The configuration page will be shown as follows:

Object Settings >> Notification Object

Profile Index: 4

Profile Name		Notify_attack	
Category		**Status**	
WAN	☐ Disconnected		☐ Reconnected
VPN Tunnel	☐ Disconnected		☐ Reconnected

[OK] [Clear] [Cancel]

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.

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

Object Settings >> Notification Object

| Set to Factory Default |

Index	Profile Name	Settings
1.	Notify_attack	WAN VPN
2.		
3.		

4.6 CSM

Content Security Management (CSM)

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

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.

Note: The priority of URL Content Filter is higher than Web Content Filter.

4.6.1 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.

 For the telnet command usage, please refer to "*Telnet Command: csm appe prof*" in the chapter of Telnet Command Reference.

CSM >> APP Enforcement Profile

APP Enforcement Profile Table: | Set to Factory Default |

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

Available settings are explained as follows:

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

Click the number under Index column for settings in detail.

There are four tabs IM, P2P, Protocol and OTHERS displayed on this page. Each tab will bring out different items that you can choose to disallow people using.

Below shows the items which are categorized under **Protocol**.

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 it to block the packets of the APP.

The profiles configured here can be applied in the **Firewall>>General Setup** and **Firewall>>Filter Setup** pages as the standard for the host(s) to follow.

4.6.2 URL Content Filter Profile

To provide an appropriate cyberspace to users, Vigor router equips with **URL Content Filter** not only to limit illegal traffic from/to the inappropriate web sites but also prohibit other web feature where malicious code may conceal.

Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines to teenagers. At office, **URL Content Filter** can also provide a job-related only environment hence to increase the employee work efficiency. How can URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.

On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from websites, you may risk bringing threat to your system. For example, an ActiveX control object is usually used for providing interactive web feature. If malicious code hides inside, it may occupy user's system.

For example, if you add key words such as "sex", Vigor router will limit web access to web sites or web pages such as "www.sex.com", "www.backdoor.net/images/sex/p_386.html". Or you may simply specify the full or partial URL such as "www.sex.com" or "sex.com".

Also the Vigor router will discard any request that tries to retrieve the malicious code.

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

CSM >> URL Content Filter Profile

URL Content Filter Profile Table: | **Set to Factory Default** |

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

Administration Message (Max 255 characters)   [Default Message]

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

[OK]

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Profile	Display the number of the profile which allows you to click to set different policy.
Name	Display the name of the URL Content Filter Profile.
Administration Message	You can type the message manually for your necessity. **Default Message** - You can type the message manually for

DrayTek

	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.
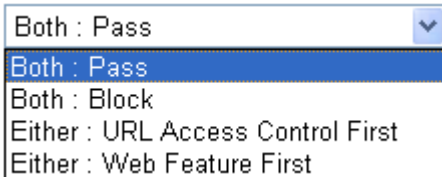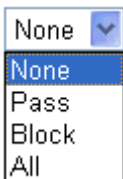
Available settings are explained as follows:

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.
	Both : Pass ▼ Both : Pass Both : Block Either : URL Access Control First Either : Web Feature First
Log	**None** – There is no log file will be recorded for this profile. **Pass** – Only the log about Pass will be recorded in Syslog. **Block** – Only the log about Block will be recorded in Syslog. **All** – All the actions (Pass and Block) will be recorded in Syslog. None ▼ None Pass Block All
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. Action: Block ▼ Pass Block **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

DrayTek

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.

Web Feature	**Enable Restrict Web Feature -** Check this box to make the keyword being blocked or passed.
	Action - This setting is available only when **Either: URL Access Control First** or **Either: Web Feature First** is selected.
	Pass **-** Allow accessing into the corresponding webpage with the keywords listed on the box below.
	Block **-** Restrict accessing into the corresponding webpage with the keywords listed on the box below.
	If the web pages do not match with the specified feature set here, it will be processed with reverse action.
	Cookie - Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy.
	Proxy - Check the box to reject any proxy transmission. To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages.
	Upload – Check the box to block the file upload by way of web page.
	File Extension Profile – Choose one of the profiles that you configured in **Object Setting>> File Extension Objects** previously for passing or blocking the file downloading.
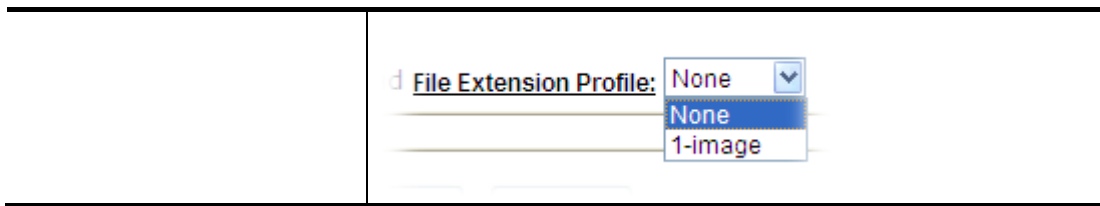
After finishing all the settings, please click **OK** to save the configuration.

4.6.3 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.

> **Note:** If you have used **Service Activation Wizard** to activate WCF service, you can skip this section.

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.

> **Note 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.
> **Note 2**: Commtouch is merged by **Cyren,** and **GlobalView** services will be continued to deliver powerful cloud-based information security solutions! Refer to:
> http://www.prnewswire.com/news-releases/commtouch-is-now-cyren-239025151.html

CSM >> Web Content Filter Profile

Web-Filter License   Activate
[Status:Not Activated]

| Setup Query Server | auto-selected | Find more |
| Setup Test Server | auto-selected | Find more |

Web Content Filter Profile Table: | Set to Factory Default |

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

Administration Message   (Max 255 characters)   Default Message   Cache : L1 + L2 Cache

```
<body><center><br><br><br><p>The requested Web page <br> from %SIP% <br>to %URL% <br>that
is categorized with %CL% <br>has been blocked by %RNAME% Web Content Filter.<p>Please
contact your system administrator for further information.</center></body>
```

Legend:
%SIP%   - Source IP ,   %DIP%   - Destination IP ,   %URL%   - URL
%CL%   - Category ,   %RNAME%   - Router Name

OK

Available settings are explained as follows:

Item	Description
Activate	Click it to access into MyVigor for activating WCF service.
Setup Query Server	It is recommended for you to use the default setting, auto-selected. You need to specify a server for categorize searching when you type URL in browser based on the web content filter profile.
Setup Test Server	It is recommended for you to use the default setting, auto-selected.
Find more	Click it to open http://myvigor.draytek.com for searching another qualified and suitable server.
Test a site to verify whether it is categorized	Click this link to do the verification.
Set to Factory Default	Click this link to retrieve the factory settings.
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**.

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 for a short time (about 1 second) 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.

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.

Dray Tek

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
Black/White List	**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.
Log	**None** – There is no log file will be recorded for this profile. **Pass** – Only the log about Pass will be recorded in Syslog. **Block** – Only the log about Block will be recorded in Syslog. **All** – All the actions (Pass and Block) will be recorded in Syslog. Block ▾ None Pass Block All

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

4.6.4 DNS Filter

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.

Note: 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.
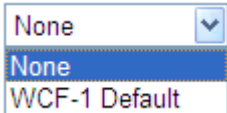
Available settings are explained as follows:

Item	Description
DNS Filter	Check Enable to enable such feature.
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.

Service	Set the filtering conditions. Specify one of the WCF profiles as Service.
	Choose the WCF profiles to apply DNS filter.
Cache Time (hour)	Set the time for DNS query.
Enable Block Page	If such function is enabled, when DNS packets are blocked by DNS filter, a web page containing the description listed on Administration Message will be shown on the screen.
Administration Message	Type the words or sentences which will be displayed when a web page is blocked by Vigor router.

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

4.6.5 APPE Support List

Such page lists all the information (name, version and note) about IM, P2P, Protocol and others applications that Vigor router supports for APPE function.

CSM >> APPE Support List

This charts lists out the APP Enforcement supported by Vigor routers.
Last update on 2014-06-16

IM	P2P		PROTOCOL	OTHERS
APP Type	**APP Name**	**Version**	**Note**	
	AIM	6/7	Only block Login. If users have already logged in, AIM services can not be blocked.	
	AliWW	2008		
	Ares	2.0.9		
	BaiduHi	37378		
	Fetion	2010		
	GaduGadu Protocol			
	Google Chat			
	ICQ	7	In ICQ6, if Videos are blocked, Voices will be blocked at the same time. In ICQ5 or former versions, Videos and Voices can be blocked separately.	
	ICU2	8.0.6		
	Jabber Protocol/Google Talk			
IM	KC	2008		
	LINE	4.4.1	To block LINE for PC (v3.6.0.32) and mobile phone (v4.4.1).	
	Lava-Lava	2007		
	MSN	2011		
	MobileMSN			
	POCO	2007	To block P2P, please check the P2P Object item.	

4.7 Bandwidth Management

Below shows the menu items for Bandwidth Management.

4.7.1 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.

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
Session Limit	**Enable -** Click this button to activate the function of limit session.
	Disable - Click this button to close the function of limit

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

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

4.7.2 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.

In the **Bandwidth Management** menu, click **Bandwidth Limit** to open the web page.

Bandwidth Management >> Bandwidth Limit

Bandwidth Limit

   ○ Enable   ☐ IP Routed Subnet   ⊙ Disable

Default TX Limit: 2000   Kbps ▾   Default RX Limit: 8000   Kbps ▾

  ☐ Allow auto adjustment to make the best utilization of available bandwidth.

Limitation List

```
Index Start IP        End IP          TX limit  RX limit  Shared
```

Specific Limitation

Start IP: [   ]   End IP: [   ]

⊙ Each ○ Shared TX Limit: [   ] Kbps ▾ RX Limit: [   ] Kbps ▾

[Add] [Edit] [Delete]

☐ Smart Bandwidth Limit

  For any LAN IP Not in Limitation List, when session number exceeds 1000

  TX Limit : 200 Kbps ▾ RX Limit : 800 Kbps ▾

Note : For TX/RX, a setting of "0" means unlimited bandwidth.

Time Schedule

  Index(1-15) in Schedule Setup: [   ], [   ], [   ], [   ]
  Note: Action and Idle Timeout settings will be ignored.

[OK]

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
Bandwidth Limit	**Enable** - Click this button to activate the function of limit bandwidth.
	Apply to 2nd Subnet – Check this box to apply the bandwidth limit to the second subnet specified in **LAN>>General Setup**.
	Disable - Click this button to close the function of limit bandwidth.
	Default TX limit - Define the default speed of the upstream for each computer in LAN.
	Default RX limit - Define the default speed of the

	downstream for each computer in LAN.
	Allow auto adjustment⋯ - Check this box to make the best utilization of available bandwidth.
Limitation List	Display a list of specific limitations that you set on this web page.
Specific Limitation	**Start IP -** Define the start IP address for limit bandwidth.
	End IP - Define the end IP address for limit bandwidth.
	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.
Smart Bandwidth Limit	Check this box to have the bandwidth limit determined by the system automatically.
	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	**Index (1-15) in Schedule Setup -** You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application >> Schedule** web page and you can use the number that you have set in that web page.

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

4.7.3 Quality of Service

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, thus 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.
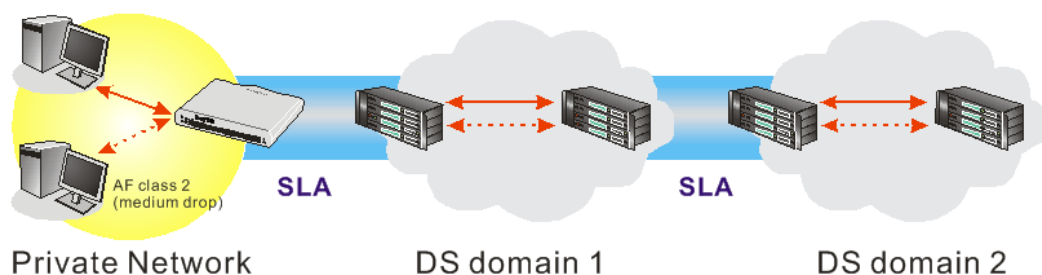
However, each node may take different attitude toward packets with high priority marking since it may bind with the business deal of SLA among different DS domain owners. It's not easy to achieve deterministic and consistent high-priority QoS traffic throughout the whole network with merely Vigor router's effort.

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 that you can edit.
	Status – Display if the WAN interface is available for such function or not.
	Bandwidth – Display the inbound and outbound bandwidth setting for the WAN interface.
	Direction – Display which direction that such function will influence.
	Class 1/Class2/Class 3/Others – Display the bandwidth percentage for each class.
	UDP Bandwidth Control – Display the UDP bandwidth control is enabled or not.
	Online Statistics – Display an online statistics for quality of service for your reference
	Setup – Allow to configure general QoS setting for WAN interface.
Class Rule	**Index** – Display the class number that you can edit.
	Name – Display the name of the class.
	Rule – Allow to configure detailed settings for the selected Class.
	Service Type – Allow to configure detailed settings for the service type.

This page displays the QoS settings result of the WAN interface. Click the **Setup** link to access into next page for the general setup of WAN interface. As to class rule, simply click the **Edit** link to access into next for configuration.

You can configure general setup for the WAN interface, edit the Class Rule, and edit the Service Type for the Class Rule for your request.

Online Statistics

Display an online statistics for quality of service for your reference. This feature is available only when the Quality of Service for WAN interface is enabled.
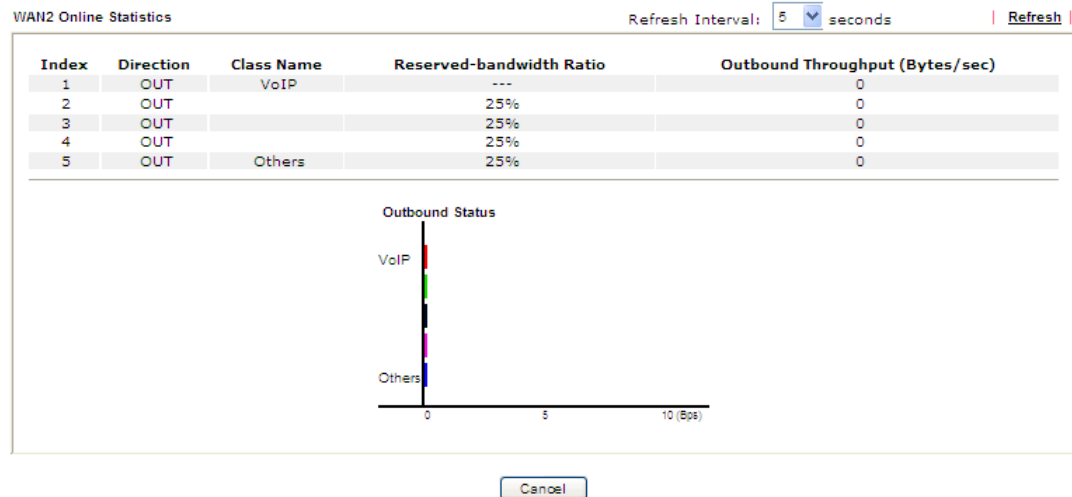
General Setup for WAN Interface

When you click **Setup**, you can configure the bandwidth ratio for QoS of the WAN interface. There are four queues allowed for QoS control. The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. Yet, the last one is reserved for the packets which are not suitable for the user-defined class rules.

Available settings are explained as follows:

Item	Description
Enable the QoS Control	The factory default for this setting is checked. Please also define which traffic the QoS Control settings will apply to. **IN -** apply to incoming traffic only. **OUT -** apply to outgoing traffic only. **BOTH -** apply to both incoming and outgoing traffic. Check this box and click **OK**, then click **Setup** link again. You will see the **Online Statistics** link appearing on this page.
WAN Inbound Bandwidth	It allows you to set the connecting rate of data input for WAN interface. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 1000kbps for this box. The default value is 10000kbps.
WAN Outbound Bandwidth	It allows you to set the connecting rate of data output for WAN interface. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 256kbps for this box. The default value is 10000kbps.
Reserved Bandwidth Ratio	It is reserved for the group index in the form of ratio of **reserved bandwidth to upstream speed** and **reserved bandwidth to downstream speed**.
Enable UDP Bandwidth Control	Check this and set the limited bandwidth ratio on the right field. This is a protection of TCP application traffic since UDP application traffic such as streaming video will exhaust lots of bandwidth.
Outbound TCP ACK Prioritize	The difference in bandwidth between download and upload are great in ADSL2+ environment. For the download speed might be impacted by the uploading TCP ACK, you can check this box to push ACK of upload faster to speed the network traffic.
Limited_bandwidth Ratio	The ratio typed here is reserved for limited bandwidth of UDP application.

Note: The rate of outbound/inbound must be smaller than the real bandwidth to ensure correct calculation of QoS. It is suggested to set the bandwidth value for inbound/outbound as 80% - 85% of physical network speed provided by ISP to maximize the QoS performance.

Edit the Class Rule for QoS

1. The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. To add, edit or delete the class rule, please click the **Edit** link of that one.

Bandwidth Management >> Quality of Service

General Setup | **Set to Factory Default** |

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics
WAN1	Enable	80000Kbps/85000Kbps	Both	25%	25%	25%	25%	Inactive	**Status** **Setup**
Backup WAN	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status **Setup**

Class Rule

Index	Name	Rule	Service Type
Class 1		**Edit**	
Class 2		**Edit**	**Edit**
Class 3		**Edit**	

2. After you click the **Edit** link, you will see the following page. Now you can define the name for that Class. In this case, "Test" is used as the name of Class Index #1.

Bandwidth Management >> Quality of Service

Class Index #1

Name [Test]   ☐ Tag packets as: [Default ▼]

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Empty	-	-	-	-

[Add] [Edit] [Delete]

[OK] [Cancel]

3. For adding a new rule, click **Add** to open the following page.

Bandwidth Management >> Quality of Service

Rule Edit
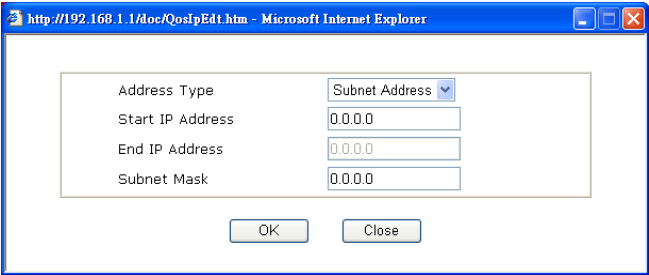
☑ ACT
Ethernet Type   ⦿ IPv4 ◯ IPv6
Local Address   [Any]   [Edit]
Remote Address   [Any]   [Edit]
DiffServ CodePoint   [ANY ▼]
Service Type   [---Predefined--- ▼]
Note: Please choose/setup the **Service Type** first.

[OK] [Cancel]

Available settings are explained as follows:

Item	Description
ACT	Check this box to invoke these settings.
Ethernet Type	Please specify which protocol (IPv4 or IPv6) will be used for this rule.
Local Address	Click the **Edit** button to set the local IP address (on LAN) for the rule.
Remote Address	Click the **Edit** button to set the remote IP address (on LAN/WAN) for the rule. **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.

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

By the way, you can set up to 20 rules for one Class. If you want to edit an existed rule, please select the radio button of that one and click **Edit** to open the rule edit page for modification.

Edit the Service Type for Class Rule

1. To add a new service type, edit or delete an existed service type, please click the Edit link under Service Type field.

2. After you click the **Edit** link, you will see the following page.

DrayTek

3. For adding a new service type, click **Add** to open the following page.

Bandwidth Management >> Quality of Service

Service Type Edit

Service Name	
Service Type	TCP ▼ 6
Port Configuration	
Type	⦿ Single ○ Range
Port Number	0 - 0

OK   Cancel

Available settings are explained as follows:

Item	Description
Service Name	Type in a new service for your request. The maximum length of the name you can set is 11 characters.
Service Type	Choose the type (TCP, UDP or TCP/UDP or other) for the new service.
Port Configuration	**Type** - Click **Single** or **Range** as the **Type**. If you select Range, you have to type in the starting port number and the end porting number on the boxes below. **Port Number** – Type in the starting port number and the end porting number here if you choose Range as the type.

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

By the way, you can set up to 10 service types. If you want to edit/delete an existed service type, please select the radio button of that one and click **Edit/Delete** 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.
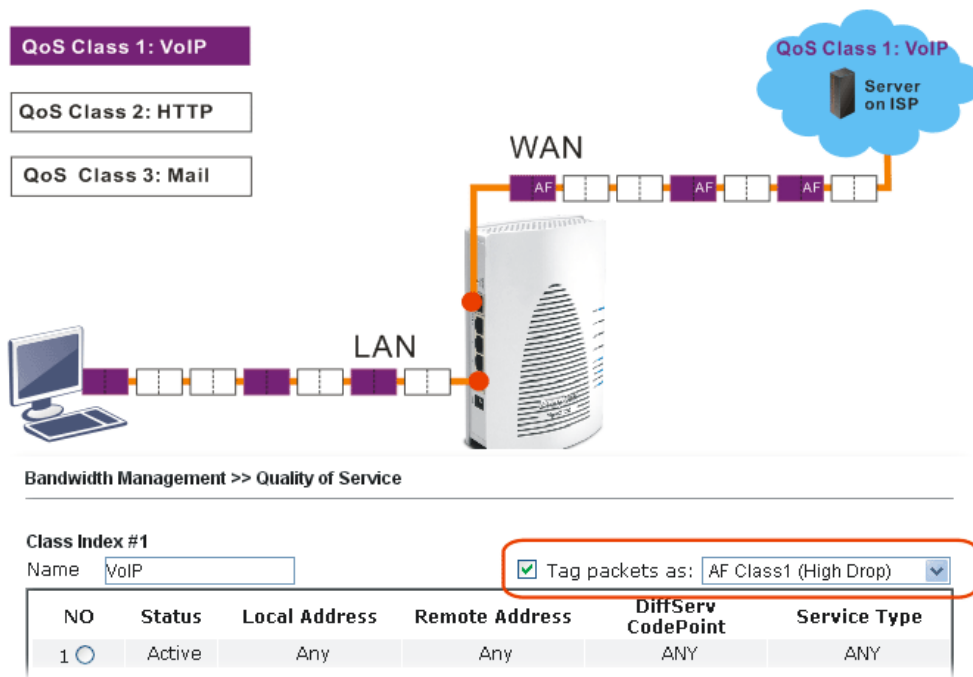
4.7.4 APP QoS

The QoS function is used to do bandwidth management for the services with certain IP or port number. However, there is no effect of bandwidth management on the service such as IM or P2P without fixed IP or port number.

APP QoS employs the function of APP Enforcement to detect several types of software in application layer. By combining the function of QoS, Vigor router can perform the bandwidth management for the application of VoIP, Streaming, IM, P2P and so on.
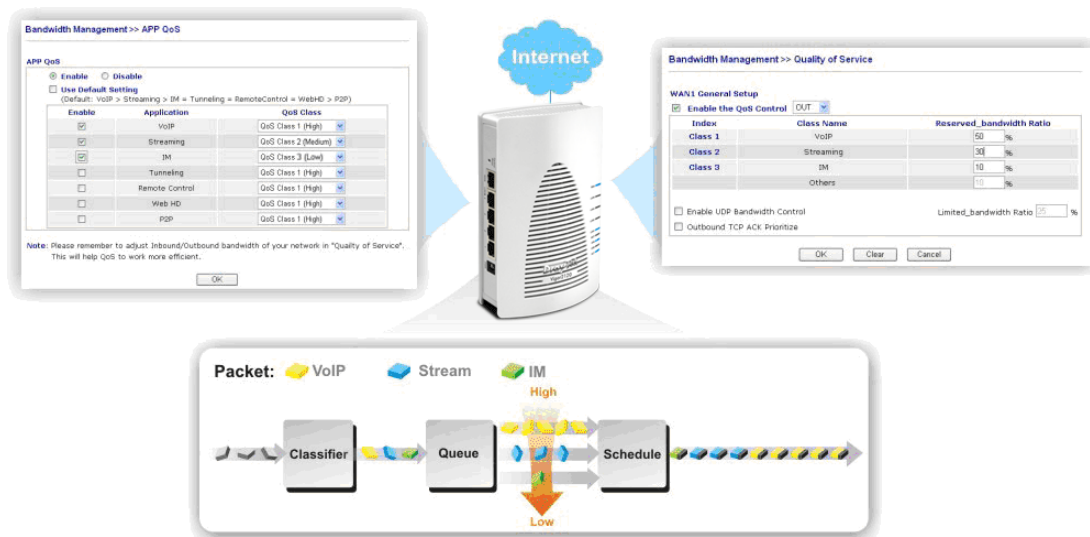
Open **Bandwidth Management>>APP QoS** to display the following page. The following shows web page under Traceable.

Bandwidth Management >> APP QoS

APP QoS

○ Enable   ⊙ Disable

| Traceable | Untraceable |

[Select All]   [Clear All]   Apply to all: [QoS Class 1 (High) ▼] [Apply]

Enable	Protocol	Action
☐	DNS	QoS Class 1 (High) ▼
☐	FTP	QoS Class 1 (High) ▼
☐	HTTP	QoS Class 1 (High) ▼
☐	IMAP	QoS Class 1 (High) ▼
☐	IRC	QoS Class 1 (High) ▼
☐	NNTP	QoS Class 1 (High) ▼
☐	POP3	QoS Class 1 (High) ▼
☐	SMB	QoS Class 1 (High) ▼
☐	SMTP	QoS Class 1 (High) ▼
☐	SNMP	QoS Class 1 (High) ▼
☐	SSH	QoS Class 1 (High) ▼
☐	SSL/TLS	QoS Class 1 (High) ▼
☐	TELNET	QoS Class 1 (High) ▼

Note: Please remember to adjust Inbound/Outbound bandwidth of your network in "Quailty of Service".
This will help QoS to work more efficient.

[OK]   [Cancel]

The following shows web page under Untraceable.

Bandwidth Management >> APP QoS

APP QoS

○ Enable   ⊙ Disable

| Traceable | Untraceable |
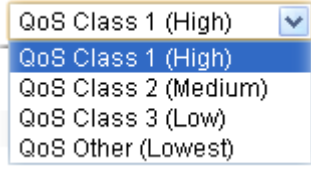
[Select All]   [Clear All]   Action: [QoS Class 1 (High) ▼]

Enable	IM
☐	AIM
☐	AliWW
☐	Ares
☐	BaiduHi
☐	Fetion
☐	GaduGadu Protocol
☐	Google Chat
☐	ICQ
☐	ICU2
☐	Jabber Protocol/Google Talk
☐	KC
☐	LINE
☐	Lava-Lava
☐	MSN
☐	MobileMSN
☐	POCO
☐	Paltalk
☐	QQ/TM

Available settings are explained as follows:

Item	Description
Enable/Disable	Click **Enable** to activate APP QoS function. Click **Disable** to deactivate APP QoS function.
Select All	Click it to choose all of the items in this page.
Clear All	Uncheck all the selected boxes.
Action	The APP can be specified with different QoS Class.

4.8 Applications

Below shows the menu items for Applications.

4.8.1 Dynamic DNS

The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your 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.

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**.

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

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

Auto-Update interval [14400]   Min(s) (1~14400)

Accounts:

Index	Domain Name	Active
1.		x
2.		x
3.		x

[OK]   [Clear All]
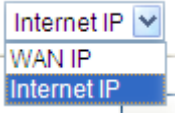
Available settings are explained as follows:

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).
Domain Name	Display the domain name that you set on the setting page of DDNS setup.
Active	Display if this account is active or inactive.

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

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

Index : 1

☑ Enable Dynamic DNS Account

Service Provider	dyndns.org (www.dyndns.org)
Service Type	Dynamic
Domain Name	chronic6653 .dyndns.org dyndns.org
Login Name	chronic6653 (max. 64 characters)
Password	•••••••••••• (max. 23 characters)
☐ Wildcards	
☐ Backup MX	
Mail Extender	
Determine Real 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).
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 Real 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: Internet IP WAN IP Internet IP **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

DrayTek

| | 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.

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.

4.8.2 LAN DNS

LAN DNS is a simple version of DNS server. It is not necessary for the user to build another DNS server in LAN. With such feature, the user can configure some services (such as ftp, www or database) with domain name which is easy to be accessed.

| | For the telnet command usage, please refer to "*Telnet Command: ip lanDNSRes*" in the chapter of Telnet Command Reference. |

Applications >> LAN DNS

LAN DNS Resolution | Set to Factory Default |

Enable	Index	Profile	Domain Name
☐	1.		
☐	2.		
☐	3.		
☐	4.		
☐	5.		
☐	6.		
☐	7.		
☐	8.		
☐	9.		
☐	10.		

<< 1-10 | 11-20 >>

OK

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profiles and recover to factory settings.
Enable	Check the box to enable the selected profile.
Index	Click the number below Index to access into the setting page.
Profile	Display the name of the LAN DNS profile.
Domain Name	Display the domain name of the LAN DNS profile.

You can set up to 20 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.
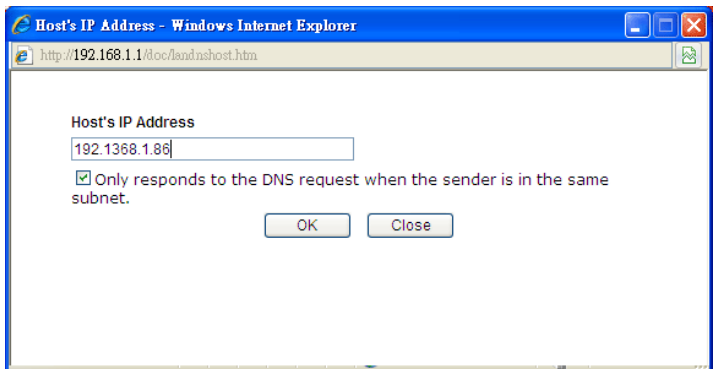
Available settings are explained as follows:

Item	Description
Enable	Check this box to enable such profile.
Profile	Type a name for such profile.
Domain Name	Type the domain name for such profile.
IP Address List	The IP address listed here will be used for mapping with the domain name specified above. In general, one domain name maps with one IP address. If required, you can configure two IP addresses mapping with the same domain name. **Add** – Click it to open a dialog to type the host's IP address. ● **Only responds to the DNS….** – Different LAN PCs can share the same domain name. However, you have to check this box to make the router identify & respond the IP address for the DNS query coming from different LAN PC. **Delete** – Click it to remove an existed IP address on the list.

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

4. A new LAN DNS profile has been created.

4.8.3 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.

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 of schedule.

Status	Display if this schedule setting is active or inactive.

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

To add a schedule:

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

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

Available settings are explained as follows:

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

DrayTek

Idle Timeout	Specify the duration (or period) for the schedule.
	How often -Specify how often the schedule will be applied **Once -**The schedule will be applied just once **Weekdays -**Specify which days in one week should perform the schedule.

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

Example

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

Office Hour: **(Force On)**		
Mon - Sun	**9:00 am** to	**6:00 pm**

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

4.8.4 RADIUS

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

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

Available settings are explained as follows:

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

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

4.8.5 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.

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

Applications >> UPnP

UPnP

☐ Enable UPnP Service   Default WAN ▾
        ☐ Enable Connection Control Service
        ☐ Enable Connection Status Service

Note: To allow NAT pass-through to a UPnP-enabled client on the LAN, enable UPnP service above and ensure that the used connection service is also ticked.

[OK]   [Clear]   [Cancel]

Available settings are explained as follows:

Item	Description
Enable UPNP Service	Accordingly, you can enable either the **Connection Control Service** or **Connection Status Service**.
Default WAN	It is used to specify the WAN interface for applying such function. Default WAN ▾ **Default WAN** WAN1

The reminder as regards concern about Firewall and UPnP

Can't work with Firewall Software

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

Security Considerations

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

● Some Microsoft operating systems have found out the UPnP weaknesses and hence you need to ensure that you have applied the latest service packs and patches.

● Non-privileged users can control some router functions, including removing and adding port mappings.

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

4.8.6 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.

Available settings are explained as follows:

Item	Description
Enable IGMP Proxy	Check this box to enable this function. The application of multicast will be executed through WAN port. In addition, such function is available in NAT mode.
Enable IGMP Snooping	Check this box to enable this function. Multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.
Refresh	Click this link to renew the working multicast group status.
Group ID	This field displays the ID port for the multicast group. The available range for IGMP starts from 224.0.0.0 to 239.255.255.254.
P1 to P4	It indicates the LAN port used for the multicast group.

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

4.8.7 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.

Available settings are explained as follows:

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

Application >> Wake on LAN

Wake on LAN

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

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

Send command to client done.

4.8.8 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.

Application >> SMS / Mail Alert Service

SMS Provider	Mail Server				Set to Factory Default
Index	**SMS Provider**	**Recipient**	**Notify Profile**	**Schedule(1-15)**	
1 ☑	1 - Line_down ▼	[ ]	1 - Notify_attack ▼	[ ] [ ]	
2 ☐	1 - Line_down ▼	[ ]	1 - Notify_attack ▼	[ ] [ ]	
3 ☐	1 - Line_down ▼	[ ]	1 - Notify_attack ▼	[ ] [ ]	
4 ☐	1 - Line_down ▼	[ ]	1 - Notify_attack ▼	[ ] [ ]	
5 ☐	1 - Line_down ▼	[ ]	1 - Notify_attack ▼	[ ] [ ]	
6 ☐	1 - Line_down ▼	[ ]	1 - Notify_attack ▼	[ ] [ ]	
7 ☐	1 - Line_down ▼	[ ]	1 - Notify_attack ▼	[ ] [ ]	
8 ☐	1 - Line_down ▼	[ ]	1 - Notify_attack ▼	[ ] [ ]	
9 ☐	1 - Line_down ▼	[ ]	1 - Notify_attack ▼	[ ] [ ]	
10 ☐	1 - Line_down ▼	[ ]	1 - Notify_attack ▼	[ ] [ ]	

[OK]   [Cancel]

Available settings are explained as follows:

Item	Description
Index	Check the box to enable such profile.
SMS Provider	Use the drop down list to choose SMS service provider. You can click **SMS Provider** link to define the SMS server.

Recipient	Type the name of the one who will receive the SMS.
Notify	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	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
Index	Check the box to enable such profile.
Mail Service	Use the drop down list to choose mail service provider. You can click **Mail Service** link to define the mail server.
Recipient	Type the e-mail address of the one who will receive the notification message.
Notify	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.

DrayTek

Schedule	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.

4.8.9 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 softwares 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.
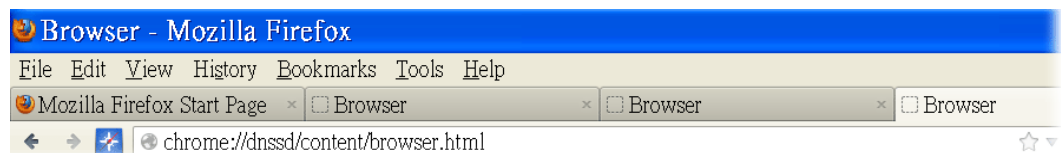
2. Open the web browse, Firefox. If Bonjour and DNSSD have been installed, you can open the web page (DNSSD) and see the following results.

chrome://dnssd/content/browser.html

DNSSD for Firefox

| Browser | Configuration Options | Diagnostic Information |

Interface	Name	Type	Domain	Service Info
2	DS1010Plus	_http._tcp.	local.	Select a service on the left to view further details.
2	DS1010Plus(WebDAV)	_http._tcp.	local.	
2	HP LaserJet 1300	_ipp._tcp.	local.	
2	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.	

3. Open **System Maintenance>>Management**. Type a name (e.g., Dray_2925) as the Router Name and click **OK**.

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

DrayTek

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.
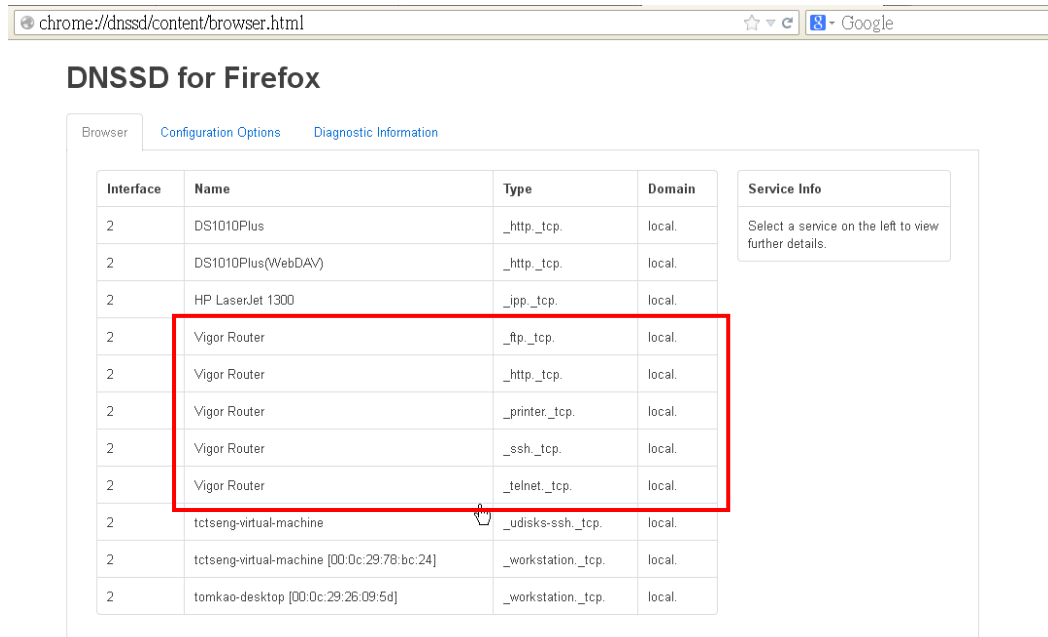
6. Now, any page or document can be printed out through Vigor router (installed with a printer).
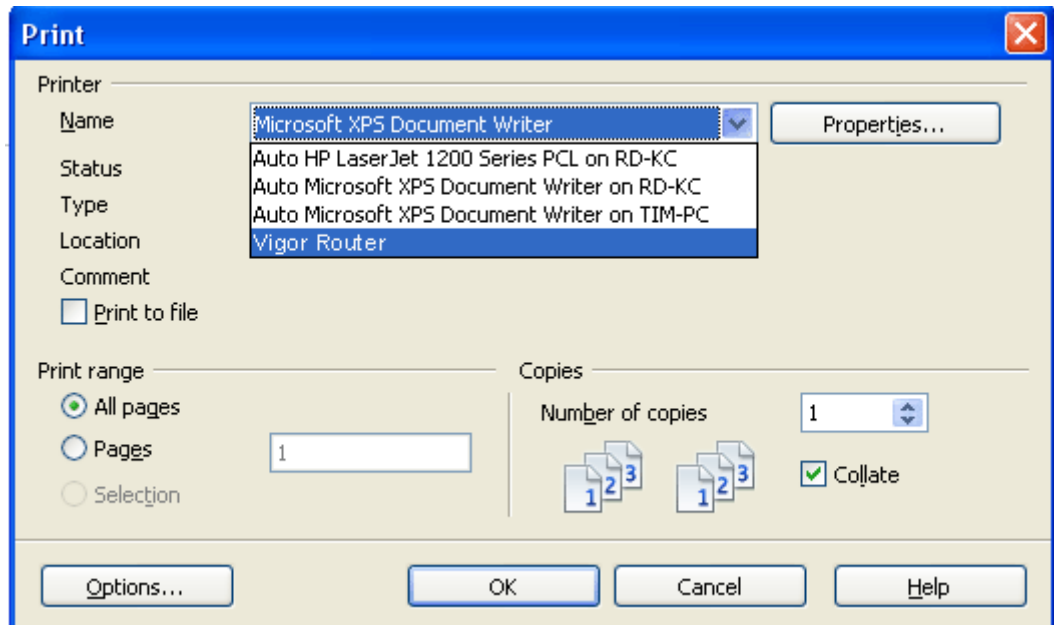
4.9 VPN and Remote Access

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.

Below shows the menu items for VPN and Remote Access.

4.9.1 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.

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

4.9.2 PPP General Setup

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

VPN and Remote Access >> PPP General Setup

PPP General Setup

PPP/MP Protocol	
Dial-In PPP Authentication	PAP/CHAP/MS-CHAP/MS-CHAPv2 ▼
Dial-In PPP Encryption(MPPE)	Optional MPPE ▼
Mutual Authentication (PAP)	○ Yes ◉ No
Username	
Password	
IP Address Assignment for Dial-In Users (When DHCP Disable set)	
Assigned IP start	LAN 1 192.168.1.200
	LAN 2 192.168.2.200

[OK]

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.
	PAP/CHAP/MS-CHAP/MS-CHAPv2 ▼
	PAP Only
	PAP/CHAP/MS-CHAP/MS-CHAPv2
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.
	Optional MPPE ▼
	Optional MPPE
	Require MPPE(40/128 bit)
	Maximum MPPE(128 bit)
	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 **Username** and **Password** of the mutual authentication peer. The length of the name/password is limited to 23/19 characters.
Assigned IP Start	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.

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

4.9.3 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 Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method	
Certificate for Dial-in	None ▾
Pre-Shared Key	
Pre-Shared Key	
Confirm Pre-Shared Key	
IPsec Security Method	

☑ Medium (AH)
Data will be authentic, but will not be encrypted.

High (ESP)   ☑ DES   ☑ 3DES   ☑ AES
Data will be encrypted and authentic.

[OK]   [Cancel]

Available settings are explained as follows:

Item	Description
IKE Authentication Method	This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPsec-related VPN connections such as L2TP over IPsec and IPsec tunnel. 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 for Dial-in –Choose one of the local certificates from the drop down list.
	Pre-Shared Key- Specify a key for IKE authentication.
	Confirm Pre-Shared Key- Retype the characters to confirm the pre-shared key.
	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	**Medium (AH)** - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.
	High (ESP) - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

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

4.9.4 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 32 entries of digital certificates for peer dial-in users.

VPN and Remote Access >> IPsec Peer Identity

X509 Peer ID Accounts: | Set to Factory Default |

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

Available settings are explained as follows:

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

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

Profile Index : 4

Profile Name   ???

☑ Enable this account

○ Accept Any Peer ID

◉ Accept Subject Alternative Name

Type	Domain Name ▾
Domain Name	

○ Accept Subject Name

Country (C)	
State (ST)	
Location (L)	
Orginization (O)	
Orginization Unit (OU)	
Common Name (CN)	
Email (E)	

[OK]   [Clear]   [Cancel]

Available settings are explained as follows:

Item	Description
Profile Name	Type the name of the profile. The maximum length of the name you can set is 32 characters.
Enable this account	Check it to enable such account profile.
Accept Any Peer ID	Click to accept any peer regardless of its identity.
Accept Subject Alternative Name	Click to check one specific field of digital signature to accept the peer with matching value. The field can be **IP Address, Domain,** or **E-mail 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.

DrayTek

4.9.5 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 **32** access accounts for dial-in users. Besides, you can extend the user accounts to the RADIUS server through the built-in RADIUS client function. The following figure shows the summary table.

VPN and Remote Access >> Remote Dial-in User

Remote Access User Accounts: | **Set to Factory Default** |

Index	User	Active	Status	Index	User	Active	Status
1.	???	☐	---	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.	???	☐	---

[OK]   [Cancel]

Available settings are explained as follows:

Item	Description
Set to Factory Default	Click to clear all indexes.
Index	Click the number below Index to access into the setting page of Remote Dial-in User.
User	Display the username for the specific dial-in user of the LAN-to-LAN profile. The symbol **???** represents that the profile is empty.
Active	Check the box to enable the selected profile.
Status	Display the access state of the specific dial-in user. The symbol V and X represent the specific dial-in user to be active and inactive, respectively.

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

VPN and Remote Access >> Remote Dial-in User

Index No. 12

User account and Authentication			Username	???
Enable this account			Password(Max 19 char)	
Idle Timeout	300	second(s)		

Allowed Dial-In Type
- ☑ PPTP
- ☑ IPsec Tunnel
- ☑ L2TP with IPsec Policy None
- ☑ SSL 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

SSL VPN
  Set SSL Application

☐ Enable Mobile One-Time Passwords(mOTP)
  PIN Code
  Secret

IKE Authentication Method
☑ Pre-Shared Key
  IKE Pre-Shared Key
☐ Digital Signature(X.509)
  None

IPsec Security Method
☑ Medium(AH)
High(ESP)   ☑ DES ☑ 3DES ☑ AES
Local ID (optional)

[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.
Allowed Dial-In Type	**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 make 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 make an SSL VPN connection through Internet.
	Specify Remote Node -You can specify the IP address of the remote dial-in user, or peer ID (used in IKE aggressive mode).
	Uncheck the checkbox means the connection type you select above will apply the authentication methods and security methods in the **general settings**.
	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.
	- 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.
	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).
Subnet	Chose one of the subnet selections for such VPN profile.
	Assign Static IP Address – Please type a static IP address for the subnet you specified.
SSL VPN	**Set SSL Application** – Choose the SSL application profile to be applied by such dial-in user profile.
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 specifying 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.**
IPsec Security Method	This group of fields is a must for IPsec Tunnels and L2TP with IPsec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method.
	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-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 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.

4.9.6 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 router supports up to 32 VPN tunnels simultaneously. The following figure shows the summary table.

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

LAN-to-LAN Profiles: | **Set to Factory Default** |

Index	Name	Active	Status	Index	Name	Active	Status
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.	???	☐	---

[OK]   [Cancel]

Available settings are explained as follows:

Item	Description
Set to Factory Default	Click to clear all indexes.
Name	Indicate the name of the LAN-to-LAN profile. The symbol **???** represents that the profile is empty.
Active	V – means the profile has been enabled. X – means the profile has not been enabled.
Status	Online – means such LAN to LAN profile is in use. Offline – means such LAN to LAN profile isn't in use even if the profile has been enabled.

To edit each profile:

1. Click each index to edit each profile and you will get the following page. Each LAN-to-LAN profile includes 4 subgroups. If the fields gray out, it means you may leave it untouched. The following explanations will guide you to fill all the necessary fields.

   For the web page is too long, we divide the page into several sections for explanation.

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.
	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.
	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 disconnect 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 wild 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 **Yes** 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.

Dray Tek

- **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.

<table>
<tr><td></td><td>Index(1-15) - Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in Applications >> Schedule setup. The default setting of this field is blank and the function will always work.</td></tr>
</table>

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.

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 named 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. 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 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.
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 Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.

Dray Tek
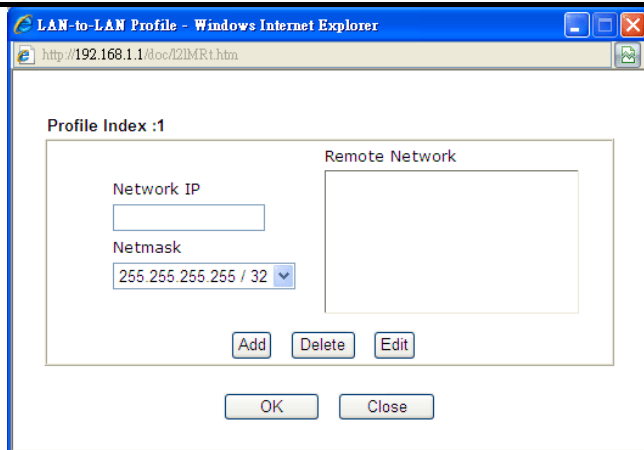
RIP Direction - The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable.

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.

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

4.9.7 Connection Management

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

VPN and Remote Access >> Connection Management

Dial-out Tool   Refresh Seconds : [10 ▾] [Refresh]

[▾] [Dial]

VPN Connection Status
Current Page: 1   Page No. [   ] [Go] [>>]

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime

xxxxxxxx : Data is encrypted.
xxxxxxxx : Data isn't encrypted.

Available settings are explained as follows:

Item	Description
Dial-out Tool	**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.

4.10 Certificate Management

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

Any entity wants to utilize digital certificates should first request a certificate issued by a CA server. It should also retrieve certificates of other trusted CA servers so it can authenticate the peer with certificates issued by those trusted CA servers.

Here you can manage generate and manage the local digital certificates, and set trusted CA certificates. Remember to adjust the time of Vigor router before using the certificate so that you can get the correct valid period of certificate.

Below shows the menu items for Certificate Management.

VPN and Remote Access
Certificate Management
Local Certificate
Trusted CA Certificate
Certificate Backup
SSL VPN

4.10.1 Local Certificate

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify
---	---	---	[View] [Delete]
---	---	---	[View] [Delete]
---	---	---	[View] [Delete]

[GENERATE] [IMPORT] [REFRESH]

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	test11

Subject Alternative Name

Type	IP Address ▾
IP	

Subject Name

Country (C)	TW
State (ST)	Taiwan
Location (L)	HS
Organization (O)	DT
Organization Unit (OU)	MKT
Common Name (CN)	
Email (E)	press@draytek.com

Key Type	RSA ▾
Key Size	1024 Bit ▾

[Generate]

> **Note:** 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	
test11	/C=TW/ST=Taiwan/L=HS/O=DT/OU...	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.
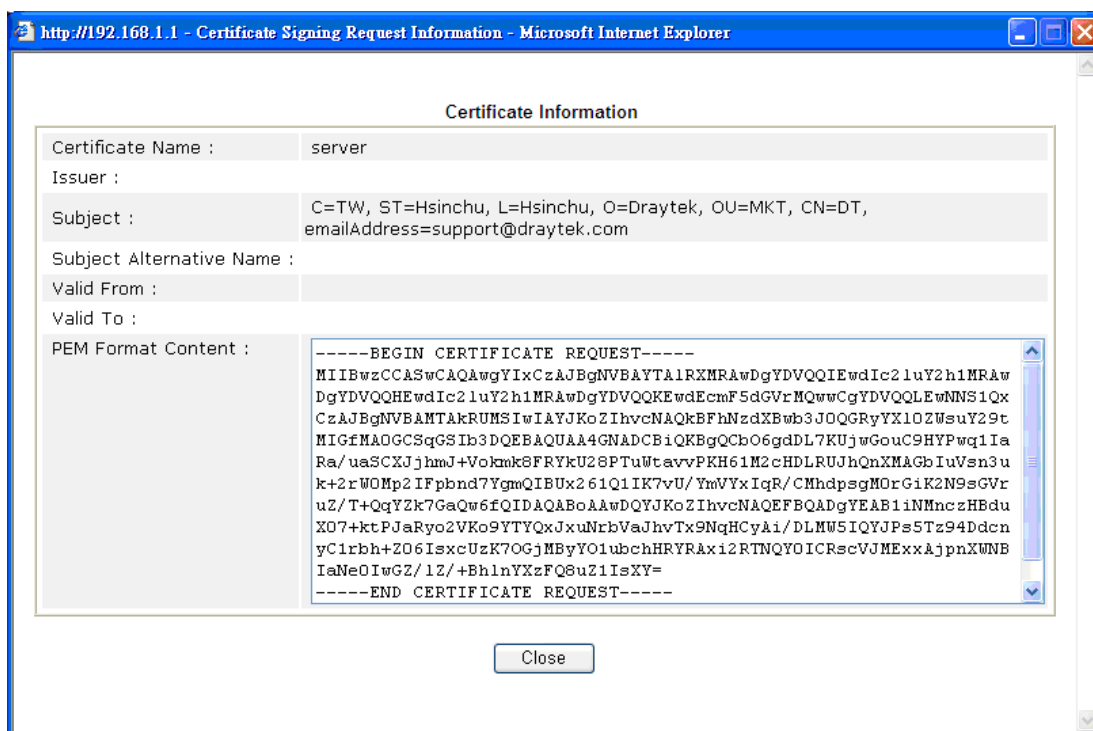
Note: You have to copy the certificate request information from above window. Next, access your CA server and enter the page of certificate request, copy the information into it and submit a request. A new certificate will be issued to you by the CA server. You can save it.

Delete

Click this button to remove the selected certificate.

4.10.2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate.

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. Then click **Import** to use the pre-saved file.

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.
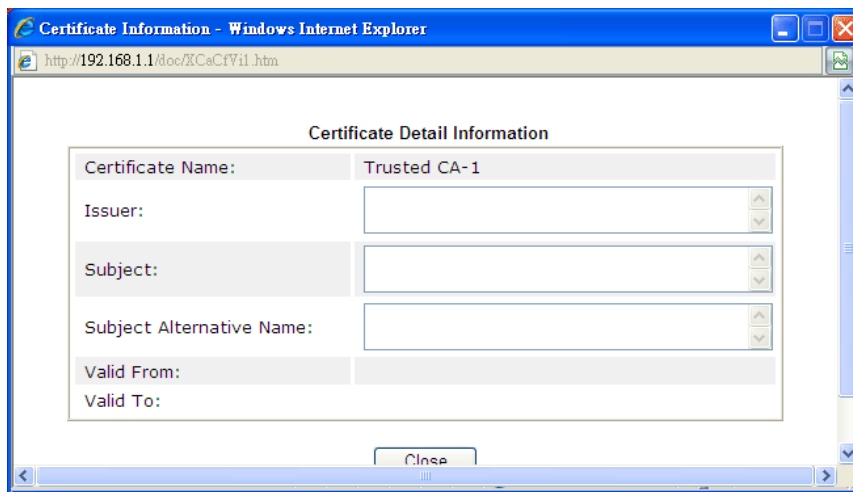
4.10.3 Certificate Backup

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 **Retype password**.

Also, you can use **Restore** to retrieve these two settings to the router whenever you want.

Certificate Management >> Certificate Backup

Certificate Backup / Restoration

Backup

Encrypt password: [   ]

Confirm password: [   ]

Click [Backup] to download certificates to your local PC as a file.

Restoration

Select a backup file to restore.

[   ] [Browse.]

Decrypt password: [   ]

Click [Restore] to upload the file.

4.11 Wireless LAN(2.4GHz/5GHz)

This function is used for "*n/n-plus*" models only.

4.11.1 Basic Concepts

Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The Vigor "n" model, a.k.a. Vigor wireless router, is designed for maximum flexibility and efficiency of a small office/home. Any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access.

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

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

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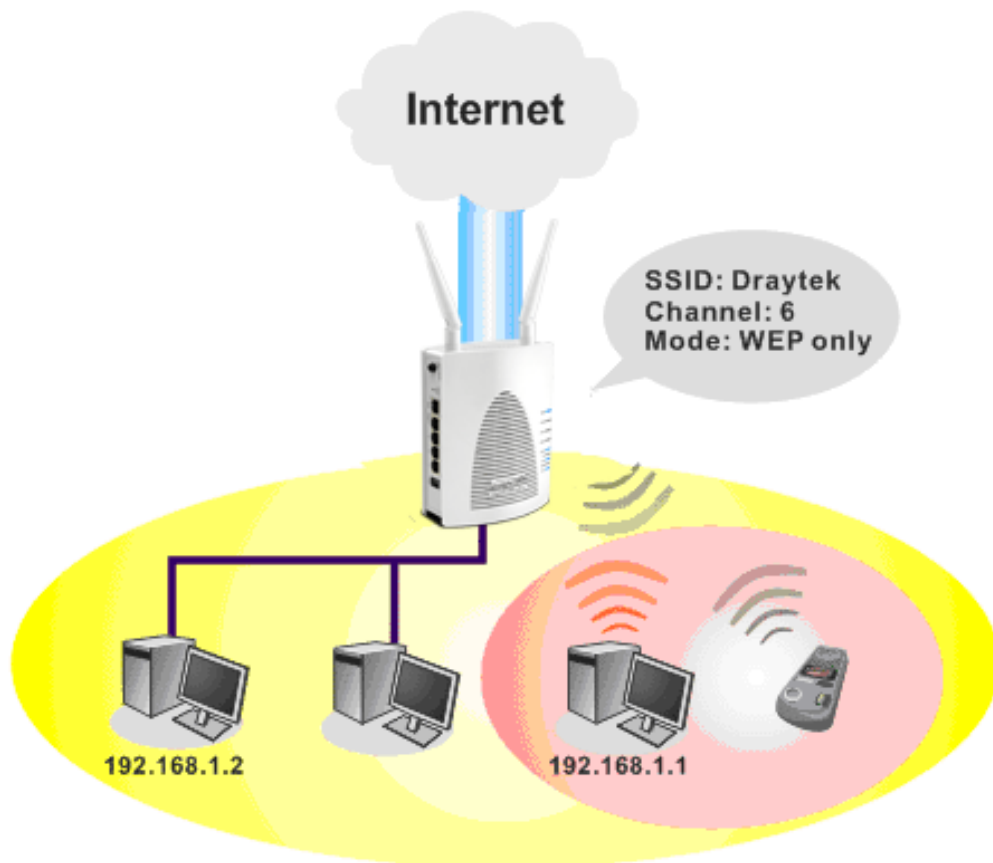
Multiple SSIDs

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

Security Overview

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

Complete Security Standard Selection: To ensure the security and privacy of your wireless communication, we provide several prevailing standards on market.

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

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

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

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

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

Manage Wireless Stations - Station List will display all the stations in your wireless network and the status of their connection.

Below shows the menu items for Wireless LAN.

Wireless LAN (2.4 GHz)
- General Setup
- Security
- Access Control
- WPS
- WDS
- Advanced Setting
- WMM Configuration
- AP Discovery
- Station List
- Station Control

Wireless LAN (5 GHz)
- General Setup
- Security
- Access Control
- WPS
- WDS
- Advanced Setting
- WMM Configuration
- AP Discovery
- Station List
- Station Control
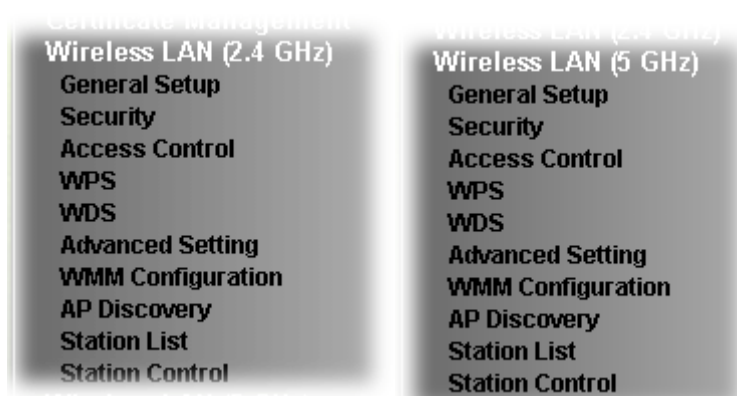
In this section, we take Wireless LAN (2.4G) as the examples of function explanations.

DrayTek

4.11.2 General Setup

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

Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Mode	At present, the router can connect to 11b Only, 11g Only, 11n Only(2.4 GHz), Mixed (11b+11g), Mixed (11g+11n), and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode. 2.4G 5G

Channel	Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.
	2.4G 5G
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity.
SSID	Means the identification of the wireless LAN. SSID can be any text numbers or various special characters.
Isolate	**Member** –Check this box to make the wireless clients (stations) with the same SSID not accessing for each other. **VPN** – Check this box to restrict the wireless clients (stations) to access VPN network.
Rate Control	It controls the data transmission rate through wireless connection. **Upload** – Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps. **Download** – Type the transmitting rate for data download. Default value is 30,000 kbps.
Schedule	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.

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

4.11.3 Security

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

The password (PSK) of default security mode is provided and stated on the label pasted on the bottom of the router. For the wireless client who wants to access into Internet through such router, please input the default PSK value for connection.
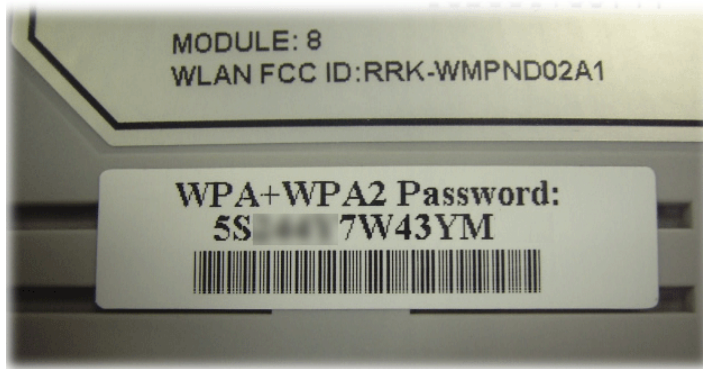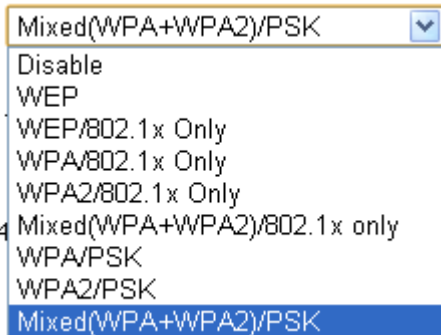
By clicking the **Security Settings**, a new web page will appear so that you could configure the settings of WPA and WEP.

Available settings are explained as follows:

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

	Note: You should also set **RADIUS Server** simultaneously if 802.1x mode is selected.
	Disable - Turn off the encryption mechanism.
	WEP-Accepts only WEP clients and the encryption key should be entered in WEP Key.
	WEP/802.1x Only - Accepts only WEP clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.
	WPA/802.1x Only- Accepts only WPA clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.
	WPA2/802.1x Only- Accepts only WPA2 clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.
	Mixed (WPA+WPA2/802.1x only) - Accepts WPA and WPA2 clients simultaneously and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.
	WPA/PSK-Accepts only WPA clients and the encryption key should be entered in PSK.
	WPA2/PSK-Accepts only WPA2 clients and the encryption key should be entered in PSK.
	Mixed (WPA+ WPA2)/PSK - Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.
WPA	The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via authentication. Either **8~63** ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
	Type - Select from Mixed (WPA+WPA2) or WPA2 only. **Pre-Shared Key (PSK)** - Either **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
WEP	**64-Bit** - For 64 bits WEP key, either **5** ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)
	128-Bit - For 128 bits WEP key, either **13** ASCII

characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D).

Encryption Mode: 64-Bit ▾
                   64-Bit
                   128-Bit

All wireless devices must support the same WEP encryption bit size and have the same key. **Four keys** can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.

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

4.11.4 Access Control

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

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

Available settings are explained as follows:

Item	Description
Enable Mac Address Filter	Select to enable the MAC Address filter for wireless LAN identified with SSID 1 to 4 respectively. All the clients (expressed by MAC addresses) listed in the box can be grouped under different wireless LAN. For example, they can be grouped under SSID 1 and SSID 2 at the same time if you check SSID 1 and SSID 2.
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Apply SSID	After entering the client's MAC address, check the box of the SSIDs desired to insert this MAC address into their access control list.
Attribute	**s: Isolate the station from LAN -** select to isolate the wireless connection of the wireless client of the MAC address from LAN.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.

Dray Tek

Cancel	Give up the access control set up.
OK	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.

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

4.11.5 WPS

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

Note: Such function is available for the wireless station with WPS supported.

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

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

- On the side of Vigor2120 series which served as an AP, press **WPS** button once on the front panel of the router or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.
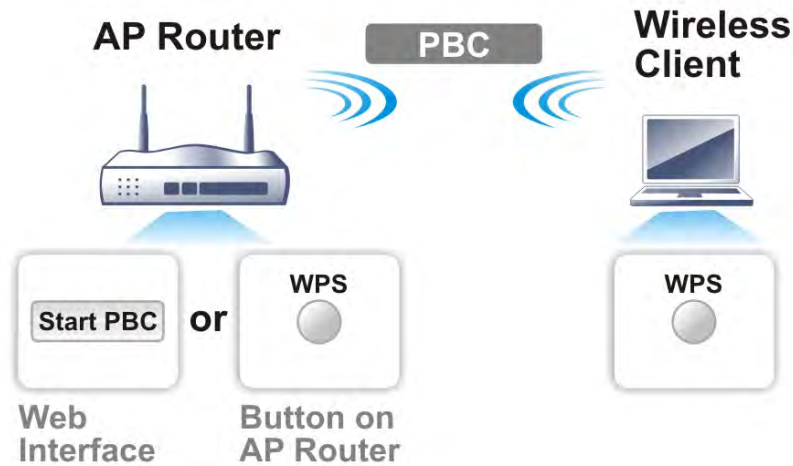
- If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the vigor router.
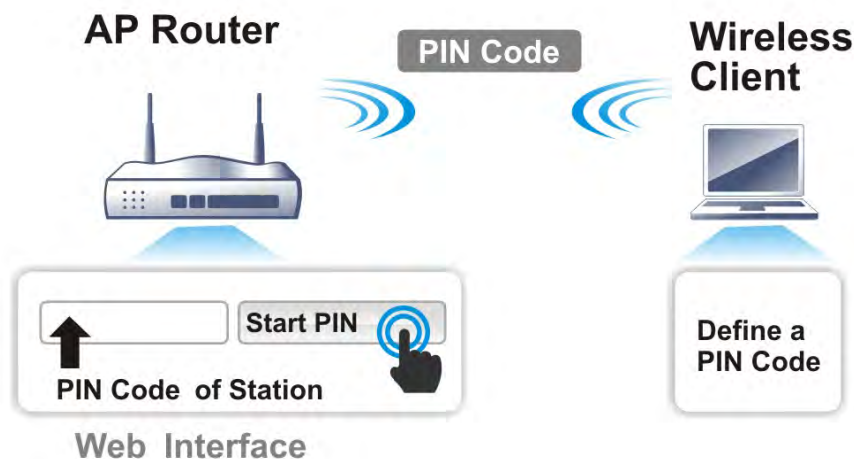
For WPS is supported in WPA-PSK or WPA2-PSK mode, if you do not choose such mode in **Wireless LAN>>Security**, you will see the following message box.
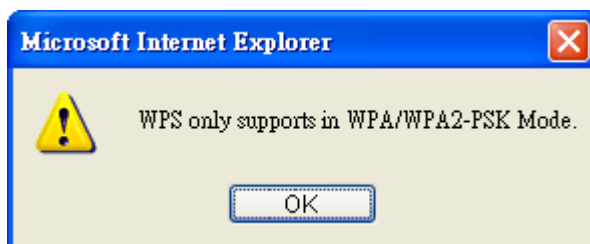
Please click **OK** and go back **Wireless LAN>>Security** to choose WPA-PSK or WPA2-PSK mode and access WPS again.

DrayTek

Below shows **Wireless LAN>>WPS** web page:

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

☑ Enable WPS

Wi-Fi Protected Setup Information

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

Device Configure

Configure via Push Button	Start PBC
Configure via Client PinCode	[ ] Start PIN

Status: Wireless LAN is NOT enabled!!

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

: WPS is Disabled.

: WPS is Enabled.

: Waiting for WPS requests from wireless clients.

Available settings are explained as follows:

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

4.11.6 WDS

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

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

To meet the above requirement, two WDS modes are implemented in Vigor router. One is **Bridge**, the other is **Repeater**. Below shows the function of WDS-bridge interface:
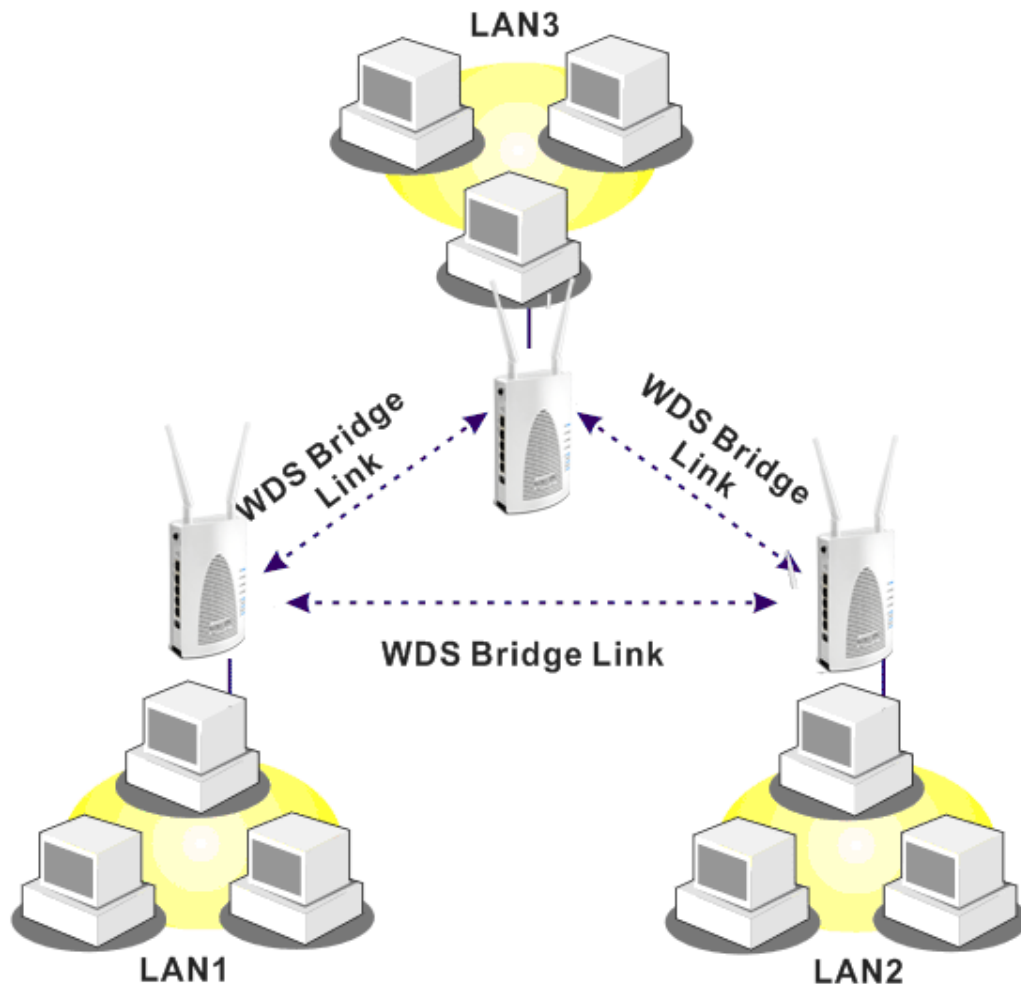
The application for the WDS-Repeater mode is depicted as below:

Dray Tek

Host with bridge Interface 1 — WDS Link — Host with repeater Interface — WDS Link — Host with bridge Interface 2
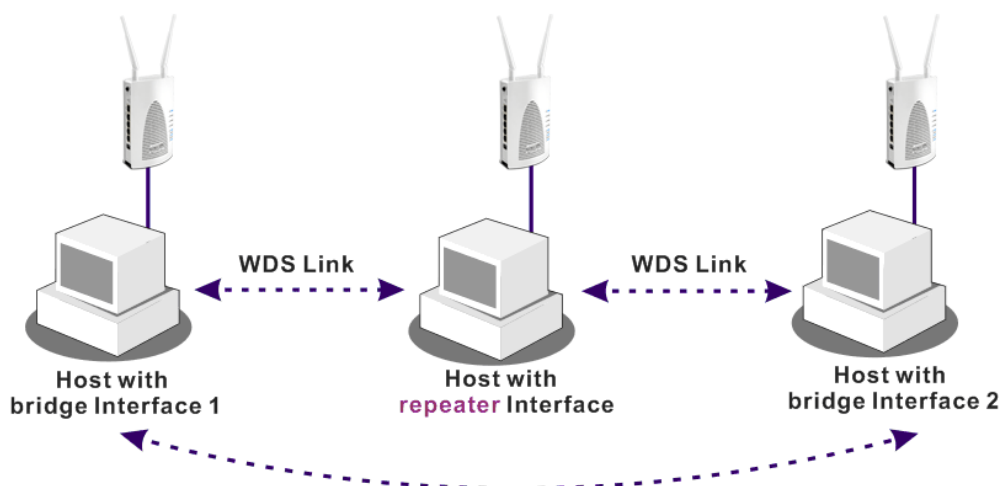
The major difference between these two modes is that: while in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links. Yet in **Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words, only Repeater mode can do WDS-to-WDS packet forwarding.

In the following examples, hosts connected to Bridge 1 or 3 can communicate with hosts connected to Bridge 2 through WDS links. However, hosts connected to Bridge 1 CANNOT communicate with hosts connected to Bridge 3 through Bridge 2.

Host with bridge Interface 1 — WDS Link — Host with bridge Interface 2 — WDS Link — Host with bridge Interface 3
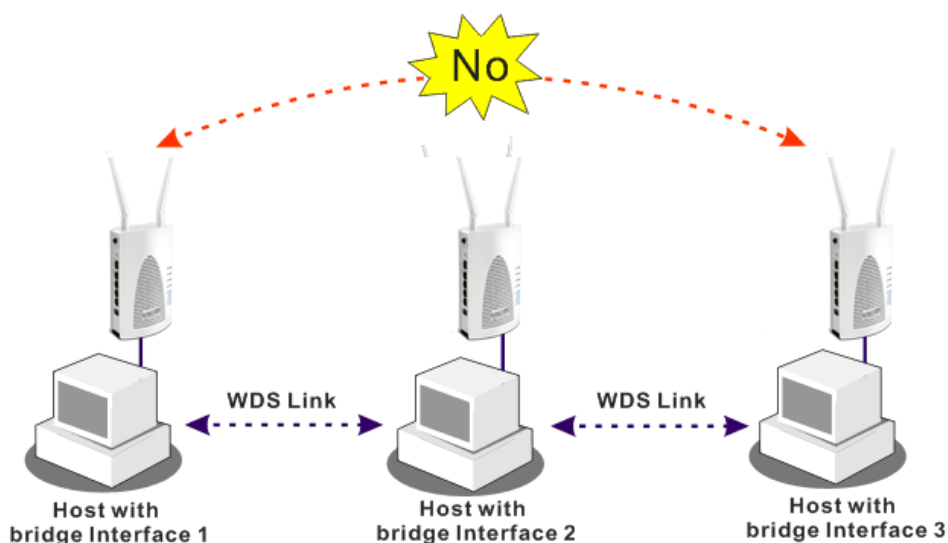
Click **WDS** from **Wireless LAN** menu. The following page will be shown.

Available settings are explained as follows:

Item	Description
Mode	Choose the mode for WDS setting. **Disable** mode will not invoke any WDS setting. **Bridge** mode is designed to fulfill the first type of application. **Repeater** mode is for the second one.
Security	There are three types for security, **Disable**, **WEP** and **Pre-shared key**. The setting you choose here will make the following WEP or Pre-shared key field valid or not. Choose one of the types for the router.
WEP	Check this box to use the same key set in **Security Settings** page. If you did not set any key in **Security Settings** page, this check box will be dimmed.
Pre-shared Key	**Type –** There are some types for you to choose. **WPA** and **WPA2** are used for WDS devices (e.g.2120n-plus wireless router, you can set the encryption mode as WPA or WPA2 to establish your WDS system between AP and the router. **Key -** Type 8 ~ 63 ASCII characters or 64 hexadecimal

	digits leading by "0x".
Bridge	If you choose Bridge as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Yet please disable the unused link to get better performance. If you want to invoke the peer MAC address, remember to check **Enable** box in the front of the MAC address after typing.
Repeater	If you choose Repeater as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Similarly, if you want to invoke the peer MAC address, remember to check **Enable** box in the front of the MAC address after typing.
Access Point Function	Click **Enable** to make this router serve as an access point; click **Disable** to cancel this function.
Status	It allows user to send "hello" message to peers. Yet, it is valid only when the peer also supports this function.

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

4.11.7 Advanced Setting

This page allows users to set advanced settings such as operation mode, channel bandwidth, guard interval, and aggregation MSDU for wireless data transmission.

2.4G

5G

Available settings are explained as follows:

Item	Description
Operation Mode	**Mixed Mode** – the router can transmit data with the ways supported in both 802.11a/b/g and 802.11n standards. However, the entire wireless transmission will be slowed down if 802.11g or 802.11b wireless client is connected.
	Green Field – to get the highest throughput, please choose such mode. Such mode can make the data transmission happen between 11n systems only. In addition, it does not have protection mechanism to avoid the conflict with neighboring devices of 802.11a/b/g.
Channel Bandwidth	**20-** the router will use 20MHz for data transmission and receiving between the AP and the stations.
	20/40 – the router will use 20MHz or 40MHz for data transmission and receiving according to the station capability. Such channel can increase the performance for data transmission.
Guard Interval	It is to assure the safety of propagation delays and reflections for the sensitive digital data. If you choose **auto** as guard interval, the AP router will choose short guard interval (increasing the wireless performance) or long guard interval for data transmit based on the station capability.

Aggregation MSDU	Aggregation MSDU can combine frames with different sizes. It is used for improving MAC layer's performance for some brand's clients. The default setting is **Enable.**
Long Preamble	This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. Click **Enable** to use **Long Preamble** if needed to communicate with this kind of devices.
Packet-OVERDRIVE	This feature can enhance the performance in data transmission about 40%* more (by checking **Tx Burst**). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too. **Note:** Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose **Enable** for **TxBURST** on the tab of **Option**). **Note:** * means the real transmission rate depends on the environment of the network.

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

4.11.8 WMM Configuration

WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC_BE , AC_BK, AC_VI and AC_VO for WMM.

APSD (automatic power-save delivery) is an enhancement over the power-save mechanisms supported by Wi-Fi networks. It allows devices to take more time in sleeping state and consume less power to improve the performance by minimizing transmission latency.

Available settings are explained as follows:

Item	Description
WMM Capable	To apply WMM parameters for wireless data transmission, please click the **Enable** radio button.
APSD Capable	The default setting is **Disable**.
Aifsn	It controls how long the client waits for each data transmission. Please specify the value ranging from 1 to 15. Such parameter will influence the time delay for WMM accessing categories. For the service of voice or video image, please set small value for AC_VI and AC_VO categories For the service of e-mail or web browsing, please set large value for AC_BE and AC_BK categories.
CWMin/CWMax	**CWMin** means contention Window-Min and **CWMax** means contention Window-Max. Please specify the value ranging from 1 to 15. Be aware that CWMax value must be greater than CWMin or equals to CWMin value. Both values will influence the time delay for WMM accessing categories. The difference between AC_VI and AC_VO categories must be smaller; however, the difference between AC_BE and AC_BK categories must be greater.

Txop	It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.
ACM	It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked. **Note:** Vigor2120provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.
AckPolicy	**"**Uncheck" (default value) the box means the AP router will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets. "Check" the box means the AP router will not answer any response request for the transmitting packets. It will have better performance with lower reliability.

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

4.11.9 AP Discovery

Vigor router can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of this router can be found. Please click **Scan** to discover APs in the neighborhood.

Access Point List

BSSID	Channel	SSID

[Scan]

See **Statistics**.

Note: During the scanning process (~5 seconds), no station is allowed to connect with the router.

Add to WDS Settings :

AP's MAC address   [ ] : [ ] : [ ] : [ ] : [ ] : [ ]

[Add to]   ⦿ Bridge   ○ Repeater

Available settings are explained as follows:

Item	Description
Scan	It is used to discover AP(s) in the neighborhood. The results will be shown on the box above this button.
Statistics	It displays the statistics for the channels used by APs. Wireless LAN >> Site Survey Statistics Recommended channels for usage:1 2 3 4 5 6 7 8 9 10 11 12 13 AP number v.s. Channel 1 2 3 4 5 6 7 8 9 10 11 12 13 14 Channel [Cancel]
Add to	If you want the found AP applying the WDS settings, please type in the AP's MAC address on the bottom of the page and click Bridge or Repeater. Next, click **Add to**. Later, the MAC address of the AP will be added to Bridge or Repeater field of WDS settings page.

DrayTek

4.11.10 Station List

Station List provides the knowledge of connecting wireless clients now along with its status code. There is a code summary below for explanation. For convenient **Access Control**, you can select a WLAN station and click **Add to Access Control** below.

Station List

Status	MAC Address	Associated with

[Refresh]

Status Codes :
C: Connected, No encryption.
E: Connected, WEP.
P: Connected, WPA.
A: Connected, WPA2.
B: Blocked by Access Control.
N: Connecting.
F: Fail to pass WPA/PSK authentication.

Note: After a station connects to the router successfully, it may be turned off without notice. In that case, it will still be on the list until the connection expires.

Add to Access Control :

Client's MAC address   [ ] : [ ] : [ ] : [ ] : [ ] : [ ]

[Add]

Available settings are explained as follows:

Item	Description
Refresh	Click this button to refresh the status of station list.
Add	Click this button to add current typed MAC address into **Access Control.**

Dray Tek

4.11.11 Station Control

Station Control is used to specify the duration for the wireless client to connect and reconnect Vigor router. If such function is not enabled, the wireless client can connect Vigor router until the router shuts down.

Such feature is especially useful for free Wi-Fi service. For example, a coffee shop offers free Wi-Fi service for its guests for one hour every day. Then, the connection time can be set as "1 hour" and reconnection time can be set as "1 day". Thus, the guest can finish his job within one hour and will not occupy the wireless network for a long time.

Note: Up to 300 Wireless Station records are supported by Vigor router.

Wireless LAN (2.4 GHz) >> Station Control

SSID 1	SSID 2	SSID 3	SSID 4	
SSID	DrayTek			
Enable	☐			
Connection Time	1 hour ▼	60		min
Reconnection Time	1 day ▼	1440		min

Display All Station Control List

WEB Portal Setup

Note: Once the feature is enabled, the Internet accessability will be restricted by the wireless station MAC address with the specific connection time.

[OK]   [Cancel]

Available settings are explained as follows:

Item	Description
SSID	Display the SSID that the wireless station will use it to connect with Vigor router.
Enable	Check the box to enable the station control function.
Connection Time / Reconnection Time	Use the drop down list to choose the duration for the wireless client connecting /reconnecting to Vigor router. Or, type the duration manually when you choose **User defined**. 1 day ▼ 1440 min User defined 30 min 1 hour 2 hours 4 hours 1 day 2 days 3 days 4 days 5 days 6 days 7 days
Display All Station Control List	All the wireless stations connecting to Vigor router by using such SSID will be listed on Station Control List.
WEB Portal Setup	Click it to access in to **LAN>>Web Portal Setup** page for

	modifying the settings if required.

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

4.12 SSL VPN

An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be sed with a standard Web browser.

There are two benefits that SSL VPN provides:

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

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

SSL VPN
General Setup
SSL Application
User Account
Online User Status

4.12.1 General Setup

This page determines the general configuration for SSL VPN Server and SSL Tunnel.

SSL VPN >> General Setup

SSL VPN General Setup

Port	443	(Default: 443)
Server Certificate	self-signed	

Note: The settings will act on all SSL applications.
Please go to **System Maintenance >> Management** to enable SSLv3.0 .

OK   Cancel

Available settings are explained as follows:

Item	Description
Port	Such port is set for SSL VPN server. It will not affect the HTTPS Port configuration set in **System Maintenance>>Management**. In general, the default setting is 443.
Server Certificate	When the client does not set any certificate, default certificate will be used for HTTPS and SSL VPN server. Choose any one of the user-defined certificates from the drop down list if users set several certificates previously. Otherwise, choose **Self-signed** to use the router's built-in default certificate. The default certificate can be used in SSL VPN server and HTTPS Web Proxy.

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

4.12.2 SSL Application

It provides a secure and flexible solution for network resources, including VNC (Virtual Network Computer) /RDP (Remote Desktop Protocol), to any remote user with access to Internet and a web browser.

SSL VPN >> SSL Application

SSL Applications Profiles: | Set to Factory Default |

Index	Name	Host Address	Service	Active
1.				x
2.				x
3.				x
4.				x
5.				x
6.				x
7.				x
8.				x
9.				x
10.				x

Each item is explained as follows:

Item	Description
Name	Display the application name of the profile that you create.
Host Address	Display the IP address for VNC/RDP.
Service	Display the type of the service selected, e.g., VNC/RDP.
Active	Display current status (active or inactive) of the selected profile.

To create a new SSL application profile:

1. Click number link under Index filed to set detailed configuration.

SSL VPN >> SSL Application

SSL Applications Profiles:

Index	Name	Hos
1.		
2.		
3.		
4.		

DrayTek

2. The following page will appear.

SSL VPN >> SSL Application

Profile Index : 8

☐ Enable Application Service

Application Name   [   ]

Application   [Virtual Network Computing (VNC) ▼]

                ---Please Select---

IP Address   Virtual Network Computing (VNC)

                Remote Desktop Protocol (RDP)

Port

Idle Timeout   [0   ] second(s)

Scaling   [100% ▼]

[OK]   [Clear]   [Cancel]

Available settings are explained as follows:

Item	Description
Enable Application Server	Check the box to enable such profile.
Application Name	Type a name for such application. The length of the name is limited to 23 characters.
Application	There are three types offered for you to create an application profile. [Virtual Network Computing (VNC) ▼] ---Please Select--- Virtual Network Computing (VNC) Remote Desktop Protocol (RDP) **Virtual Network Computing (VNC)** – It allows you to access and control a remote PC through VNC protocol. **Remote Desktop Protocol (RDP)** – It allows you to access and control a remote PC through RDP protocol.
IP Address	If you choose VNC or RDP, you have to type the IP address for this protocol.
Port	If you choose VNC or RDP, you have to specify the port used for this protocol. The default setting is 5900.
Idle Timeout	If you choose VNC, you have to specify the time for disconnecting the SSL VPN tunnel.
Scaling	If you choose VNC, you have to choose the percentage (100%, 80%, 60%) for such application.
Screen Size	If you choose RDP, you have to choose the screen size for such application.

3. Enter the required information.

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

DrayTek

     Vigor2120 Series User's Guide

SSL VPN >> SSL Application

SSL Applications Profiles: | Set to Factory Default |

Index	Name	Host Address	Service	Active
1.	VNC_1	192.168.1.51:5900	VNC	v
2.				x
3.				x

4.12.3 User Account

With SSL VPN, Vigor2120 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, Vigor2120 series allows up to 16 simultaneous incoming users.

For SSL VPN, identity authentication and power management are implemented through deploying user accounts. Therefore, the user account for SSL VPN must be set together with remote dial-in user web page. Such menu item will guide to access into **VPN and Remote Access>>Remote Dial-in User**.

SSL VPN >> Remote Dial-in User

Remote Access User Accounts: | Set to Factory Default |

Index	User	Active	Status	Index	User	Active	Status
1.	???	☐	---	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.	???	☐	---

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

[OK]   [Cancel]

Click each index to edit one remote user profile.

SSL VPN >> Remote Dial-in User
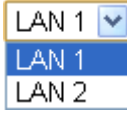
Index No. 1

User account and Authentication
☐ Enable this account
Idle Timeout [300] second(s)

Allowed Dial-In Type
☑ PPTP
☑ IPsec Tunnel
☑ L2TP with IPsec Policy [None ▼]
☑ SSL 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]
SSL VPN
[Set SSL Application]

Username [???]
Password(Max 19 char) [_____]
☐ Enable Mobile One-Time Passwords(mOTP)
  PIN Code [_____]
  Secret [_____]

IKE Authentication Method
☑ Pre-Shared Key
[IKE Pre-Shared Key] [_____]
☐ Digital Signature(X.509)
[None ▼]

IPsec Security Method
☑ Medium(AH)
High(ESP)   ☑ DES ☑ 3DES ☑ AES
Local ID (optional) [_____]

[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.
Allowed Dial-In Type	**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 make 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.

Item	Description
	● **Must -** Specify the IPSec policy to be definitely applied on the L2TP connection.
	Must - It allows the remote dial-in user to make an SSL VPN Tunnel connection through Internet, suitable for the application through network accessing (e.g., PPTP/L2TP/IPSec)
	If you check this box, the function of SSL Tunnel for this account will be activated immediately.
	Specify Remote Node - Check the checkbox to specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode). If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the **general settings**.
	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.
Subnet	Chose one of the subnet selections for such VPN profile. LAN 1 LAN 1 LAN 2 **Assign Static IP Address –** Please type a static IP address for the subnet you specified.
SSL VPN	**Set SSL Application** - Choose the SSL application profile to be applied by such dial-in user profile.
User Name	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
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).
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

Item	Description
	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.**
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method. **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-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 - 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.

4.12.4 Online User Status

If you have finished the configuration of SSL Web Proxy (server), users can find out corresponding settings when they access into **Draytek SSL VPN portal** interface.
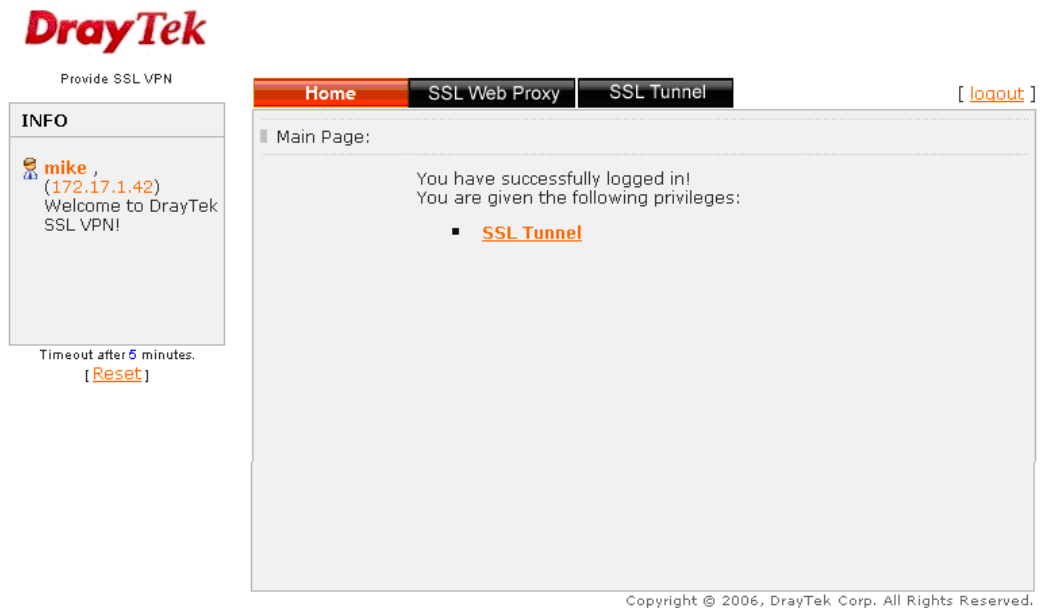
Next, users can open **SSL VPN>> Online Status** to view logging status of SSL VPN.

Available settings are explained as follows:

Item	Description
Active User	Display current user who visit SSL VPN server.
Host IP	Display the IP address for the host.
Time out	Display the time remaining for logging out.
Action	You can click **Drop** to drop certain login user from the router's SSL Portal UI.

4.13 USB Application

USB storage disk connected on Vigor router can be regarded as a server or WAN interface. By way of Vigor router, clients on LAN can access, write and read data stored in USB storage disk with different applications. After setting the configuration in **USB Application**, you can type the IP address of the Vigor router and username/password created in **USB Application>>USB User Management** on the client software. Then, the client can use the FTP site (USB storage disk) or share the files through Vigor router.

> **Note**: USB ports on Vigor router are allowed to connect to USB modem. Models of the modems supported by Vigor router can be seen from **USB Application>>Modem Support List**. For network connection via USB modem, refer to **WAN>>Internet Access** and **WAN>>General Setup** for detailed information.

USB Application
USB General Settings
USB User Management
File Explorer
USB Device Status
Modem Support List

4.13.1 USB General Settings

This page will determine the number of concurrent FTP connection, and default charset for FTP server. At present, the Vigor router can support USB storage disk with formats of FAT16 and FAT32 only. Therefore, before connecting the USB storage disk into the Vigor router, please make sure the memory format for the USB storage disk is FAT16 or FAT32. It is recommended for you to use FAT32 for viewing the filename completely (FAT16 cannot support long filename).

USB Application >> USB General Settings

USB General Settings

General Settings	
Simultaneous FTP Connections	5 (Maximum 6)
Default Charset	English

Note: 1. If Charset is set to "English", only English long file name is supported.
2. Multi-session ftp download will be banned by Router FTP server. If your ftp client have multi-connection mechanism, such as FileZilla, you may limit client connections setting to 1 to get better performance.

[OK]

Available settings are explained as follows:

Item	Description
General Settings	**Simultaneous FTP Connections -** This field is used to specify the quantity of the FTP sessions. The router allows up to 6 FTP sessions connecting to USB storage disk at one time.
	Default Charset - At present, Vigor router supports four types of character sets. Default Charset is for English based file name.

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

4.13.2 USB User Management

This page allows you to set profiles for FTP users. Any user who wants to access into the USB storage disk must type the same username and password configured in this page. Before adding or modifying settings in this page, please insert a USB storage disk first. Otherwise, an error message will appear to warn you.

Click index number to access into configuration page.
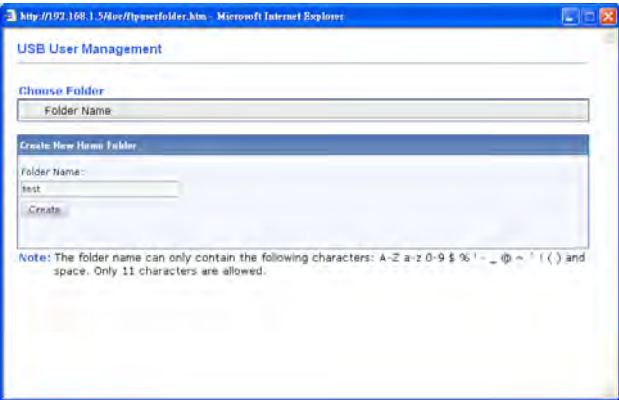
Available settings are explained as follows:

Item	Description
FTP	**Enable** – Click this button to activate this profile (account) for FTP service. Later, the user can use the username

	specified in this page to login into FTP server.
	Disable – Click this button to disable such profile.
Username	Type the username for FTP users for accessing into FTP server (USB storage disk). Be aware that users cannot access into USB storage disk in anonymity. Later, you can open FTP client software and type the username specified here for accessing into USB storage disk. The length of the name is limited to 11 characters.
	Note: "Admin" could not be typed here as username, for the word is specified for accessing into web pages of Vigor router only. Also, it is reserved for FTP firmware upgrade usage.
	Note: FTP Passive mode is not supported by Vigor Router.
	Please disable the mode on the FTP client.
Password	Type the password for FTP users for accessing FTP server. Later, you can open FTP client software and type the password specified here for accessing into USB storage disk. The length of the password is limited to 11 characters.
Confirm Password	Type the password again to make confirmation.
Home Folder	It determines the folder for the client to access into.
	The user can enter a directory name in this field. Then, after clicking **OK**, the router will create the specific/new folder in the USB storage disk. In addition, if the user types "/" here, he/she can access into all of the disk folders and files in USB storage disk.
	Note: When write protect status for the USB storage disk is **ON**, you cannot type any new folder name in this field. Only "/" can be used in such case.
	You can click to open the following dialog to add any new folder which can be specified as the Home Folder.
Access Rule	It determines the authority for such profile. Any user, who uses such profile for accessing into USB storage disk, must follow the rule specified here.
	File – Check the items (Read, Write and Delete) for such profile.
	Directory –Check the items (List, Create and Remove) for such profile.

Before you click **OK**, you have to insert a USB storage disk into the USB interface of the Vigor router. Otherwise, you cannot save the configuration.

4.13.3 File Explorer

File Explorer offers an easy way for users to view and manage the content of USB storage disk connected on Vigor router.

USB Application >> File Explorer

File Explorer

	Name	Size	Delete	Rename
⇆ ↑ 📁	Current Path: /			

↑ **Upload File**

Select a file:

[   ] [瀏覽...]

[Upload]

Note: The folder can not be deleted when it is not empty.

Available settings are explained as follows:

Item	Description
⇆ **Refresh**	Click this icon to refresh files list.
↑ **Back**	Click this icon to return to the upper directory.
📁 **Create**	Click this icon to add a new folder.
Current Path	Display current folder.
Upload	Click this button to upload the selected file to the USB storage disk. The uploaded file in the USB diskette can be shared for other user through FTP.

DrayTek

4.13.4 USB Device Status

This page is to monitor the status for the users who accessing into FTP or Samba server (USB storage disk) via the Vigor router. In addition, the status of the USB modem or USB printer connecting to Vigor router can be checked from such page. If you want to remove the storage disk from USB port in router, please click **Disconnect USB Disk** first. And then, remove the USB storage disk later.

Available settings are explained as follows:

Item	Description
Connection Status	If there is no USB storage disk connected to Vigor router, "**No Disk Connected**" will be shown here.
Disk Capacity	It displays the total capacity of the USB storage disk.
Free Capacity	It displays the free space of the USB storage disk. Click **Refresh** at any time to get new status for free capacity.
Index	It displays the number of the client connecting to FTP server.
IP Address	It displays the IP address of the user's host connecting to the FTP server.
Username	It displays the username that user uses to login to the FTP server.

When you insert USB storage disk into the Vigor router, the system will start to find out such device within several seconds.

| Disk | Modem | Printer | | Refresh | |

USB Mass Storage Device Status

Connection Status: Disk Connected   [Disconnect USB Disk]
Write Protect Status: No
Disk Capacity: 2009 MB
Free Capacity: 925 MB   **Refresh**

USB Disk Users Connected

Index	Service	IP Address(Port)	Username

Note: If the write protect switch of USB disk is turned on, the USB disk is in **READ-ONLY** mode. No data can be written to it.

4.13.5 Modem Support List

Such page provides the information about the brand name and model name of the USB modems which are supported by Vigor router.

USB Application >> Modem Support List

The following compatibility test lists 3.5G/LTE modems **supported by Vigor router under certain environment or countries.** If the LTE modem you have is on the list but cannot work properly, please write an e-mail to support@draytek.com or consult your dealer for further information.

PPP mode	DHCP mode		
Brand	**Model**	**LTE**	**Status**
Aiko	Aiko 83D		Y
Alcatel	Alcatel L100V	✓	Y
Alcatel	Alcatel W100	✓	Y
BandRich	Bandluxe C170		Y
BandRich	Bandluxe C270		Y
BandRich	Bandluxe C321		Y
BandRich	Bandluxe C330		Y
BandRich	Bandluxe C502		Y
Huawei	Huawei E169u		Y
Huawei	Huawei E220		Y
Huawei	Huawei E303D		Y
Huawei	Huawei E3131		Y

4.14 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, SNMP, Management, Reboot System, Firmware Upgrade and Activation.

Below shows the menu items for System Maintenance.

USB Application
System Maintenance
System Status
TR-069
Administrator Password
User Password
Login Page Greeting
Configuration Backup
SysLog / Mail Alert
Time and Date
SNMP
Management
Reboot System
Firmware Upgrade
Activation

4.14.1 System Status

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

System Status

Model Name	: Vigor2120n+	
Firmware Version	: 3.7.5.4_RC1	
Build Date/Time	: Jan 7 2015 20:11:29	

LAN

	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-1D-AA-9E-4F-F4	192.168.1.1	255.255.255.0	Yes	8.8.8.8
LAN2	00-1D-AA-9E-4F-F4	192.168.2.1	255.255.255.0	Yes	8.8.8.8
IP Routed Subnet	00-1D-AA-9E-4F-F4	192.168.0.1	255.255.255.0	Yes	8.8.8.8

Wireless LAN

MAC Address	Frequency Domain	Firmware Version	SSID
00-1D-AA-9E-4F-F4	Europe	2.7.1.5	DrayTek

Wireless LAN(5GHz)

MAC Address	Frequency Domain	Firmware Version	SSID
00-1D-AA-9E-4F-F6	Europe	2.7.1.5	DrayTek_5G

WAN

	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Disconnected	00-1D-AA-9E-4F-F5	---	---	---
WAN2	Disconnected	00-1D-AA-9E-4F-F6	---	---	---

IPv6

	Address	Scope	Internet Access Mode
LAN	FE80::21D:AAFF:FE9E:4FF4/64	Link	---

User Mode is OFF now.

Available settings are explained as follows:

Item	Description
Model Name	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
Build Date/Time	Display the date and time of the current firmware build.
LAN	**MAC Address** **-** Display the MAC address of the LAN Interface. **IP Address** **-** Display the IP address of the LAN interface. **Subnet Mask** **-** Display the subnet mask address of the LAN interface. **DHCP Server** **-** Display the current status of DHCP server of the LAN interface **DNS** **-** Display the assigned IP address of the primary DNS.
WAN	**Link Status** **-** Display current connection status. **MAC Address** **-** Display the MAC address of the WAN Interface. **Connection** **-** Display the connection type. **IP Address** **-** Display the IP address of the WAN interface. **Default Gateway** **-** Display the assigned IP address of the default gateway.
IPv6	**Address -** Display the IPv6 address for LAN. **Scope -** Display the scope of IPv6 address. For example, IPv6 **Link Local** could only be used for direct IPv6 link. It can't be used for IPv6 internet. **Internet Access Mode –** Display the connection mode chosen for accessing into Internet.

Dray Tek

4.14.2 TR-069

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

Available settings are explained as follows:

Item	Description
ACS Server On	Choose the interface for the router connecting to ACS server.
ACS Server	**URL/Username/Password –** Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information.
	Test With Inform – Click it to send a message based on the event code selection to test if such CPE is able to communicate with VigorACS SI server.
	Event Code – Use the drop down menu to specify an event

	to perform the test.
	Last Inform Response Time – Display the time that VigorACS server made a response while receiving Inform message from CPE last time.
CPE Client	Such information is useful for Auto Configuration Server.
	Enable/Disable – Allow/Deny the CPE Client to connect with Auto Configuration Server.
	Port – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE.
Periodic Inform Settings	The default setting is **Enable**. Please set interval time or schedule time for the router to send notification to CPE. Or click **Disable** to close the mechanism of notification.
STUN Settings	The default is **Disable**. If you click **Enable**, please type the relational settings listed below:
	Server IP – Type the IP address of the STUN server.
	Server Port – Type the port number of the STUN server.
	Minimum Keep Alive Period – If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds".
	Maximum Keep Alive Period – If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.

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

4.14.3 Administrator Password

This page allows you to set new password.

System Maintenance >> Administrator Password Setup

Administrator Password

Old Password		
New Password		(Max. 23 characters allowed)
Confirm Password		(Max. 23 characters allowed)

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

OK

Available settings are explained as follows:

Item	Description
Old Password	Type in the old password. The factory default setting for password is **"admin"**.

New Password	Type in new password in this field. The length of the password is limited to 23 characters.
Confirm Password	Type in the new password again.

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

4.14.4 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	After checking this box, you can access into the web user interface with the password typed here for simple web configuration. The settings on simple web user interface will be different with full web use interface accessed by using the administrator password.
Password	Type in new password in this field. The length of the password is limited to 31 characters.
Confirm Password	Type in the new password again.

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

Below shows an example for accessing into User Operation with User Password.

1. Open **System Maintenance>>User Password**.

2. Check the box of **Enable User Mode for simple web configuration** to enable user mode operation. Type a new password in the field of New Password and click **OK**.

3. The following screen will appear. Simply click **OK**.

4. Log out Vigor router web user interface by clicking the Logout button.

5. The following window will be open to ask for username and password. Type the new user password in the filed of **Password** and click **Login**.

DrayTek

6. The main screen with User Mode will be shown as follows.
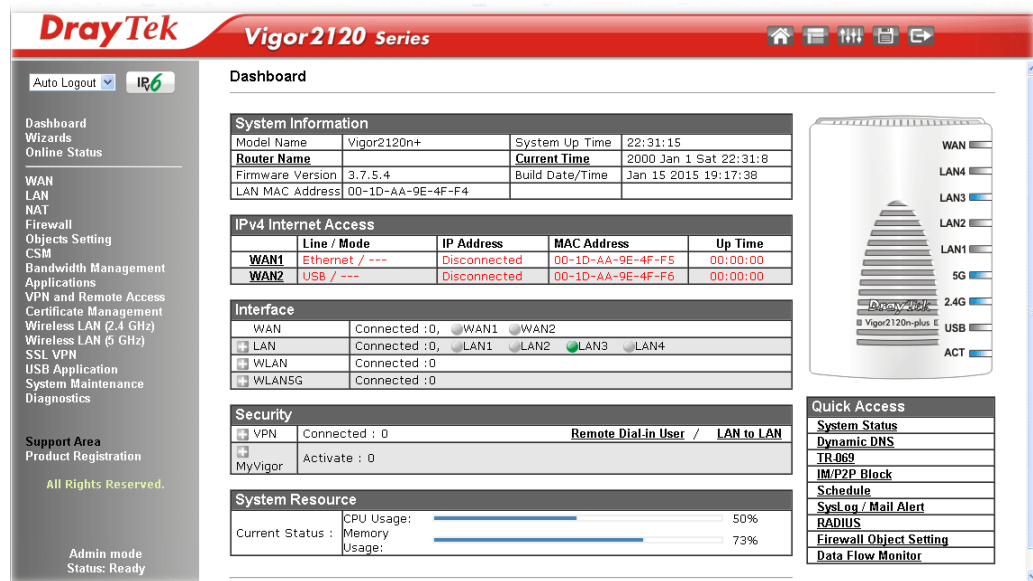
Settings to be configured in User Mode will be less than settings in Admin Mode. Only basic configuration settings will be available in User Mode.

Note: Setting in User Mode can be configured as same as in Admin Mode.

4.14.5 Login Page Greeting

When you want to access into the web user interface of Vigor router, the system will ask you to offer username and password first. At that moment, the background of the web page is blank and no heading will be displayed on the Login window. This page allows you to specify login URL and the heading on the Login window if you have such requirement.

System Maintenance >> Login Page Greeting

Login Page Greeting

☐ Enable

Login Page Title   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	Type a brief description (e.g., Welcome to DrayTek) which will be shown on the heading of the login dialog.
Welcome Message and Bulletin	Type words or sentences here. It will be displayed for bulletin message. In addition, it can be displayed on the login dialog at the bottom. Note that do not type URL redirect link here.
Preview	Click it to display the preview of the login window based on the settings on this web page.
Set to Factory Default	Click to return to the factory default setting.

Dray Tek

Below shows an example of login customization with the information typed in Login Description and Bulletin.
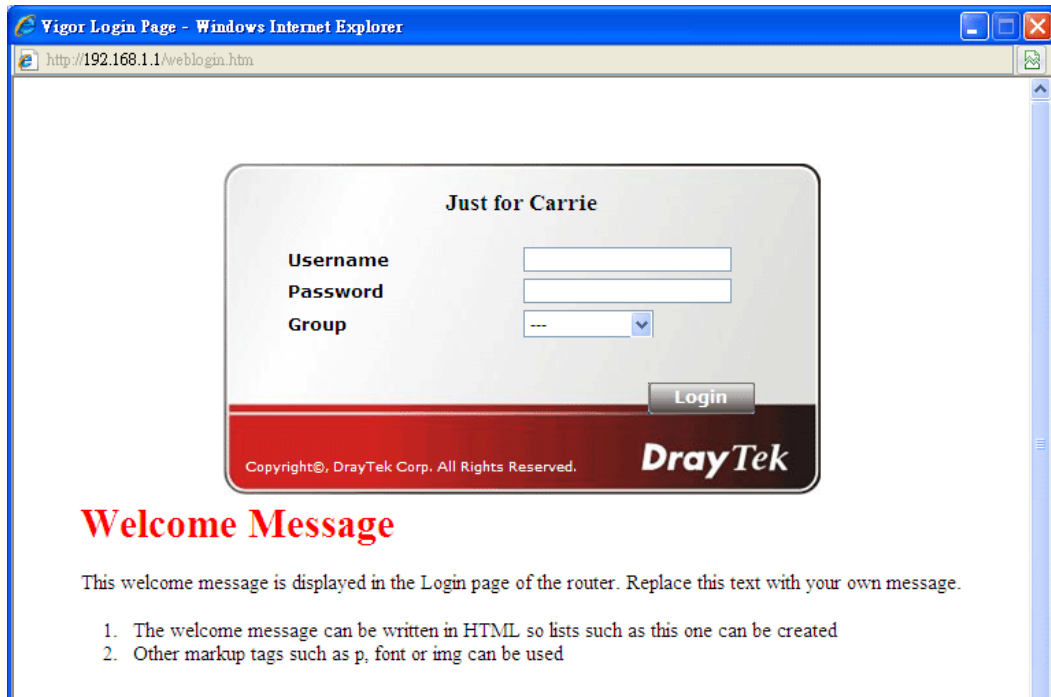
4.14.6 Configuration Backup

Such function can be used to apply the router settings configured by Vigor2110 to Vigor2120.

Backup the Configuration

Follow the steps below to backup your configuration.

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

System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restoration
Select a configuration file.
[Choose File]
Click Restore to upload the file.
[Restore]

Backup
Click Backup to download current running configurations as a file.
[Backup] [Cancel]

Note: Configuration restoration from V2110 supported, but verification after restoration is recommended as it's not guaranteed that every setting will map across perfectly.

Support Model List

Model	Firmware Version	Note
Vigor2110	3.6.5	The configuration of TR069 will not be converted and applied to Vigor2120.

Available settings are explained as follows:

Item	Description
Restoration	**Choose File** – Click it to specify a file to be restored. Click **Restore** to restore the configuration. If the file is encrypted, the system will ask you to type the password to decrypt the configuration file.
Backup	Click the **Backup** button to perform the configuration backup of this router.
Support Model List	Web configuration file from *other* Vigor router can be applied to Vigor2120 series. At present, the configuration file of Vigor2110 is accepted for Vigor 2120. This field displays model name(s) and firmware which web configuration file saved can be used by such router.

2. Click **Backup** button to get into the following dialog. Click **Save** button to open another dialog for saving configuration as a file.
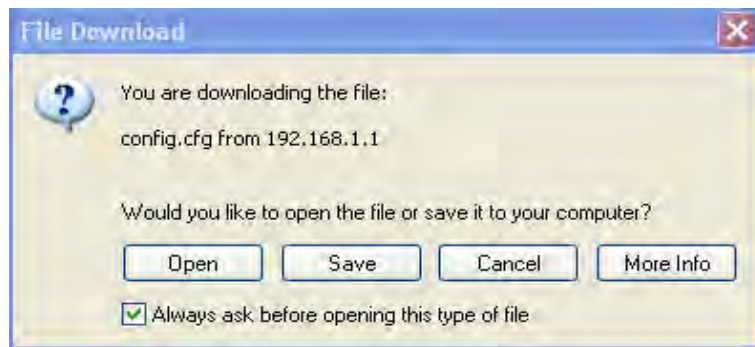
3. In **Save As** dialog, the default filename is **config.cfg**. You could give it another name by yourself.
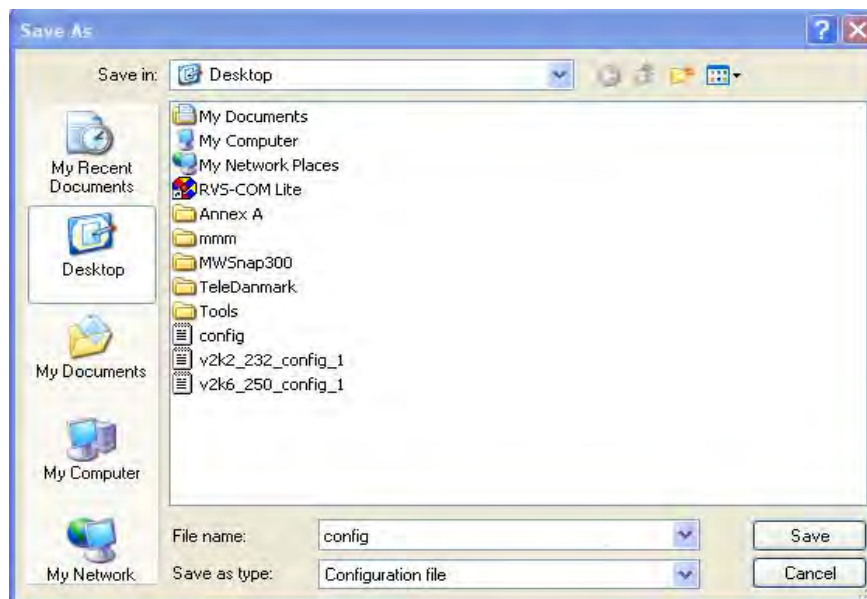
4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

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

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

Restore Configuration

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

System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restoration

Select a configuration file.

[Choose File]

Click Restore to upload the file.

[Restore]

Backup

Click Backup to download current running configurations as a file.

[Backup]   [Cancel]

Note: Configuration restoration from V2110 supported, but verification after restoration is recommended as it's not guaranteed that every setting will map across perfectly.

Support Model List

Model	Firmware Version	Note
Vigor2110	3.6.5	The configuration of TR069 will not be converted and applied to Vigor2120.

2. Click the **Choose File** button to choose the correct configuration file for uploading to the router.

3. Click the **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

4.14.7 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.
	USB Disk - Check **USB Disk** to save the log to the attached USB storage disk.
	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 Address -The IP address 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.
	● **User Name -** Type the user name for authentication.
	● **Password -** Type the password for authentication.
	Enable E-mail Alert - Check the box to send alert message to the e-mail box while the router detecting the item(s) you specify here.

Click **OK** to save these settings.

For viewing the Syslog, please do the following:

1. Just set your monitor PC's IP address in the field of Server IP Address

2. Install the Router Tools in the **Utility** within provided CD. After installation, click on the **Router Tools>>Syslog** from program menu.
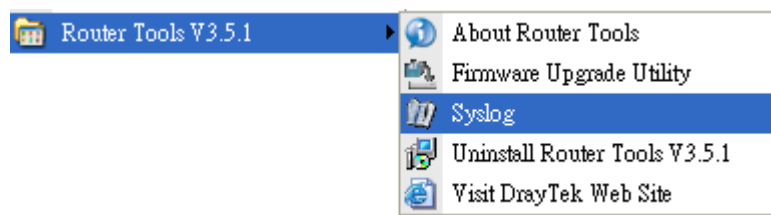
3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.
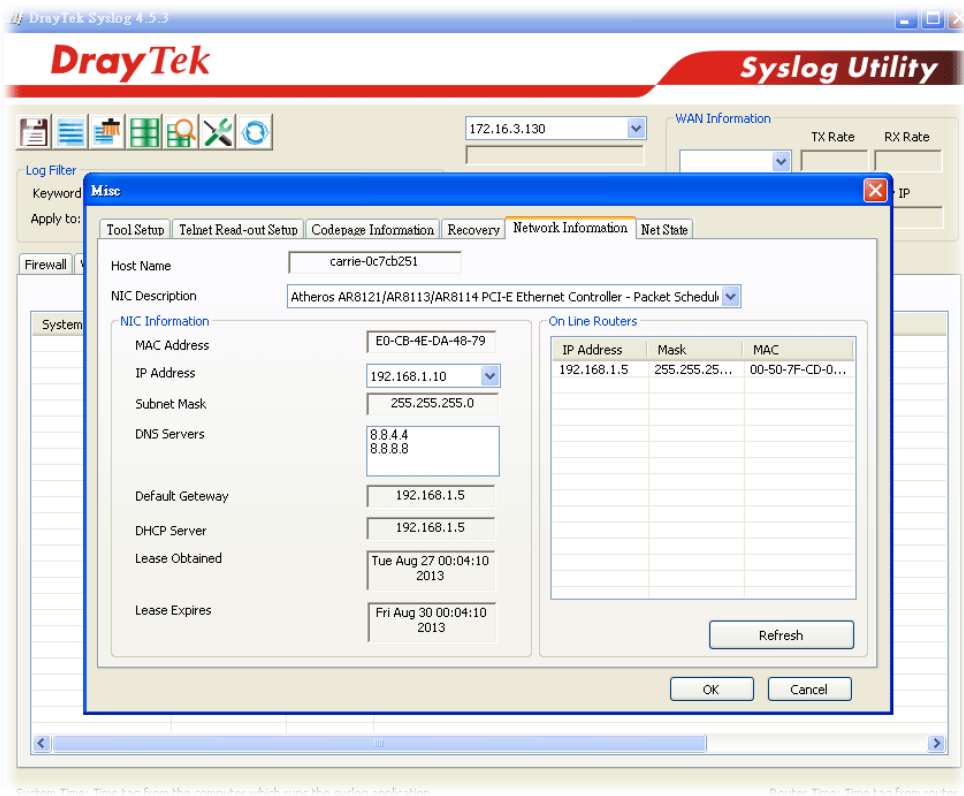
4.14.8 Time and Date

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

System Maintenance >> Time and Date

Time Information
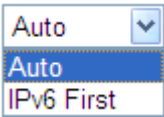
| Current System Time | 2013 Dec 19 Thu 7 : 2 : 29 | Inquire Time |

Time Setup

- ○ Use Browser Time
- ◉ Use Internet Time
  - Time Server: pool.ntp.org
  - Priority: Auto
  - Time Zone: (GMT) Greenwich Mean Time : Dublin
  - Enable Daylight Saving: ☐
  - Automatically Update Interval: 30 min

[OK] [Cancel]

Available settings are explained as follows:

Item	Description
Current System Time	Click **Inquire Time** to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.
Time Server	Type the IP address or domain name of the time server.
Priority	**IPv6 First** – If the time server configured with a domain name that supports IPv6; such option will be the first choice. **Auto** – It is the default setting. If you have no idea whether the time server supports IPv6 or IPv4, simply choose Auto as the priority. Auto Auto IPv6 First
Time Zone	Select the time zone where the router is located.
Enable Daylight Saving	Check the box to enable the daylight saving. Such feature is available for certain area.
Automatically Update Interval	Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

Dray Tek

4.14.9 SNMP

This page allows you to configure settings for SNMP and SNMPV3 services.

The SNMPv3 is **more secure than** SNMP through the encryption method (support AES and DES) and authentication method (support MD5 and SHA) for the management needs.

Available settings are explained as follows:
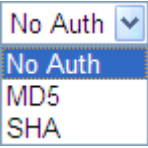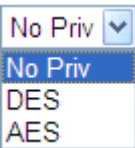
Item	Description
Enable SNMP Agent	Check it to enable this function.
Get Community	Set the name for getting community by typing a proper character. The default setting is **public.** The maximum length of the text is limited to 23 characters.
Set Community	Set community by typing a proper name. The default setting is **private.** The maximum length of the text is limited to 23 characters.
Manager Host IP (IPv4)	Set one host as the manager to execute SNMP function. Please type in IPv4 address to specify certain host.
Manager Host IP (IPv6)	Set one host as the manager to execute SNMP function. Please type in IPv6 address to specify certain host.
Trap Community	Set trap community by typing a proper name. The default setting is **public.** The maximum length of the text is limited to 23 characters.
Notification Host IP (IPv4)	Set the IPv4 address of the host that will receive the trap community.

Notification Host IP (IPv6)	Set the IPv6 address of the host that will receive the trap community.
Trap Timeout	The default setting is 10 seconds.
Enable SNMPV3 Agent	Check it to enable this function.
USM User	USM means user-based security mode. Type a username which will be used for authentication. The maximum length of the text is limited to 23 characters.
Auth Algorithm	Choose one of the encryption methods listed below as the authentication algorithm. No Auth ▾ No Auth MD5 SHA
Auth Password	Type a password for authentication. The maximum length of the text is limited to 23 characters.
Privacy Algorithm	Choose one of the methods listed below as the privacy algorithm. No Priv ▾ No Priv DES AES
Privacy Password	Type a password for privacy. The maximum length of the text is limited to 23 characters.

Click **OK** to save these settings.

4.14.10 Management

This page allows you to manage the settings for access control, access list and port setup. For example, as to management access control, the port number is used to send/receive SIP message for building a session.

The management pages for IPv4 and IPv6 protocols are different.
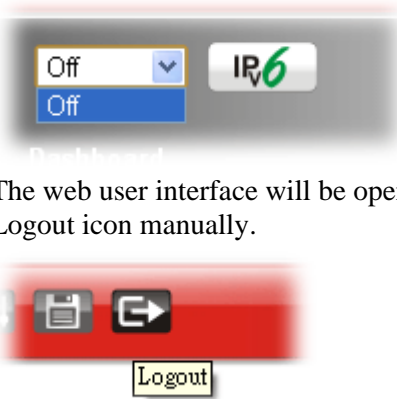
For IPv4

System Maintenance >> Management

IPv4 Management Setup	IPv6 Management Setup

Router Name [   ]

☐ Default:Disable Auto-Logout

Internet Access Control
☐ Allow management from the Internet
   ☐ FTP Server
   ☑ HTTP Server
   ☑ HTTPS Server
   ☑ Telnet Server
   ☑ TR069 Server
   ☐ SSH Server
☑ Disable PING from the Internet

Access List from the Internet

List	IP	Subnet Mask
1	[ ]	[▼]
2	[ ]	[▼]
3	[ ]	[▼]

Management Port Setup
  ◉ User Define Ports
  ○ Default Ports

Telnet Port	[23]	(Default: 23)
HTTP Port	[80]	(Default: 80)
HTTPS Port	[443]	(Default: 443)
FTP Port	[21]	(Default: 21)
TR069 Port	[8069]	(Default: 8069)
SSH Port	[22]	(Default: 22)

TLS/SSL Encryption Setup
☐ Enable SSL 3.0

External Device Control
☑ No respond to External Device

[OK]

Available settings are explained as follows:

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

Internet Access Control	**Allow management from the Internet** - Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.
	Disable PING from the Internet - Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.
Access List from the Internet	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.
	List IP - Indicate an IP address allowed to login to the router.
	Subnet Mask - Represent a subnet mask allowed to login to the router.
Management Port Setup	**User Define Ports -** Check to specify user-defined port numbers for the Telnet, HTTP and FTP servers.
	Default Ports - Check to use standard port numbers for the Telnet and HTTP servers.
TLS/SSL Encryption Setup	**Enable SSL 3.0 –** Check the box to enable the function of SSL 3.0 if required.
	Due to for security consideration, the built-in HTTPS and SSL VPN server of the router had upgraded to TLS1.x protocol. If you are using old browser(eg. IE6.0) or old SmartVPN Client, you may still need to enable SSL 3.0 to make sure you can connect, however, it's not recommended.
External Device Control	**No respond to External Device –** Check the box to make Vigor2120n-plus be detected by other router and not being displayed as an external device.

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

For IPv6

IPv4 Management Setup	IPv6 Management Setup

Management Access Control

Allow management from the Internet

☐ Telnet Server (Port : 23)

☐ HTTP Server (Port : 80)

☐ HTTPS Server (Port : 443)

☐ SSH Server (Port : 22)

☐ Enable PING from the Internet

Access List

List   IPv6 Address / Prefix Length

1. [   ] / [128]

2. [   ] / [128]

3. [   ] / [128]

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** - Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.
	Enable PING from the Internet - Check the checkbox to enable all PING packets from the Internet. For security issue, this function is disabled by default.
Access List	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.
	IPv6 Address /Prefix Length- Indicate the IP address(es) allowed to login to the router.

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

4.14.11 Reboot System

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

System Maintenance >> Reboot System

Reboot System

Do you want to reboot your router ?

⊙ Using current configuration
○ Using factory default configuration

Reboot Now

Auto Reboot Time Schedule

Index(1-15) in Schedule Setup: [   ], [   ], [   ], [   ]
Note: Action and Idle Timeout settings will be ignored.

OK   Cancel

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

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

Note: 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.

4.14.12 Firmware Upgrade

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

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

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

```
System Maintenance >> Firmware Upgrade

Web Firmware Upgrade
    Select a firmware file.
    [ Select ]

    Click Upgrade to upload the file.   [ Upgrade ]

TFTP Firmware Upgrade from LAN
    Current Firmware Version: 3.7.5.4

    Firmware Upgrade Procedures:

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

    Do you want to upgrade firmware ?   [ OK ]
```

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

Or, click **OK**. The following screen will appear. Then, execute the firmware upgrade utility.

```
System Maintenance >> Firmware Upgrade


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

4.14.13 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.

Available settings are explained as follows:

Item	Description
Activate via Interface	Choose WAN interface used by such device for activating Web Content Filter. auto-selected auto-selected WAN 1 Backup WAN
Activate	The **Activate** link brings you accessing into www.vigorpro.com to finish the activation of the account and the router.
Authentication Message	As for authentication information of **web filter**, the process of authenticating will be displayed on this field for your reference.

Below shows the successful activation of Web Content Filter:

4.15 Diagnostics

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

Below shows the menu items for Diagnostics.

4.15.1 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.

DrayTek

4.15.2 Routing Table

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

Diagnostics >> View Routing Table

| Current Running Routing Table | IPv6 Routing Table | | Refresh | |

```
Key: C - connected, S - static, R - RIP, * - default, ~ - private
C~       192.168.1.0/ 255.255.255.0    directly connected    LAN1
```

And,

Diagnostics >> View Routing Table

| Current Running Routing Table | IPv6 Routing Table | | Refresh | |

```
Destination                     Interface Flags     Metric    Next Hop
FE80::/64                       LAN       U         256
FF00::/8                        LAN       U         256
```

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

4.15.3 ARP Cache Table

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

```
Diagnostics >> View ARP Cache Table

Ethernet ARP Cache Table                                      | Clear | Refresh |
IP Address        MAC Address        Netbios Name    Interface
192.168.1.5       00-50-7F-CD-07-48                  LAN1
192.168.1.49      E0-CB-4E-DA-48-79  CARRIE-0C7CB251 LAN1
```

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

4.15.4 IPv6 Neighbour Table

The table shows a mapping between an Ethernet hardware address (MAC Address) and an IPv6 address. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **IPv6 Neighbour Table** to open the web page.

```
Diagnostics >> View IPv6 Neighbour Table

IPv6 Neighbour Table                                            | Refresh |
IPv6 Address                          Mac Address        Interface
FF02::2                               33-33-00-00-00-02  LAN
FF02::1:3                             33-33-00-01-00-03  LAN
FE80::3D5E:E74:8751:A44B              e8-9d-87-87-69-2f  LAN
FF02::1:FF51:A44B                     33-33-ff-51-a4-4b  LAN
FE80::250:7FFF:FEC9:1E79              00-50-7f-c9-1e-79  LAN
FE80::250:7FFF:FEC8:4305              00-50-7f-c8-43-05  LAN
FF02::1                               33-33-00-00-00-01  LAN
FF02::1                               00-00-00-00-00-00  USB2
FF02::1:2                             00-00-00-00-00-00  USB2
FE80::9D5C:CA86:5428:3CA7             00-26-2d-fe-63-4f  LAN
FF02::1:FF0A:673C                     33-33-ff-0a-67-3c  LAN
```

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

DrayTek

4.15.5 DHCP Table

The facility provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

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

Diagnostics >> View DHCP Assigned IP Addresses

| DHCP IP Assignment Table | DHCPv6 IP Assignment Table | | Refresh | |

```
LAN1 : 192.168.1.1/255.255.255.0, DHCP server: On
Index      IP Address          MAC Address          Leased Time     HOST ID
```

☐ Show Comment

And,

Diagnostics >> View DHCP Assigned IP Addresses

| DHCP IP Assignment Table | DHCPv6 IP Assignment Table | | Refresh | |

```
DHCPv6 server binding client:
Index    IPv6 Address                         MAC Address      Leased Time
```

☐ Show Comment

Available settings are explained as follows:

Item	Description
Index	It displays the connection item number.
IP Address	It displays the IP address assigned by this router for specified PC.
MAC Address	It displays the MAC address for the specified PC that DHCP assigned IP address for it.

Leased Time	It displays the leased time of the specified PC.
HOST ID	It displays the host ID name of the specified PC.
Refresh	Click it to reload the page.

4.15.6 NAT Sessions Table

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

Diagnostics >> NAT Sessions Table

NAT Active Sessions Table | Refresh |

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

Available settings are explained as follows:

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

DrayTek

4.15.7 Ping Diagnosis

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

And,

Available settings are explained as follows:

Item	Description
IPV4 /IPV6	Choose the interface for such function.
Ping to	Use the drop down list to choose the destination that you want to ping.
IP Address	Type the IP address of the Host/IP that you want to ping.
Ping IPv6 Address	Type the IPv6 address that you want to ping.
Run	Click this button to start the ping work. The result will be displayed on the screen.
Clear	Click this link to remove the result on the window.

4.15.8 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.

Bandwidth Management >> Sessions Limit

Sessions Limit

◉ Enable   ○ Disable
Default Max Sessions: 100
Limitation List

Index	Start IP	End IP

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

Diagnostics >> Data Flow Monitor

☐ Enable Data Flow Monitor

Refresh Seconds: 10 ▾ Page: 1 ▾ | **Refresh** |

Index	IP Address	TX rate(Kbps)	RX rate(Kbps) ▾	Sessions	Action	APP QoS

		Current / Peak / Speed	Current / Peak / Speed	Current / Peak
WAN1	---	0 / 0 / 0	0 / 0 / 0	0
Total		0 / 0 / 0	0 / 0 / 0	0 / 59
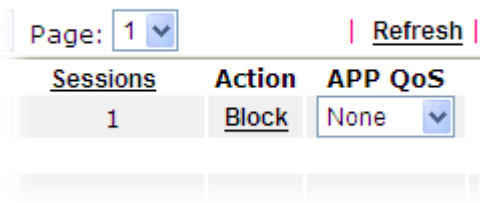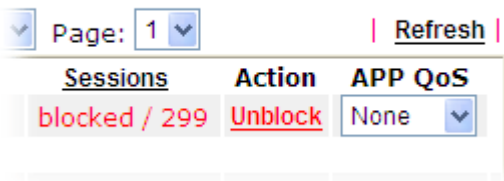
Note: 1. Click "Block" to prevent specified PC from surfing Internet for 5 minutes.
2. The IP blocked by the router will be shown in red, and the session column will display the remaining time that the specified IP will be blocked.
3. (Kbps): shared bandwidth
  + : residual bandwidth used

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.

DrayTek

	Refresh Seconds: 10 ☑
	10
	15
	30
Refresh	Click this link to refresh this page manually.
Index	Display the number of the data flow.
IP Address	Display the IP address of the monitored device.
TX rate (kbps)	Display the transmission speed of the monitored device.
RX rate (kbps)	Display the receiving speed of the monitored device.
Sessions	Display the session number that you specified in Limit Session web page.
Action	**Block** - can prevent specified PC accessing into Internet within 5 minutes.
	Page: 1 ☑ | Refresh |
	Sessions **Action** **APP QoS**
	1 Block None ☑
	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.
	Page: 1 ☑ | Refresh |
	Sessions **Action** **APP QoS**
	blocked / 299 Unblock None ☑
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.

4.15.9 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to open the web page. Choose WAN1 Bandwidth, Backup WAN 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.
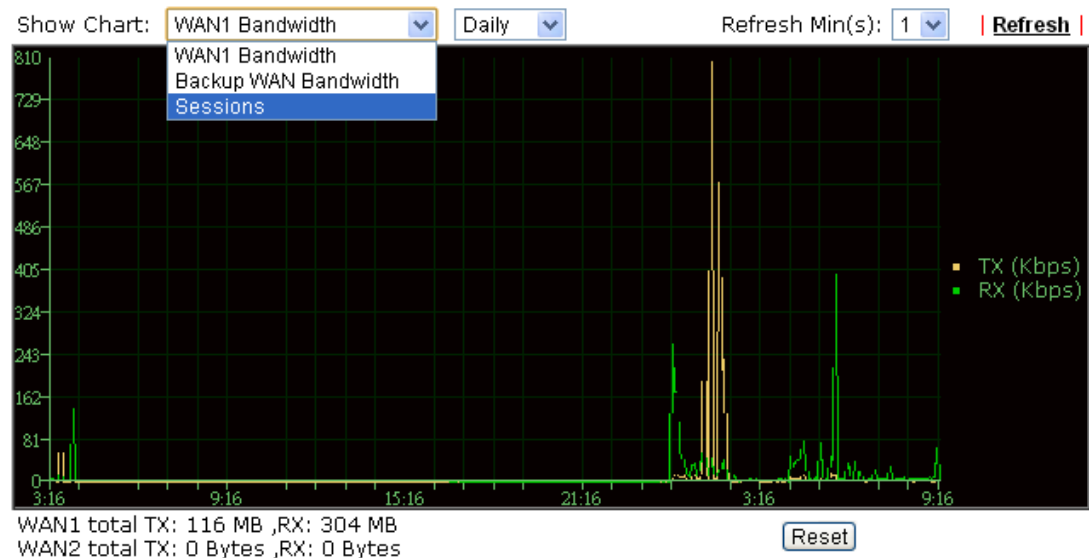
The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1 Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

For Sessions chart, the numbers displayed on vertical axis represent the numbers of the NAT sessions during the past.

4.15.10 Trace Route

Click **Diagnostics** and click **Trace Route** to open the web page. This page allows you to trace the routes from router to the host. Simply type the IP address of the host in the box and click **Run**. The result of route trace will be shown on the screen.

```
Diagnostics >> Trace Route
_____

Trace Route
 ┌─────────────────────────────────────────────────────────────┐
 │        ⊙ IPV4   ○ IPV6                                        │
 │        Protocol:        [ICMP ▼]                             │
 │        Host / IP Address: [_____]                │
 │                      [  Run  ]                               │
 │        Result                              | Clear |         │
 │        ┌──────────────────────────────────────────┐         │
 │        │                                          │         │
 │        │                                          │         │
 │        │                                          │         │
 │        │                                          │         │
 │        │                                          │         │
 │        │                                          │         │
 │        └──────────────────────────────────────────┘         │
 └─────────────────────────────────────────────────────────────┘
```

And,

```
Diagnostics >> Trace Route
_____

Trace Route
 ┌─────────────────────────────────────────────────────────────┐
 │        ○ IPV4   ⊙ IPV6                                        │
 │        Trace Host / IP Address: [_____]   │
 │                      [  Run  ]                               │
 │        Result                              | Clear |         │
 │        ┌──────────────────────────────────────────┐         │
 │        │                                          │         │
 │        │                                          │         │
 │        │                                          │         │
 │        │                                          │         │
 │        │                                          │         │
 │        │                                          │         │
 │        └──────────────────────────────────────────┘         │
 └─────────────────────────────────────────────────────────────┘
```

Available settings are explained as follows:

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

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

4.15.11 System Explorer
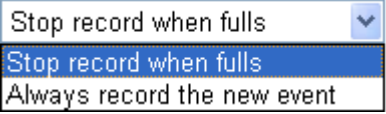
Such page provides real-time syslog and displays the information on the screen.

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.

Available settings are explained as follows:

Item	Description
Enable Web Syslog	Check this box to enable the function of Web Syslog.
Syslog Type	Use the drop down list to specify a type of Syslog to be displayed.
Export	Click this link to save the data as a file.
Refresh	Click this link to refresh this page manually.
Clear	Click this link to clear information on this page.
Display Mode	There are two modes for you to choose. **Stop record when fulls –** when the capacity of syslog is full, the system will stop recording. **Always record the new event –** only the newest events

	will be recorded by the system.
Time	Display the time of the event occurred.
Message	Display the information for each event.

For USB Syslog

This page displays the syslog recorded on the USB storage disk.

Available settings are explained as follows:

Item	Description
Time	Display the time of the event occurred.
Log Type	Display the type of the record.
Message	Display the information for each event.

4.15.12 IPv6 TSPC Status

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

Diagnostics >> IPv6 TSPC Status

WAN1	WAN2		Refresh	

TSPC Disabled

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

```
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.

5 Trouble Shooting

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 for advanced help.

5.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

1. Check the power line and WLAN/LAN cable connections.
   Refer to "**1.3 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.
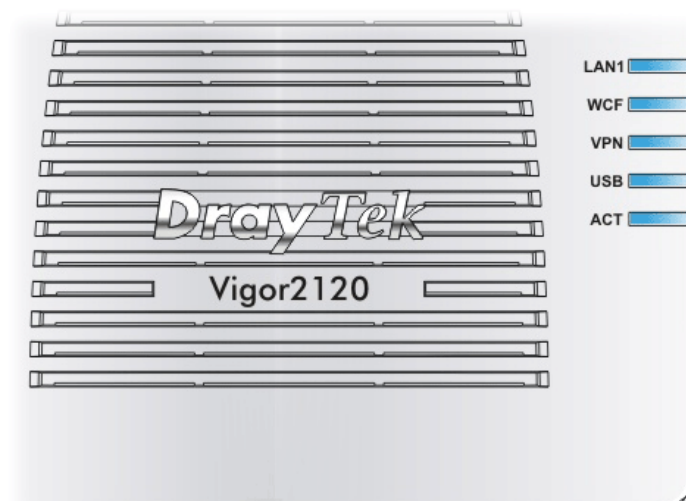
3. If not, it means that there is something wrong with the hardware status. Simply back to **"1.3 Hardware Installation"** to execute the hardware installation again. And then, try again.

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

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

For Windows

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

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

2. In the following window, click **Change adapter settings**.
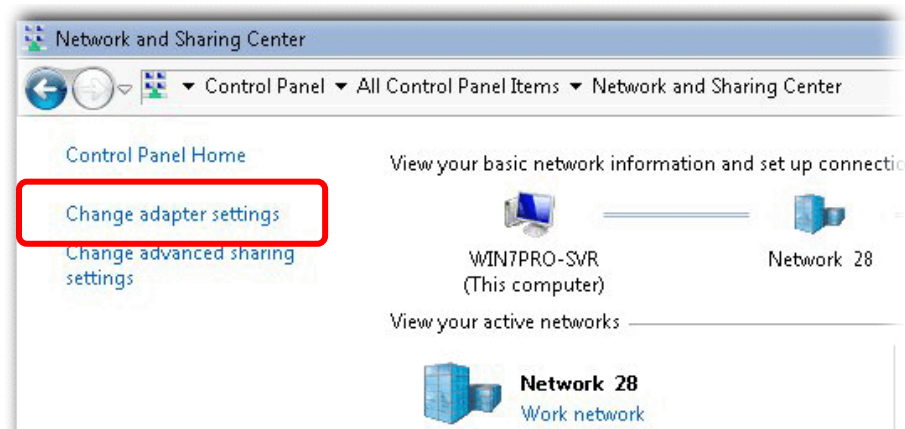
3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.

DrayTek
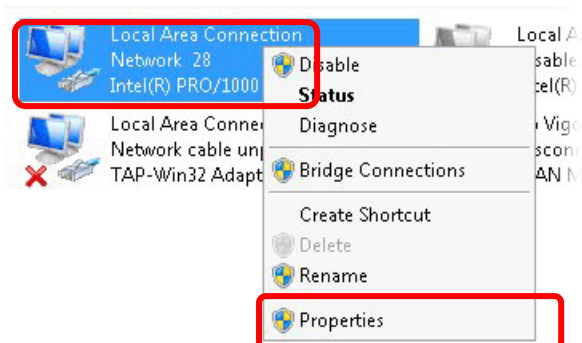
4. Select **Internet Protocol Version 4 (TCP/IP)** and then click **Properties**.
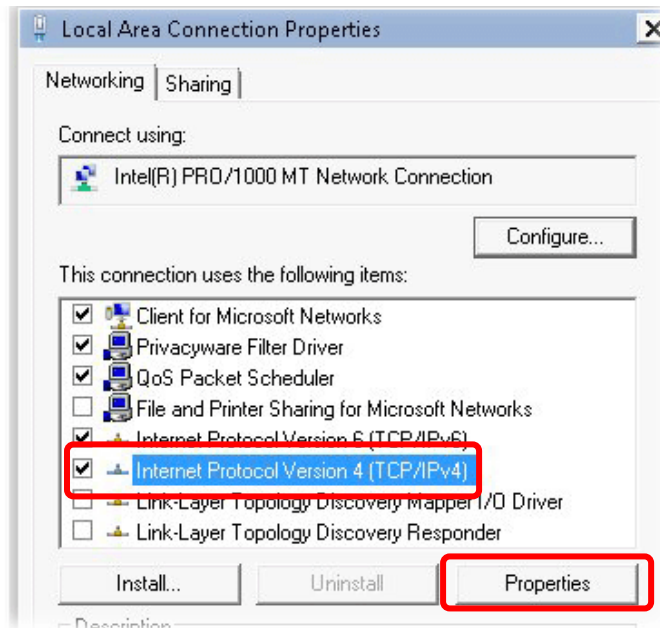
5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.
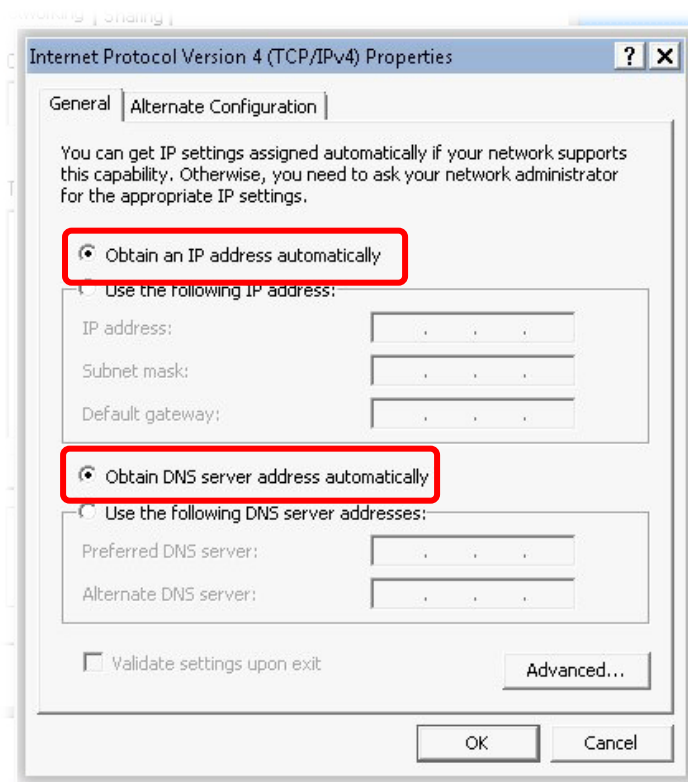
For Mac OS

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.
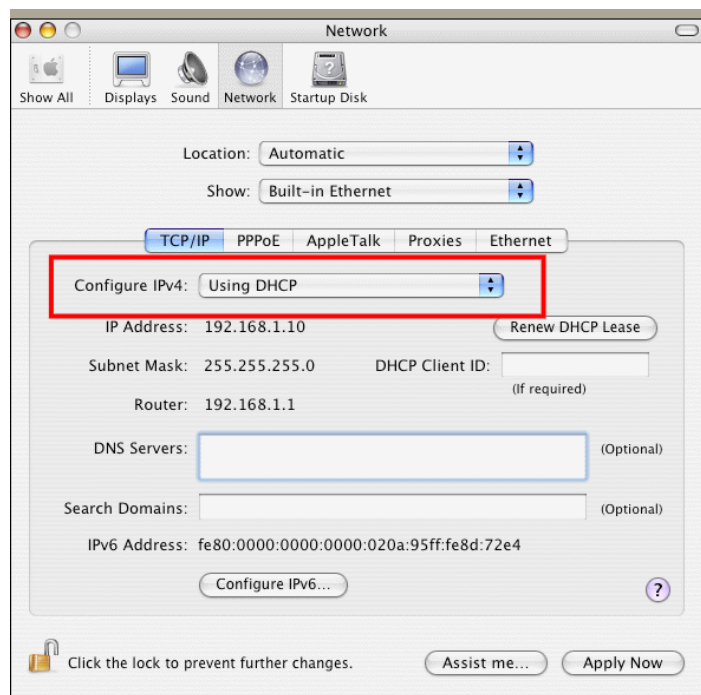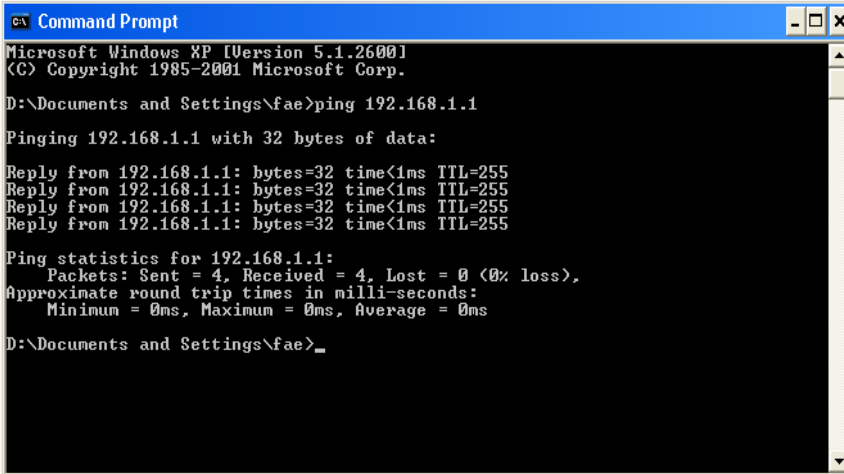
5.3 Pinging the Router from Your Computer

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 5.2)

Please follow the steps below to ping the router correctly.

For Windows

1. Open the **Command** Prompt window (from **Start menu> Run**).

2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista/7). The DOS command dialog will appear.

```
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 Mac Os on the desktop.

2. Open the **Application** folder and get into **Utilities**.

3. Double click **Terminal**. The Terminal window will appear.

4. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of **"64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms"** will appear.

5.4 Checking If the ISP Settings are OK or Not

If WAN connection cannot be up, check if the LEDs (according to the LED explanations listed on section 1.2) are correct or not. If the LEDs are off, please:

● Change the **Physical Type** from **Auto negotiation** to other values (e.g., 100M full duplex).

● Next, 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-WAN2 to review the settings that you configured previously.

5.5 Problems for 3G Network Connection

When you have trouble in using 3G/4G network transmission, please check the following:

Check if USB LED lights on or off

You have to wait about 15 seconds after inserting 3G/4G USB Modem into your Vigor2120. Later, the USB LED will light on which means the installation of USB Modem is successful.

If the USB LED does not light on, please remove and reinsert the modem again. If it still fails, restart Vigor2120.

USB LED lights on but the network connection does not work

Check the PIN Code of SIM card is disabled or not. Please use the utility of 3G/4G USB Modem to disable PIN code and try again. If it still fails, it might be the compliance problem of system. Please open DrayTek Syslog Tool to capture the connection information (WAN Log) and send the page (similar to the following graphic) to the service center of DrayTek.

Transmission Rate is not fast enough

Please connect your Notebook with 3G/4G USB Modem to test the connection speed to verify if the problem is caused by Vigor2120. In addition, please refer to the manual of 3G/4G USB Modem for LED Status to make sure if the modem connects to Internet via HSDPA mode. If you want to use the modem indoors, please put it on the place near the window to obtain better signal receiving.

5.6 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.

> **Warning:** After pressing **factory default setting**, you will loose all settings you did before. Make sure you have recorded all useful settings before you pressing.

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.

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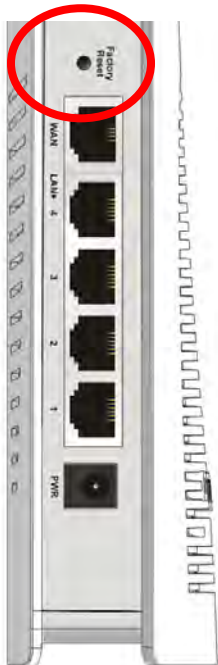
After restore the factory default setting, you can configure the settings for the router again to fit your personal request.

5.7 Contacting DrayTek

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

This page is left blank.

Dray Tek

Telnet Command Reference

Accessing Telnet of Vigor2120

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

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

Type **cmd** and press Enter. The Telnet terminal will be open later.
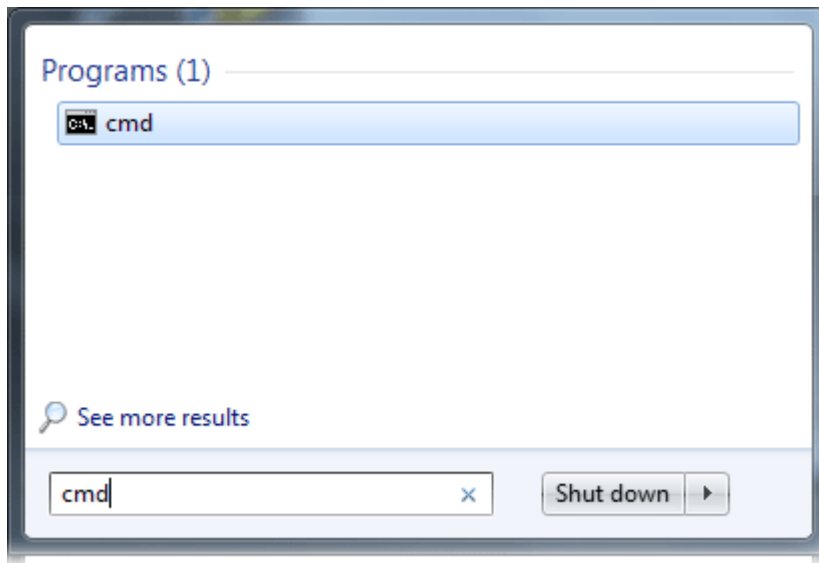
In the following window, type **Telnet 192.168.1.1** as below and press Enter. Note that the IP address in the example is the default address of the router. If you have changed the default, enter the current IP address of the router.
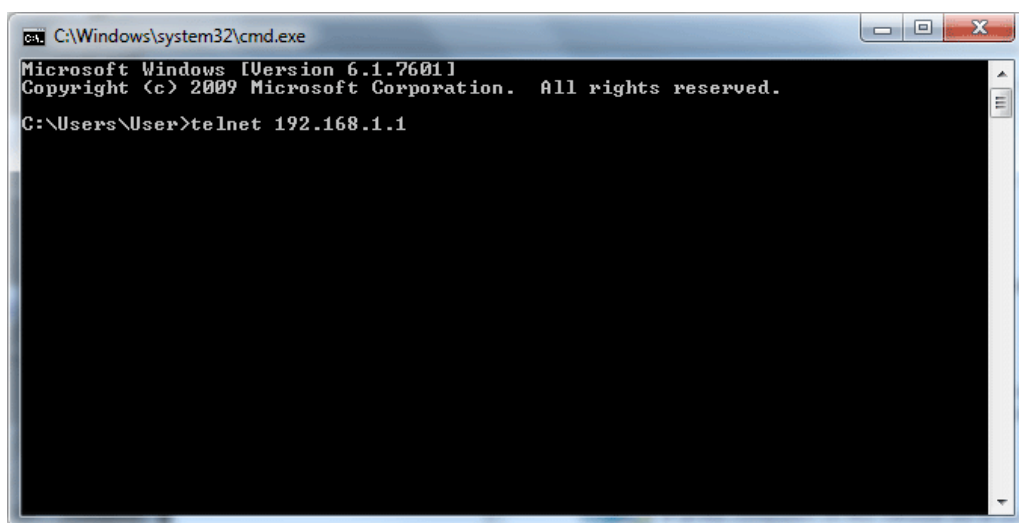
Next, type admin/admin for Account/Password. Then, type **?**. You will see a list of valid/common commands depending on the router that your use.
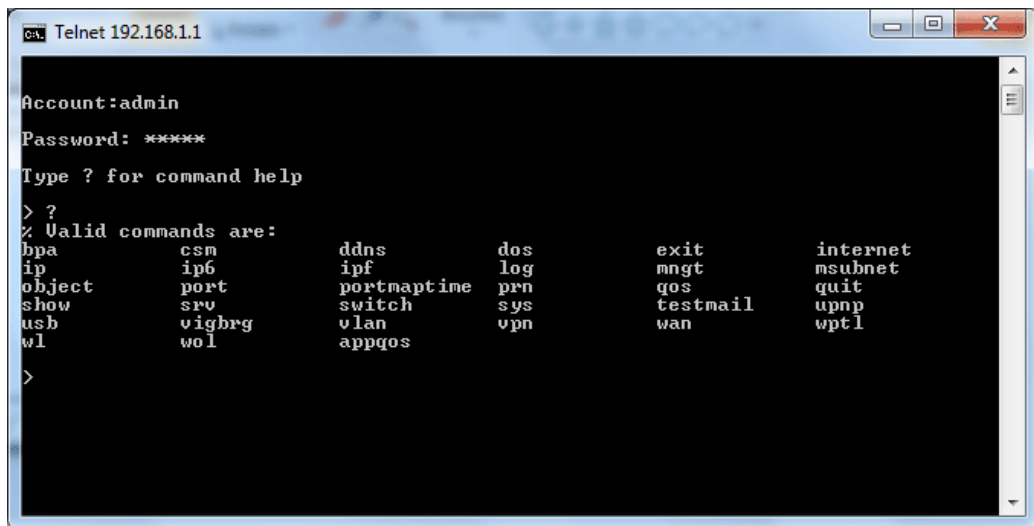
For users using previous Windows system (e.g., 2000/XP), simply click **Start >> Run** and type **Telnet 192.168.1.1** in the Open box as below. Next, type admin/admin for Account/Password. And, type **?** to get a list of valid/common commands
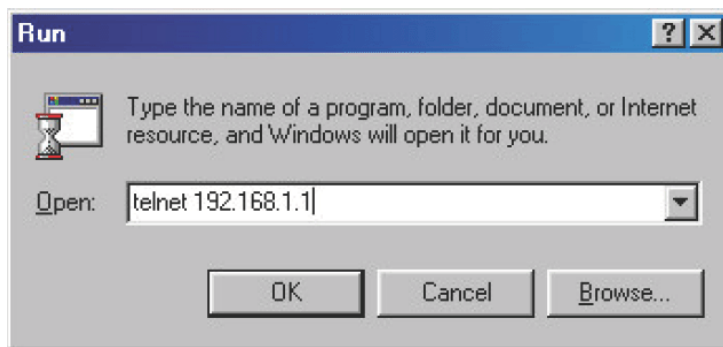
Telnet Command: bpa

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

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

Syntax Description

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

-l <List>	List all settings configured.

Example

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

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

>
```

Telnet Command: csm appe prof

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

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

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

Syntax Description

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

Example

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

Telnet Command: csm appe set

It is used to block or pass settings for APP Enforcement Profile.

csm appe set -i *INDEX [-v GROUP | -e AP_IDX | -d AP_IDX | -a AP_IDX [ACTION]]*

Syntax Description

Parameter	Description
INDEX	It means to specify the index number of CSM profile, from 1 to 32.
GROUP	It means the types to be specified for the APP Enforcement profile. Available types include:

	IM, P2P, Protocol and MISC,
AP_IDX	It means to specify the index of the APP Enforcement profile.
- v	It means to view the configuration (IM/P2P/Protocol/MISC) of the profile.
-e	It means to enable blocking for a specific application.
-d	It means to disable blocking for a specific application.
-a	It means to set the action for specific application

Example

```
> csm appe set -i 1 -e 1
Profile 1 - games: AliWW is enabled.
```

Telnet Command: csm appe show

It is used to show configuration for all groups of APP Enforcement profiles.

csm appe show *[-a/-i/-p/-t/-m]*

Syntax Description

Parameter	Description
a	It means to show configuration for All groups.
-i	It means to show configuration for IM group.
-p	It means to show configuration for P2P group.
-t	It means to show configuration for PROTOCOL group.
-m	It means to show configuration for MISC group.

Example

```
> csm appe show -m

  Group          Type    Index              Name          Advance
 Advanced Option: (M)essage, (F)ile Transfer, (G)ame, (C)onference, and
(O)ther
Activities
------------------------------------------------------------------
   OTHERS        TUNNEL     69              DynaPass
   OTHERS        TUNNEL     70               FreeU
   OTHERS        TUNNEL     71             HTTP Proxy
   OTHERS        TUNNEL     72             HTTP Tunnel
   OTHERS        TUNNEL     73              Hamachi
   OTHERS        TUNNEL     74           Hotspot Shield
   OTHERS        TUNNEL     75             MS Teredo
   OTHERS        TUNNEL     76              PGPNet
   OTHERS        TUNNEL     77             Ping Tunnel
   OTHERS        TUNNEL     78             RealTunnel
   OTHERS        TUNNEL     79              Skyfire
   OTHERS        TUNNEL     80             Socks 4/5
.
```

DrayTek

```
    .
```

Telnet Command: csm appe config

It is used to show configuration of **specified** APP Enforcement profile.

csm appe config *-v INDEX [-i|-p|-t|-m]*

Syntax Description

Parameter	Description
- v	It means to view the configuration of the profile.
INDEX	It means to specify the index number of profile, from 1 to 32.
-i	It means to show IM group setting configuration for the specified profile.
-p	It means to show P2P group setting configuration for the specified profile
-t	It means to show PROTOCOL group setting configuration for the specified profile.
-m	It means to show MISC group setting configuration for the specified profile.
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 config -v 1 -i


    Group          Type     Index        Name        Enable   Advance
Enable
 Advance abbreviation: Message, File Transfer, Game, Conference, and
Other
 Advance abbreviation: : M, F, G, C, and O

------------------------------------------------------------------
     IM          IM        0           AIM           Disable
     IM          IM        1          AliWW           Enable
     IM          IM        2           Ares          Disable
     IM          IM        3          BaiduHi        Disable
     IM          IM        4          Fetion         Disable
     IM          IM        5 GaduGadu Protocol        Disable
     IM          IM        6       Google Chat       Disable
     IM          IM        7          ICQ            Disable
     IM          IM        8          ICU2           Disable
     IM          IM        9  Jabber Protocol/Goog    Disable
     IM          IM        10          KC            Disable
     IM          IM        11          LINE          Disable
```

Telnet Command: csm ucf

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

csm ucf show

csm ucf cache

csm ucf setdefault

csm ucf msg *MSG*

csm ucf obj *INDEX [-n PROFILE_NAME | -l [P|B|A|N] | uac | wf]*

csm ucf obj *INDEX -n PROFILE_NAME*

csm ucf obj *INDEX -p VALUE*

csm ucf obj *INDEX -l P|B|A|N*

csm ucf obj *INDEX uac*

csm ucf obj *INDEX wf*

Syntax Description

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

Dray Tek

Example

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

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


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

Telnet Command: csm ucf obj INDEX uac

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

csm ucf obj *INDEX uac -v*

csm ucf obj *INDEX uac -e*

csm ucf obj *INDEX uac -d*

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

csm ucf obj *INDEX uac -i E/D*

csm ucf obj *INDEX uac -o KEY_WORD_Object_Index*

csm ucf obj *INDEX uac -g KEY_WORD_Group_Index*

Syntax Description

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

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

Example

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

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


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


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

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


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

Dray Tek

Telnet Command: csm ucf obj INDEX wf

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

csm ucf obj *INDEX wf -v*

csm ucf obj *INDEX wf -e*

csm ucf obj *INDEX wf -d*

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

csm ucf obj *INDEX wf -s WEB_FEATURE*

csm ucf obj *INDEX wf -u WEB_FEATURE*

csm ucf obj *INDEX wf -f File_Extension_Object_index*

Syntax Description

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

Example

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

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

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


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

Telnet Command: csm wcf

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

csm wcf show

csm wcf look

csm wcf cache

csm wcf server WCF_SERVER

csm wcf msg MSG

csm wcf setdefault

csm wcf obj *INDEX -v*

csm wcf obj *INDEX -a P|B*

csm wcf obj *INDEX -n PROFILE_NAME*

csm wcf obj *INDEX -l N|P|B|A*

csm wcf obj *INDEX -o KEY_WORD Object Index*

csm wcf obj *INDEX -g KEY_WORD Group Index*

csm wcf obj *INDEX -w E|D|P|B*

csm wcf obj *INDEX -s CATEGORY|WEB_GROUP*

csm wcf obj *INDEX -u CATEGORY|WEB_GROUP*

Syntax Description

Parameter	Description
show	It means to display the web content filter profiles.
Look	It means to display the license information of WCF.
Cache	It means to set the cache level for the profile.
Server WCF_SERVER	It means to set web content filter server.
Msg MSG	It means de set the administration message.
	MSG means the content (less than 255 characters) of the message itself.
setdefault	It means to return to default settings for all of the profile.
obj	It means to specify the object profile.
INDEX	It means to specify the index number of web content filter

Dray Tek

	profile, from 1 to 8.
- v	It means to view the web content filter profile.
-a	Set the action of web content filter profile, P or B.
	B: Block. The web access meets the web feature will be blocked.
	P: Pass. The web access meets the web feature will be passed.
-n	It means to set the profile name.
PROFILE_NAME	It means to specify the name of the profile (less than 16 characters)
-l	It means the log type of the profile. They are:
	P: Pass,
	B: Block,
	A: All,
	N: None
-o	Set the keyword object.
KEY_WORD_Object_Index	Specify the index number of the object profile.
-g	Set the keyword group.
KEY_WORD_Group_Index	Specify the index number of the group profile.
-w	It means to set the action for the black and white list.
	E:Enable,
	D:Disable,
	P:Pass,
	B:Block
-s	It means to choose the items under CATEGORY or WEB_GROUP.
-u	It means to discard items under CATEGORY or WEB_GROUP.
WEB_GROUP	Child_Protection, Leisure, Business, Chating, Computer Internet, Other
CATEGORY	Includes:
	Alcohol & Tobacco, Criminal Activity, Gambling, Hate & Intoleranc, Illegal Drug, Nudity, Pornography/Sexually Explicit, Weapons, Violence, School Cheating,Sex Education, Tasteless, Child Abuse Imges, Entertainment, Games, Sports, Travel, Leisure & Recreation, Fashin & Beauty, Business, Job Search, Web-based Emai, Chat, Instant Messaging, Anonymizers, Forums & Newsgroups, Computers & Technology, Download Sites, Streaming Media & Downloads, Phishing & Fraud, Search Engines & Portals, Social Networking, Spam Sites,Malware, Botnets, Hacking, Illegal Software, Information Security,Peer-to-eer, Advertisements & Pop-Ups, Arts, Transportation, Compromised, Dating & Personals, , Education, Finance, Government,Health & Medcine, News, Non-profits & NGOs, Personal Sites,Politics, Real Estate, Rligion, Restaurants &

	Dining,Shopping, Translators, General, Cults,Greetig cards, Image Sharing, Network Errors, Parked Domains, Private IP Addresses)

Example

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

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

Telnet Command: csm dnsf

It means to configure the settings regarding to DNS filter.

csm dnsf enable *ON/OFF*

csm dnsf syslog *N/P/B/A*

csm dnsf service WCF_PROFILE

csm dnsf time CACHE_TIME

csm dnsf blockpage *show/on/off*

Syntax Description

Parameter	Description
enable	It means to enable or disable DNS Filter. ON: enable. OFF: disable.
syslog	It means to 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

Dray Tek

	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.

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 log

Displays the DDNS log.

Example

```
>ddns log
>
```

Telnet Command: ddns time

Sets and displays the DDNS time.

ddns time *<update in minutes>*

Syntax Description

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

Example

```
> ddns time
```

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

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

Telnet Command: dos

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

dos *[-V | D | A]*

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

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

Syntax Description

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

Example

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

Telnet Command: exit

Type this command will leave telnet window.

Telnet Command: Internet

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

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

Syntax Description

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

-s <server ip>	It means to set PPTP/L2TP server IP.
-V	It means to view Internet Access profile.

Example

```
>internet -M 1 -S tcom -u username -p password -a 0 -t -1  -i 0.0.0.0
 WAN1 Internet Mode set to PPPoE/PPPoA
 WAN1 ISP Name set to tcom
 WAN1 Username set to username
 WAN1 Password set successful
 WAN1 PPP Authentication Type set to PAP/CHAP
 WAN1 Idle timeout set to always-on
 WAN1 Gateway IP set to 0.0.0.0
> internet -V
WAN1 Internet Mode:PPPoE
ISP Name: tcom
Username: username
Authentication: PAP/CHAP
Idle Timeout: -1
WAN IP: Dynamic IP
> internet -M 1 -u link1 -p link1 -a 0
 WAN1 Internet Mode set to PPPoE/PPPoA
 WAN1 Username set to link1
 WAN1 Password set successful
 WAN1 PPP Authentication Type set to PAP/CHAP
```

Telnet Command: ip pubsubnet

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

ip pubsubnet *<Enable/Disable>*

Syntax Description

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

Example

```
> ip pubsubnet disable
public subnet disabled!
```

Telnet Command: ip pubaddr

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

ip pubaddr *?*

ip pubaddr *<public subnet IP address>*

Syntax Description

Dray Tek

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 public IP address for your router.

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 aux

This command is used for configuring WAN IP Alias.

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

ip aux remove *[index]*

Syntax Description

Parameter	Description
add	It means to create a new WAN IP address.
remove	It means to delete an existed WAN IP address.

Dray Tek

IP	It means the auxiliary WAN IP address.
Join to NAT Pool	0 (disable) or 1 (enable).
index	Type the index number of the table displayed on your screen.

Example

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

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

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

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

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

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

Telnet Command: ip addr

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

ip addr *[IP address]*

Syntax Description

Parameter	Description
IP address	It means the LAN IP address.

Example

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

Note: When the LAN IP address is changed, the start IP address of DHCP server are still the same. To make the IP assignment of the DHCP server being consistent with this new IP address (they should be in the same network segment), the IP address of the PC must be fixed with the same LAN IP address (network segment) set by this command for accessing into the web user interface of the router. Later, modify the start addresses for the DHCP server.

Telnet Command: ip nmask

This command allows users to set/add a specified netmask for your router.

ip nmask *[IP netmask]*

Syntax Description

Parameter	Description
IP netmask	It means the netmask of LAN IP.

Example

```
> ip nmask 255.255.0.0
% Set IP netmask OK !!!
```

Telnet Command: ip arp

ARP displays the matching condition for IP and MAC address.

ip arp add *[IP address] [MAC address] [LAN or WAN]*

ip arp del *[IP address] [LAN or WAN]*

ip arp flush

ip arp status

ip arp accept *[0/1/2/3/4/5status]*

ip arp setCacheLife *[time]*

In which, **arp add** allows users to add a new IP address into the ARP table; **arp del** allows users to remove an IP address; **arp flush** allows users to clear arp cache; **arp status** allows users to review current status for the arp table; **arp accept** allows to accept or reject the source /destination MAC address; arp **setCacheLife** allows users to configure the duration in which ARP caches can be stored on the system. If **ip arp setCacheLife** is set with "60", it means you have an ARP cache at 0 second. Sixty seconds later without any ARP messages received, the system will think such ARP cache is expired. The system will issue a few ARP request to see if this cache is still valid.

Syntax Description

Parameter	Description
IP address	It means the LAN IP address.
MAC address	It means the MAC address of your router.
LAN or WAN	It indicates the direction for the arp function.
0/1/2/3/4/5	0: disable to accept illegal source mac address
	1: enable to accept illegal source mac address
	2: disable to accept illegal dest mac address
	3: enable to accept illegal dest mac address
	4: Decline VRRP mac into arp table
	5: Accept VRRP mac into arp table
	status: display the setting status.
Time	Available settings will be 10, 20, 30,....2550 seconds.

Example

```
> ip arp accept status
Accept illegal source mac arp: disable

Accept illegal dest mac arp: disable

Accept VRRP mac into arp table: disable
> ip arp status
[ARP Table]
 Index IP Address       MAC Address       Netbios Name
   1   192.168.1.113     00-05-5D-E4-D8-EE   A1000351
```

Telnet Command: ip dhcpc

This command is available for WAN DHCP.

ip dhcpc *option*

ip dhcpc *option -h/l*

ip dhcpc *option -d [idx]*

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

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

ip dhcpc *option -u [idx unmber]*

ip dhcpc *release*

ip dhcpc *renew*

ip dhcpc *status*

Syntax Description

Parameter	Description
option	It is an optional setting for DHCP server. -h: display usage -l: list all custom set DHCP options -d: delete custom dhcp client option by index number -e: enable/disable option feature, 1:enable, 0:disable -w: set WAN number (e.g., 1=WAN1) -c: set option number: 0~255 -v: set option value by string -x: set option value by raw byte (hex) -u: update by index number
release	It means to release current WAN IP address.
renew	It means to renew the WAN IP address and obtain another new one.
status	It displays current status of DHCP client.

Example

```
>ip dhcpc status
I/F#3 DHCP Client Status:

DHCP Server IP      : 172.16.3.7
WAN Ipm             : 172.16.3.40
WAN Netmask         : 255.255.255.0
WAN Gateway         : 172.16.3.1
Primary DNS         : 168.95.192.1
Secondary DNS       : 0.0.0.0
Leased Time         : 259200
Leased Time T1      : 129600
Leased Time T2      : 226800
Leased Elapsed      : 259194
Leased Elapsed T1   : 129594
Leased Elapsed T2   : 226794
```

Telnet Command: ip ping

This command allows users to ping IP address of WAN1/WAN2/PVC3/PVC4/PVC5 for verifying if the WAN connection is OK or not.

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

Syntax Description

Parameter	Description
IP address	It means the WAN IP address.
WAN1/PVC3/PVC4/PVC5	It means the WAN port /PVC that the above IP address passes through.

Example

```
>ip ping 172.16.3.229 WAN1
Pinging 172.16.3.229 with 64 bytes of Data:
Receive reply from 172.16.3.229, time=0ms
Receive reply from 172.16.3.229, time=0ms
Receive reply from 172.16.3.229, time=0ms
Packets: Sent = 5, Received = 5, Lost = 0 <0% loss>
```

Telnet Command: ip tracert

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

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

Syntax Description

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

Example

```
>ip tracert 22.128.2.62 WAN1
Traceroute to 22.128.2.62, 30 hops max
1   172.16.3.7   10ms
2   172.16.1.2   10ms
3   Request Time out.
4   168.95.90.66    50ms
5   211.22.38.134   50ms
6   220.128.2.62    50ms
Trace complete
```

Telnet Command: ip telnet

This command allows users to access specified device by telnet.

ip telnet *[IP address][Port]*

Syntax Description

Parameter	Description
IP address	Type the WAN or LAN IP address of the remote device.
Port	Type a port number (e.g., 23). Available settings: 0 ~65535.

Example

```
> ip telnet 172.17.3.252 23
>
```

Telnet Command: ip rip

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

ip rip *[0/1/2]*

Syntax Description

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

Example

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

Dray Tek

Telnet Command: ip wanrip

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

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

Syntax Description

Parameter	Description
ifno	It means the connection interface.
	1: WAN1,2: WAN2, 3: PVC3,4: PVC4,5: PVC5
	Note: PVC3 ~PVC5 are virtual WANs.
-e	It means to disable or enable RIP setting for specified WAN interface.
	1: Enable the function of setting RIP of WAN IP.
	0: Disable the function.

Example

```
> ip wanrip ?
 Valid ex:ip wanrip <ifno> -e <0/1>
 <ifno> 1: WAN1,2: WAN2
        3: PVC3,4: PVC4,5: PVC5
 -e <0/1>  0: disable, 1: enable
 Now status:
 WAN[1] Rip Protocol disable
 WAN[2] Rip Protocol disable
 WAN[3] Rip Protocol disable
 WAN[4] Rip Protocol disable
 WAN[5] Rip Protocol disable
> ip wanrip 5 -e 1
> ip wanrip ?
 Valid ex:ip wanrip <ifno> -e <0/1>
 <ifno> 1: WAN1,2: WAN2
        3: PVC3,4: PVC4,5: PVC5
 -e <0/1>  0: disable, 1: enable
 Now status:
 WAN[1] Rip Protocol disable
 WAN[2] Rip Protocol disable
 WAN[3] Rip Protocol disable
 WAN[4] Rip Protocol disable
 WAN[5] Rip Protocol enable
>
```

Telnet Command: ip route

This command allows users to set static route.

ip route *add [dst] [netmask][gateway][ifno][rtype]*

ip route *del [dst] [netmask][rtype]*

ip route *status*

ip route *cnc*

ip route *default [wan1/wan2/off/?]*

ip route *clean [1/0]*

Syntax Description

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

Example

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

Codes: C - connected, S - static, R - RIP, * - default, ~ - private
C~      192.168.1.0/  255.255.255.0 is directly connected, LAN1
S       172.16.2.0/  255.255.255.0 via 172.16.2.4, WAN1
```

Dray Tek

Telnet Command: ip igmp_proxy

This command allows users to enable/disable igmp proxy server.

ip igmp_proxy *set*

ip igmp_proxy *reset*

ip igmp_proxy *wan*

ip igmp_proxy *t_home[on/off/show/help]*

ip igmp_proxy *query*

ip igmp_proxy *ppp [0/1]*

ip igmp_proxy *status*

Syntax Description

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

Example

```
> ip igmp t_home on
%T-Home Setting:
%T-Home Service is turned on.
%WAN1 : Enabled, connection type: PPPoE, without tag for ADSL
%WAN5 : Enabled, connection type: DHCP, tag: 8
%: PVC4(WAN5) is bound to PVC0(WAN1), protocol=MPoA 1483 Bridge
%IGMP Proxy Interface: WAN5(PVC)
%WAN5 for Router-borne Application/ IPTV on/off: ON
> ip igmp_proxy query 130000
 This command is for setting IGMP General Query Interval
 The default value is 125000 ms
 Current Setting is:130000 ms
>
```

Telnet Command: ip igmp_snoop

This command allows users to enable or disable IGMP snoop function.

ip igmp_snoop enable

ip igmp_snoop disable

ip igmp_snoop status

ip igmp_snoop table

ip igmp_snoop txquery

ip igmp_snoop mode

ip igmp_snoop chkleave

ip igmp_snoop separate

ip igmp_snoop portchk

Syntax Description

Parameter	Description
enable	It means to enable igmp snoop function
disable	It means to disable igmp snoop function.
status	It means to display current igmp configuration.
table	It means to display current configuration of igmp.
txquery	It means to send out IGMP QUERY to LAN periodically.
mode	It means to set software or hardware mode for snooping working on.
chkleave	It means to check the leave status. On: enable the IGMP snoop leave checking function. Off: it will drop LEAVE if still clients on the same group.
separate	It means to set IGMP packets being separated by NAT/Bridge. On: The packets will be separated. Off: The packets will not be separated by NAT/Bridge.
portchk	It means to perform LAN port checking for IGMP packets. On: Perform the LAN port checking. Off: No perform the LAN port checking.

Example

```
> ip igmp_snoop enable
%% ip igmp snooping [enable|disable|status], IGMP Snooping is Enabled.
> ip igmp_snoop disable
%% ip igmp snooping [enable|disable|status], IGMP Snooping is Disabled.
> ip igmp_snoop mode hw
 igmp snooping works on SW mode now.
> ip igmp_snoop mode ?
% ip igmp mode [hw/sw]
 igmp snooping works on HW mode now.
> ip igmp_snoop separate ?
% ip igmp separate [on/off]
 igmp snoop seprate is ON now.
 igmp packets will be separated by  NAT/Bridge.
```

Telnet Command: ip wanaddr

This command is used to configure WAN IP address.

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

Syntax Description

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

Example

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

Telnet Command: ip wanttr

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

ip wanttr *[time in seconds]*

Syntax Description

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

Example

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

Telnet Command: ip dmz

Specify MAC address of certain device as the DMZ host.

ip dmz *[mac]*

Syntax Description

Parameter	Description
mac	It means the MAC address of the device that you want to specify

Example

```
>ip dmz ?
% ip dmz <mac>,  now : 00-00-00-00-00-00
> ip dmz 11-22-33-44-55-66
> ip dmz ?
% ip dmz <mac>,  now : 11-22-33-44-55-66
>
```

Telnet Command: ip dmzswitch

This command allows users to set DMZ mode.

ip dmzswitch *off*

ip dmzswitch *private*

ip dmzswitch *trueip (請問這邊所說的 trueip 跟下方所說的 active_trueip 的差異是??)*

ip dmzswitch *active_trueip*

Syntax Description

Parameter	Description
off	It means to turn off DMZ function.
private	It means to set DMZ with private IP.
trueip	It means to set DMZ with true IP.
active_trueip	It means to set the DMZ with active true IP.

Example

```
> ip dmzswitch off
>
```

Telnet Command: ip session

This command allows users to set maximum session limit number for the specified IP; set message for exceeding session limit and set how many seconds the IP session block works.

ip session *on*

ip session *off*

ip session *default [num]*

ip session *defaultp2p [num]*

ip session *status*

ip session *show*

ip session *timer [num]*

ip session *[block/unblock][IP]*

ip session *[add/del][IP1-IP2][num][p2pnum]*

Syntax Description

Parameter	Description
on	It means to turn on session limit for each IP.
off	It means to turn off session limit for each IP.
default [num]	It means to set the default number of session num limit.
Defautlp2p [num]	It means to set the default number of session num limit for p2p.

Dray Tek

status	It means to display the current settings.
show	It means to display all session limit settings in the IP range.
timer [num]	It means to set when the IP session block works. The unit is second.
[block/unblock][IP]	It means to block/unblock the specified IP address. Block: The IP cannot access Internet through the router. Unblock: The specified IP can access Internet through the router.
add	It means to add the session limits in an IP range.
del	It means to delete the session limits in an IP range.
IP1-IP2	It means the range of IP address specified for this command.
num	It means the number of the session limits, e.g., 100.
p2pnum	It means the number of the session limits, e.g., 50 for P2P.

Example

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

  IP range:
    192.168.1.5 - 192.168.1.100 : 100

  Current ip session limit is turn on

  Current default session number is 100
```

Telnet Command: ip bandwidth

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

ip bandwidth *on*

ip bandwidth *off*

ip bandwidth *default [tx_rate][rx_rate]*

ip bandwidth *status*

ip bandwidth *show*

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

Syntax Description

Parameter	Description
on	It means to turn on the IP bandwidth limit.
off	It means to turn off the IP bandwidth limit.
default [tx_rate][rx_rate]	It means to set default tx and rx rate of bandwidth limit. The

	range is from 0 – 65535 Kpbs.
status	It means to display the current settings.
show	It means to display all the bandwidth limits settings within the IP range.
add	It means to add the bandwidth within the IP range.
del	It means to delete the bandwidth within the IP range.
IP1-IP2	It means the range of IP address specified for this command.
tx	It means to set transmission rate for bandwidth limit.
rx	It means to set receiving rate for bandwidth limit.
shared	It means that the bandwidth will be shared for the IP range.

Example

```
> ip bandwidth default 200 800
> ip bandwidth add 192.168.1.50-192.168.1.100 10 60
> ip bandwidth status

  IP range:
    192.168.1.50 - 192.168.1.100 : Tx:10K Rx:60K

  Current ip Bandwidth limit is turn off


  Auto adjustment is off
```

Telnet Command: ip bindmac

This command allows users to set IP-MAC binding for LAN host.

ip bindmac *on*

ip bindmac *off*

ip bindmac *strict_on*

ip bindmac *show*

ip bindmac *add [IP][MAC][Comment]*

ip bindmac *del [IP]/all*

Syntax Description

Parameter	Description
on	It means to turn on IP bandmac policy. Even the IP is not in the policy table, it can still access into network.
off	It means to turn off all the bindmac policy.
strict_on	It means that only those IP address in IP bindmac policy table can access into network.

DrayTek

show	It means to display the IP address and MAC address of the pair of binded one.
add	It means to add one ip bindmac.
del	It means to delete one ip bindmac.
IP	It means to type the IP address for binding with specified MAC address.
MAC	It means to type the MAC address for binding with the IP address specified.
Comment	It means to type words as a brief description.
All	It means to delete all the IP bindmac settings.

Example

```
> ip bindmac add 192.168.1.46 00:50:7f:22:33:55 just for test
> ip bindmac show
ip bind mac function is turned ON
IP : 192.168.1.46 bind MAC : 00-50-7f-22-33-55 Comment : just
```

Telnet Command: ip maxnatuser

This command is used to set the maximum number of NAT users.

ip maxnatuser *user no*

Syntax Description

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

Example

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

Telnet Command: ip lanDNSRes

This command is used to set LAN DNS profiles. With such feature, the user can configure some services (such as ftp, www or database) with domain name which is easy to be accessed.

ip lanDNSRes *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
-a <IP Address>	It is used to configure IP address mapping (IPv4/IPv6 Address or multiple subnet addresses).
	IP Address: type the IP address (e.g., 192.168.1.56).
-d <address mapping index number>	It means to delete index number with address mapping configured.
	address mapping index number : type the index number which represents the address mapping profile.
-e <0/1>	It means to enable or disable the function of LAN DNS or DNS Forwarding Profile.
	0: disable
	1: enable
-i <profile setting index number>	It means to create LAN DNS profile with specified domain name.
	profile setting index number : type the index number which represents the profile with domain name configured.
-l	It means to list detailed information of profile configuration.
	> ip lanDNSRes -l
	%
	% Idx: 7
	% State: Enable
	% Profile: DrayTekFTP
	% Domain Name: ftp.draytek.com
	% -------- Address Mapping Table --------

Dray Tek

	% Idx ReplyOnlySameSubnet IP Address % 1　Yes　　　　172.16.2.10 % 2　Yes　　　　172.16.3.10 % 3　Yes　　　　172.16.4.10
-n\<domain name\>	It means to specify a domain name to be accessed.
-p\<profile name\>	It means to set name of the LAN DNS profile.
-r	It means to clear specified domain name profile and the address mapping setting.
-s\<0/1\>	It means to determine all subnet packets or only the packets with the same subnet will be replied for address mapping profile. *0:* reply all subnet packets. *1*: reply only same subnet packet.
-z	It means to update LAN DNS configuration to DNS cache.

Example

```
> ip lanDNSRes -i 1 -n ftp.drayTek.com
% Configure Set1's DomainName:ftp.drayTek.com
> ip lanDNSRes -i 1 -n ftp.drayTek.com
> ip lanDNSRes -i 1 -a 172.16.2.10 -s 1
> ip lanDNSRes -i 1 -a 172.16.3.10 -s 1
> ip lanDNSRes -i 1 -a 172.16.4.10 -s 1
> ip lanDNSRes -l
%
% Idx: 7
% State: Enable
% Profile: DrayTekFTP
% Domain Name: ftp.draytek.com
% -------- Address Mapping Table --------
% Idx ReplyOnlySameSubnet IP Address
% 1   Yes                 172.16.2.10
% 2   Yes                 172.16.3.10
% 3   Yes                 172.16.4.10
```

Telnet Command: ip6 addr

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

ip6 addr -s *[prefix] [prefix-length] [LAN|WAN1|WAN2|iface#]*

ip6 addr -d *[prefix] [prefix-length] [LAN|WAN1|WAN2|iface#]*

ip6 addr -a *[LAN|WAN1|WAN2|iface#]*

Syntax Description

Parameter	Description
-s	It means to add a static ipv6 address.

-d	It means to delete an ipv6 address.
-a	It means to show current address(es) status.
-u	It means to show only unicast addresses.
prefix	It means to type the prefix number of IPv6 address.
prefix-length	It means to type a fixed value as the length of the prefix.
LAN/*WAN1*/*WAN2*/*iface#*	It means to specify LAN or WAN interface for such address.

Example

```
> ip6 addr -a
LAN
Unicast Address:
 FE80::250:7FFF:FE00:0/64 (Link)
Multicast Address:
 FF02::2
 FF02::1:FF00:0
 FF02::1
```

Telnet Command: ip6 dhcp req_opt

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

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

Syntax Description

Parameter	Description
req_opt	It means option-request.
LAN/*WAN1*/*WAN2*/*iface#*	It means to specify LAN or WAN interface for such address.
[<command> <parameter>/...]	The available commands with parameters are listed below. *[...]* means that you can type in several commands in one line.
-a	It means to show current DHCPv6 status.
-s	It means to ask the SIP.
-S	It means to ask the SIP name.
-d	It means to ask the DNS setting.
-D	It means to ask the DNS name.
-n	It means to ask NTP.
-i	It means to ask NIS.
-I	It means to ask NIS name.
-p	It means to ask NISP.
-P	It means to ask NISP name.
-b	It means to ask BCMCS.

-B	It means to ask BCMCS name.
-r	It means to ask refresh time.
Parameter	1: the parameter related to the request will be displayed.
	0: the parameter related to the request will not be displayed.

Example

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

Telnet Command: ip6 dhcp client

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

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

Syntax Description

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

Example

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

```
      DHCPv6 client enabled
      request IA_NA whose IAID equals to 2008
> system reboot
```

Telnet Command: ip6 dhcp server

This command allows you to configure DHCPv6 server.

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

Syntax Description

Parameter	Description
server	It means the dhcp server settings.
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-a	It means to show current DHCPv6 status.
-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
```

Dray Tek

Telnet Command: ip6 internet

This command allows you to configure settings for accessing Internet.

ip6 internet *-W n -M n [-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
-W n	**W** means to set WAN interface and **n** means different selections. Default is WAN1. n=1: WAN1 n=2: WAN2 n=3: WAN3 . . n=X: WANx
-M n	M means to set Internet Access Mode (Mandatory) and n means different modes (represented by 0 – 5) n= 0: Offline, n=1: PPP, n=2: TSPC, n=3: AICCU, n=4: DHCPv6, n=5: Static n=6:6in4-Static n=7:6rd
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-m n	It means to set IPv6 MTU. N = any value (0 means "unspecified").
-u <username>	It means to set Username. <username>= type a name as the username (maximum 63 characters).
-p <password>	It means to set Password. <password> = type a password (maximum 63 characters).
-l n	It means to set IPv6 prefix length for protocol of 6rd. n: IPv6 prefix length.
-s <server>	It means to set Tunnel Server IP. <server>= IPv4 address or URL (maximum 63 characters).
-d <server>	It means to set the primary DNS Server IP. <server>= type an IPv6 address for first DNS server.
-D <server>	It means to set the secondary DNS Server IP. <server>= type an IPv6 address for second DNS server.
-t <dhcp/ra/none>	It means to set IPv6 PPP WAN test mode for DHCP or

	RADVD.
	<dhcp/ra/none>= type IPv6 address.
-V	It means to view IPv6 Internet Access Profile.
-o	It means to set AICCU always on. 1=On, 0=Off

Example

```
> ip6 internet -W 2 -M 2 -u 88886666 -p draytek123456 -s
amsterdam.freenet6.net
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
> system reboot
```

Telnet Command: ip6 neigh

This command allows you to display IPv6 neighbour table.

ip6 neigh *-s[inet6_addr] [eth_addr] [LAN/WAN1/WAN2]*

ip6 neigh *-d [inet6_addr] [LAN/WAN1/WAN2]*

ip6 neigh *-a [inet6_addr] [-N LAN/WAN1/WAN2]*

Syntax Description

Parameter	Description
-s	It means to add a neighbour.
-d	It means to delete a neighbour.
-a	It means to show neighbour status.
inet6_addr	Type an IPv6 address
eth_addr	Type submask address.
LAN/WAN1/WAN2	Specify an interface for the neighbor.

Example

```
> ip6 neigh -s 2001:2222:3333::1111 00:50:7F:11:ac:22:WAN2
        Neighbour 2001:2222:3333::1111 successfully added!
> ip6 neigh -a

I/F  ADDR                                    MAC                STATE
--------------------------------------------------------------------
LAN FF02::1                                  33-33-00-00-00-01  CONNECTED
WAN2 2001:5C0:1400:B::10B8                   00-00-00-00-00-00  CONNECTED
WAN2 2001:2222:3333::1111                    00-00-00-00-00-00  CONNECTED
WAN2 2001:2222:6666::1111                    00-00-00-00-00-00  CONNECTED
WAN2 ::                                      00-00-00-00-00-00  CONNECTED
LAN  ::                                                         NONE
>
```

Telnet Command: ip6 pneigh

This command allows you to add a proxy neighbour.

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

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

ip6 pneigh *-a [inet6_addr] [-N LAN/WAN1/WAN2]*

Syntax Description

Parameter	Description
-s	It means to add a proxy neighbour.
-d	It means to delete a proxy neighbour.
-a	It means to show proxy neighbour status.
inet6_addr	Type an IPv6 address
LAN/WAN1/WAN2	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

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
```

Dray Tek

Vigor2120 Series User's Guide

```
 PREFIX/PREFIX-LEN _EXPIRES_ _NEXT-HOP_  I/F  METRIC   STATE    FLAGS
--------------------------------------------------------------------
 FE80::/128                               LAN    0   UNICAST    U
                     0   ::
 FE80::250:7FFF:FE00:0/128                LAN    0   UNICAST    U
                     0   ::
 FE80::/64                                LAN   256  UNICAST    U
                     0
 FE80::/16                                LAN  1024  UNICAST    UGA
                     0   FE80::250:7FFF:FE12:100
 FF02::1/128                              LAN    0   UNICAST    UC
                     0   FF02::1
 FF00::/8                                 LAN   256  UNICAST    U
                     0
 ::/0                                     LAN   -1   UNREACHABLE !
                     0
```

Telnet Command: ip6 ping

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

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

Syntax Description

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

Example

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

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

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


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

DrayTek

Telnet Command: ip6 tspc

This command allows you to display TSPC status.

ip6 tspc *[ifno]*

Syntax Description

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

Example

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

Status: Connected

>
```

Telnet Command: ip6 radvd

This command allows you to enable or disable RADVD server.

Ip6 radvd *–s [1/0] [lifetime]*

ip6 radvd *–V*

Syntax Description

Parameter	Description
-s	It means to enable or disable the default lifetime of the RADVD server.
	1: Enable the RADVD server.
	0: Disable the RADVD server.
Lifetime	It means to set the lifetime.
	The lifetime associated with the default router in units of seconds. It's used to control the lifetime of the prefix. The maximum value corresponds to 18.2 hours. A lifetime of 0 indicates that the router is not a default router and should not appear on the default router list.
	Type the number (unit: second) you want.
-V	It means to show the RADVD configuration.
-r	It means RA default test.

-r [num]	It means RA test for item [num].

Example

```
> ip6 radvd -s 1 1800
> ip6 radvd -V
%  IPv6 Radvd Config:
Radvd : Enable, Default Lifetime : 1800 seconds
```

Telnet Command: ip6 mngt

This command allows you to manage the settings for access list.

ip6 mngt list

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

ip6 mngt status

ip6 mngt *[http|telnet|ping|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.

ip6 *online [ifno]*

Syntax Description

Parameter	Description
ifno	It means the connection interface.
	0=LAN1
	1=WAN1
	2=WAN2

Example

```
> ip6 online 0
 % LAN 1 online status :
 % Interface : UP
 % IPv6 DNS Server: :: Static
 % IPv6 DNS Server: :: Static
 % IPv6 DNS Server: :: Static
 % Tx packets = 408, Tx bytes = 32160, Rx packets = 428, Rx bytes =
33636

> ip6 online 1
 % WAN 1 online status :
 % IPv6 WAN1 Disabled
 % Default Gateway : ::
 % UpTime : 0:00:00
 % Interface : DOWN
 % IPv6 DNS Server: :: Static
 % IPv6 DNS Server: :: Static
 % IPv6 DNS Server: :: Static
 % Tx packets = 0, Tx bytes = 0, Rx packets = 0, Rx bytes = 0
```

Telnet Command: ip6 aiccu

This command allows you to set IPv6 settings for WAN interface with connection type of AICCU.

ip6 aiccu *[ifno]*

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

Syntax Description

Parameter	Description

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

Example

```
> ip6 aiccu subnet add 2 2001:1111:0000::1111 64
> ip6 aiccu 2
Status: Connecting

>ip6 aiccu subnet show 2
IPv6 WAN2 AICCU Subnet Prefix Config:
2001:1111::1111/64
>
```

Telnet Command: ip6 ntp

This command allows you to set IPv6 settings for NTP (Network Time Protocols) server.

ip6 ntp –h

ip6 ntp –v

ip6 ntp –p [0/1]

Syntax Description

Parameter	Description
–h	It is used to display the usage of such command.
-v	It is used to show the NTP state.
-p <0/1>	It is used to specify NTP server for IPv6. 0 – Auto 1 – First Query IPv6 NTP Server.

Example

```
> ip6 ntp -p 1
% Set NTP Priority: IPv6 First
```

Telnet Command: ipf view

IPF users to view the version of the IP filter, to view/set the log flag, to view the running IP filter rules.

Dray Tek

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.

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.

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 following lists all of the available commands with parameters.
-e	It means to enable or disable the rule setting. 0- disable 1- enable
-s o:g <obj>	It means to specify source IP object and IP group. 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

Dray Tek

Vigor2120 Series User's Guide

–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,

Dray Tek

	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>	It means to set Window size and Session timeout (Minute).

<Session_Timeout>	<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.

ipf flowtrack set *[-re]*

ipf flowtrack view *[-f] [-b]*

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

Syntax Description

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

Example

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

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

Telnet Command: Log

This command allows users to view log for WAN interface such as call log, IP filter log, flush log buffer, etc.

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

Syntax Description

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

Example

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

Dray Tek

Telnet Command: mngt ftpport

This command allows users to set FTP port for management.

mngt ftpport *[FTP port]*

Syntax Description

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

Example

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

Telnet Command: mngt httpport

This command allows users to set HTTP port for management.

mngt httpport *[Http port]*

Syntax Description

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

Example

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

Telnet Command: mngt httpsport

This command allows users to set HTTPS port for management.

mngt httpsport *[Https port]*

Syntax Description

Parameter	Description
Https port	It means to type the number for HTTPS port. The default setting is 443.

Example

```
> mngt httpsport 443
% Set web server port to 443 done.
```

Dray Tek

Telnet Command: mngt telnetport

This command allows users to set telnet port for management.

mngt telnetport *[Telnet port]*

Syntax Description

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

Example

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

Telnet Command: mngt sshport

This command allows users to set SSH port for management.

mngt sshport *[ssh port]*

Syntax Description

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

Example

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

Telnet Command: mngt ftpserver

This command can enable/disable FTP server.

mngt ftpserver *[enable]*

mngt ftpserver *[disable]*

Syntax Description

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

Example

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

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

Dray Tek

Telnet Command: mngt noping

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

mngt noping *[on]*

mngt noping *[off]*

mngt noping *[viewlog]*

mngt noping *[clearlog]*

Syntax Description

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

Example

```
> mngt noping off
No Ping Packet Out is OFF!!
```

Telnet Command: mngt defenseworm

This command can block specified port for passing through the router.

mngt defenseworm *[on]*

mngt defenseworm *[off]*

mngt defenseworm *[add port]*

mngt defenseworm *[del port]*

mngt defenseworm *[viewlog]*

mngt defenseworm *[clearlog]*

Syntax Description

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

Example

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

Telnet Command: mngt rmtcfg

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

mngt rmtcfg *[status]*

mngt rmtcfg *[enable]*

mngt rmtcfg *[disable]*

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

Syntax Description

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

Dray Tek

disable	It means to deny the system administrators to login from the Internet.
http/https/ftp/telnet/ssh/tr0 69	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 echoicmp

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

mngt echoicmp *[enable]*

mngt echoicmp *[disable]*

Syntax Description

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

Example

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

Telnet Command: mngt accesslist

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

mngt accesslist *list*

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

mngt accesslist *remove [index]*

mngt accesslist *flush*

Syntax Description

Parameter	Description

list	It can display current setting for your reference.
add	It means adding a new entry.
index	It means to specify the number of the entry.
ip addr	It means to specify an IP address.
mask	It means to specify the subnet mask for the IP address.
remove	It means to delete the selected item.
flush	It means to remove all the settings in the access list.

Example

```
> mngt accesslist add 1 192.168.1.89 255.255.255.0
%% Set OK.
> mngt accesslist list
%% Access list :
  Index IP address      Subnet mask
=========================================
  1    192.168.1.89    255.255.255.0
```

Telnet Command: mngt snmp

This command allows you to configure SNMP for management.

mngt snmp *[-<command> <parameter> | ...]*

Syntax Description

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

Example

Dray Tek

```
> 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: msubnet switch

This command is used to configure multi-subnet.

msubnet switch *[2][On/Off]*

Syntax Description

Parameter	Description
2	It means LAN interface. 2=LAN2
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.

msubnet addr *[2][IP address]*

Syntax Description

Parameter	Description
2	It means LAN interface. 2=LAN2
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.

msubnet nmask *[2][IP address]*

Syntax Description

Parameter	Description
2	It means LAN interface. 2=LAN2
IP address	Type the subnet mask address for the specified LAN interface.

Example

```
> msubnet nmask 2 255.255.0.0
% Set LAN2 subnet mask done !!!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet status

This command is used to display current status of subnet.

msubnet status *[2]*

Syntax Description

Parameter	Description
2	It means LAN interface.

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.

msubnet dhcps *[2][On/Off]*

Syntax Description

Parameter	Description
2	It means LAN interface. 2=LAN2
On/Off	On means enabling the DHCP server for the specified LAN interface.

Dray Tek

| | Off means disabling the DHCP server. |

Example

```
> msubnet dhcps 2 off
% LAN2 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.

msubnet nat *[2] [On/Off]*

Syntax Description

Parameter	Description
2	It means LAN interface. 2=LAN2
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.

msubnet gateway *[2] [Gateway IP]*

Syntax Description

Parameter	Description
2	It means LAN interface. 2=LAN2
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.

msubnet ipcnt *[2] [IP counts]*

Syntax Description

Parameter	Description
2	It means LAN interface. 2=LAN2
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.

msubnet talk *[1/2] [1/2] [On/Off]*

Syntax Description

Parameter	Description
1/2/3/4/5/6	It means LAN interface. 1=LAN1 2=LAN2
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> <1/2> <On/Off>
% where 1:LAN1, 2:LAN2
% Now:
%           LAN1   LAN2
% LAN1        V
```

```
% LAN2          V      V
>
```

Telnet Command: msubnet startip

This command is used to configure a starting IP address for DCHP.

msubnet startip *[2] [Gateway IP]*

Syntax Description

Parameter	Description
2	It means LAN interface. 2=LAN2
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> <Gateway IP>
% Now: LAN2 192.168.2.90
```

Telnet Command: msubnet pppip

This command is used to configure a starting IP address for PPP connection.

msubnet pppip *[2] [Start IP]*

Syntax Description

Parameter	Description
2	It means LAN interface. 2=LAN2
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> <Start IP>
% Now: LAN2 192.168.2.250
```

Telnet Command: msubnet nodetype

This command is used to specify the type for node which is required by DHCP option.

msubnet nodetype *[2][count]*

Syntax Description

Parameter	Description
2	It means LAN interface. 2=LAN2
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 2 1
% Set LAN2 Dhcp Node Type done !!!

> > msubnet nodetype
% msubnet nodetype <2> <count>
% Now: LAN2 1

% 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.

msubnet primWINS *[2] [WINS IP]*

Syntax Description

Parameter	Description
2	It means LAN interface. 2=LAN2
WINS IP	Type the IP address as the WINS IP.

Example

```
> msubnet primWINS 2 192.168.3.5
% Set LAN2 Dhcp Primary WINS IP done !!!

> msubnet primWINS
% msubnet primWINS <2> <WINS IP>
% Now: LAN2 192.168.3.5 2.168.3.5; LAN3 0.0.0.0; LAN4 0.0.0.0; LAN5
0.0.0.0; LAN6 0.0.0.0
```

DrayTek

Telnet Command: msubnet secWINS

This command is used to configure secondary WINS server.

msubnet secWINS *[2] [WINS IP]*

Syntax Description

Parameter	Description
2	It means LAN interface. 2=LAN2
WINS IP	Type the IP address as the WINS IP.

Example

```
>  msubnet secWINS 2 192.168.3.89
% Set LAN2 Dhcp Secondary WINS IP done !!!

> msubnet secWINS
% msubnet secWINS <2> <WINS IP>
% Now: LAN2 192.168.3.89
```

Telnet Command: msubnet tftp

This command is used to set TFTP server for multi-subnet.

msubnet tftp *[2 [TFTP server name]*

Syntax Description

Parameter	Description
2	It means LAN interface. 2=LAN2
TFTP server name	Type a name to indicate the TFTP server.

Example

```
> msubnet tftp ?
% msubnet tftp <2> <TFTP server name>
% Now: LAN2
> msubnet tftp 2 publish
% Set LAN2 TFTP Server Name done !!!

> msubnet tftp
% msubnet tftp <2> <TFTP server name>
% Now: LAN2 publish
```

Telnet Command: msubnet mtu

This command allows you to configure MTU value for LAN/DMZ/IP Routed Subnet.

msubnet mtu *[interface][value]*

Syntax Description

Parameter	Description
interface	Available settings include LAN1~LAN2 and IP_Routed_Subnet.
value	1000 ~ 1496 (Bytes).

Example

```
> msubnet mtu LAN1 1492
> > msubnet mtu
Usage:

  >msubnet mtu <interface> <value>

  <interface>: LAN1~LAN2,IP_Routed_Subnet,  <value>:  1000 ~ 1496
(Bytes), de
fault: 1500 (Bytes)

  e.x: >msubnet mtu LAN1 1492

Current Settings:
```

```
  LAN1 MTU:            1492 (Bytes)
  LAN2 MTU:            1500 (Bytes)
  IP Routed Subnet MTU: 1500 (Bytes)
>
```

Telnet Command: object ip obj

This command is used to create an IP object profile.

object ip obj setdefault

object ip obj *INDEX -v*

object ip obj *INDEX -n NAME*

object ip obj *INDEX -i INTERFACE*

object ip obj *INDEX -s INVERT*

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

Syntax Description

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

[START_IP]	When the TYPE is set with 2, you have to type an IP address as a starting point and another IP address as end point. Type an IP address.
[END/MASK_IP]	Type an IP address (different with START_IP) as the end IP address.

Example

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

Telnet Command: object ip grp

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

object ip grp setdefault

object ip grp *INDEX -v*

object ip grp *INDEX -n NAME*

object ip grp *INDEX -i INTERFACE*

object ip grp *INDEX -a IP_OBJ_INDEX*

Syntax Description

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

Dray Tek

	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.

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 ipv6 grp

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

object ip grp setdefault

object ip grp *INDEX -v*

object ip grp *INDEX -n NAME*

object ip grp *INDEX -i INTERFACE*

object ip grp *INDEX -a IP_OBJ_INDEX*

Syntax Description

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

Example

```
> > object ip grp 2 -n First
 IP Group Profile 2
```

```
 Name   :[First]
 Interface:[Any]
 Included ip object index:
 [0:][0]
 [1:][0]
 [2:][0]
 [3:][0]
 [4:][0]
 [5:][0]
 [6:][0]
 [7:][0]
 [8:][0]
 [9:][0]
 [10:][0]
 [11:][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]
 [8:][0]
 [9:][0]
 [10:][0]
 [11:][0]
```

Telnet Command: object service obj

This command is used to create service object profile.

object service obj setdefault

object service obj *INDEX -v*

object service obj *INDEX -n NAME*

object service obj *INDEX -p PROTOCOL*

object service obj *INDEX -s CHK [START_P] [END_P]*

object service obj *INDEX -d CHK [START_P] [END_P]*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.

Dray Tek

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

Example

```
> object service obj 1 -n limit
> object service obj 1 -p 255
> object service obj 1 -s 1 120 240
> object service obj 1 -d 1 200 220
> object service obj 1 -v
 Service Object Profile 1
 Name   :[limit]
 Protocol:[255]
 Source port check action:[!=]
 Source port range:[120~240]
 Destination port check action:[!=]
 Destination port range:[200~220]
```

Telnet Command: object service grp

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

object service grp setdefault

object service grp *INDEX -v*

object service grp *INDEX -n NAME*

object service grp *INDEX -a SER_OBJ_INDEX*

Syntax Description

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

Example

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

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

DrayTek

```
[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]
```

Telnet Command: object kw

This command is used to create keyword profile.

object kw obj setdefault

object kw obj show PAGE

object kw obj *INDEX -v*

object kw obj *INDEX -n NAME*

object kw obj *INDEX -a CONTENTS*

Syntax Description

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

Example

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

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

Telnet Command: object fe

This command is used to create File Extension Object profile.

object fe show

object fe setdefault

object fe obj *INDEX -v*

object fe obj *INDEX -n NAME*

object fe obj *INDEX -e CATEGORY|FILE_EXTENSION*

object fe obj *INDEX -d CATEGORY|FILE_EXTENSION*

Syntax Description

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

Dray Tek

Example

```
> object fe obj 1 -n music
> object fe obj 1 -e Audio
> object fe obj 1 -v
Profile Index: 1
Profile Name:[music]

----------------------------------------------------------------------
------
Image category:
 [ ].bmp   [ ].dib   [ ].gif   [ ].jpeg  [ ].jpg   [ ].jpg2  [ ].jp2   [ ].pct
 [ ].pcx   [ ].pic   [ ].pict  [ ].png   [ ].tif   [ ].tiff
----------------------------------------------------------------------
------
Video category:
 [ ].asf   [ ].avi   [ ].mov   [ ].mpe   [ ].mpeg  [ ].mpg   [v].mp4   [ ].qt
 [ ].rm    [v].wmv   [ ].3gp   [ ].3gpp  [ ].3gpp2 [ ].3g2
----------------------------------------------------------------------
------
Audio category:
 [v].aac   [v].aiff  [v].au    [v].mp3   [v].m4a   [v].m4p   [v].ogg   [v].ra
 [v].ram   [v].vox   [v].wav   [v].wma
----------------------------------------------------------------------
------
Java category:
 [ ].class [ ].jad   [ ].jar   [ ].jav   [ ].java  [ ].jcm   [ ].js    [ ].jse
 [ ].jsp   [ ].jtk
----------------------------------------------------------------------
------
ActiveX category:
 [ ].alx   [ ].apb   [ ].axs   [ ].ocx   [ ].olb   [ ].ole   [ ].tlb   [ ].viv
 [ ].vrm
----------------------------------------------------------------------
------
Compression category:
 [ ].ace   [ ].arj   [ ].bzip2 [ ].bz2   [ ].cab   [ ].gz    [ ].gzip  [ ].rar
 [ ].sit   [ ].zip
----------------------------------------------------------------------
------
Execution category:
 [ ].bas   [ ].bat   [ ].com   [ ].exe   [ ].inf   [ ].pif   [ ].reg   [ ].scr
```

Telnet Command: port

This command allows users to check the connection speed used by each port.

port status

Syntax Description

Parameter	Description
status	It means to view the Ethernet port status.

Example

```
> port status
% port 1 : link DOWN, speed= ---- Mbps, duplex= ----, FlowControl= --
% port 2 : link DOWN, speed= ---- Mbps, duplex= ----, FlowControl= --
% port 3 : link UP  , speed=  100 Mbps, duplex= FULL, FlowControl= OFF
% port 4 : link DOWN, speed= ---- Mbps, duplex= ----, FlowControl= --
% WAN1  : link DOWN, speed= ---- Mbps, duplex= ----, FlowControl= --
```

Telnet Command: portmaptime

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

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

Syntax Description

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

Dray Tek

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.

prn status

Example

```
> prn status
Interface: USB bus 2.0
Printer: NotReady


VR9 USB host : USB1: NotReady , USB2: NotReady
```

Telnet Command: qos setup

This command allows user to set general settings for QoS.

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

Syntax Description

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

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

Example

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

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

Dray Tek

Telnet Command: qos class

This command allows user to set QoS class.

qos class -c *[no] –[a|e|d] [no][-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
[<command> <parameter>|...]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-h	Type it to display the usage of this command.
-c <no>	Specify the inde number for the class. Available value for <no> contains 1, 2 and 3. The default setting is class 1.
-n <name>	It means to type a name for the class.
-a	It means to add rule for specified class.
-e <no>	It means to edit specified rule. <no>: type the index number for the rule.
-d <no>	It means to delete specified rule. <no>: type the index number for the rule.
-m <mode>	It means to enable or disable the specified rule. 0: disable, 1: enable
-l <addr>	Set the local address. *Addr1* – It means Single address. Please specify the IP address directly, for example, "*-l 172.16.3.9*". *addr1:addr2* – It means Range address. Please specify the IP addresses, for example, "*-l 172.16.3.9: 172.16.3.50.*" *addr1:subnet* – It means the subnet address with start IP address. Please type the subnet and the IP address, for example, "*-l 172.16.3.9:255.255.0.0".0* *any* – It means Any address. Simple type "*-l*" to specify any address for this command.
-r <addr>	Set the remote address. *addr1* – It means Single address. Please specify the IP address directly, for example, "*-l 172.16.3.9*". *addr1:addr2* – It means Range address. Please specify the IP addresses, for example, "*-l 172.16.3.9: 172.16.3.50.*" *addr1:subnet* – It means the subnet address with start IP address. Please type the subnet and the IP address, for example, "*-l 172.16.3.9:255.255.0.0".0* *any* – It means Any address. Simple type "*-l*" to specify any address for this command.
-p <DSCP id>	Specify the ID.

Dray Tek

Vigor2120 Series User's Guide

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

Example

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

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

Telnet Command: qos type

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

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

Syntax Description

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

DrayTek

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
```

DrayTek

```
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 traffic

This comman can display traffic graph for WAN1, WAN2, transmitted bytes, receivied bytes and sessions.

show traffic *[wan1/wan2] [tx/rx] [weekly]*

show traffic session *[weekly]*

Example

```
> show traffic session weekly0 ,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 ,2 ,1 ,0 ,0 ,0 ,0 ,0 ,0 ,
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,1 ,3 ,0 ,0 ,0 ,0 ,0 ,2 ,15 ,5 ,4 ,1 ,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
> show traffic wan1 tx weekly0 ,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 ,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
```

Telnet Command: show statistic

This command displays statistics for WAN interface.

show statistic

show statistic reset *[interface]*

Syntax Description

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

Example

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

Dray Tek

Telnet Command: srv dhcp dhcp2

This command is used to enable DCHP2 server.

srv dhcp dhcp2 *[-<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.
-l<enable>	It menas to enable the LAN port to public DHCP. 0: Disenable 1: Enable
-m<enable>	It menas to enable MAC address to public DHCP. 0: Disenable 1: Enable
-e<id>	It menas to turn on the flag of LAN port 1/2/3/4.
-d<id>	It menas to turn off the flag of LAN port 1/2/3/4.
-v	It menas to view current status.

Example

```
> srv dhcp dhcp2 -l 1 -e 1
> srv dhcp dhcp2 -v
 2nd DHCP server flag status --
   Server works on specified MAC address: ON
   Server works on specified LAN port: ON
   Port 1 flag: ON
   Port 2 flag: ON
   Port 3 flag: OFF
   Port 4 flag: OFF
```

Telnet Command: srv dhcp public

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

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.

srv dhcp dns1 *[lan1/lan2/lan3/lan4] [DNS IP address]*

Syntax Description

Parameter	Description
lan1/lan2/lan3/lan4	It means to specify the LAN port.
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 lan1 168.95.1.1
% srv dhcp dns1 lan1 <DNS IP address>
% Now: 168.95.1.1
```

Telnet Command: srv dhcp dns2

This command allows users to set Secondary IP Address for DNS Server in LAN.

srv dhcp dns2 *[lan1/lan2/lan3/lan4] [DNS IP address]*

Syntax Description

Parameter	Description
lan1/lan2/lan3/lan4	It means to specify the LAN port.
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 lan2 10.1.1.1
% srv dhcp dns2 lan2 <DNS IP address>
% Now: 10.1.1.1
```

Telnet Command: srv dhcp frcdnsmanl

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

srv dhcp frcdnsmanl *[on]*

srv dhcp frcdnsmanl *[off]*

Syntax Description

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

Example

```
> srv dhcp frcdnsmanl on

% Domain name server now is using manual settings!

> srv dhcp frcdnsmanl off

% Domain name server now is using auto settings!
```

Telnet Command: srv dhcp gateway

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

srv dhcp gateway *[?]*

srv dhcp gateway *[Gateway IP]*

Syntax Description

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

Example

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

Telnet Command: srv dhcp ipcnt

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

srv dhcp ipcnt *[?]*

srv dhcp ipcnt *[IP counts]*

Syntax Description

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

Example

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

Telnet Command: srv dhcp off

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

Telnet Command: srv dhcp on

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

Telnet Command: srv dhcp relay

This command allows users to set DHCP relay setting.

srv dhcp relay servip *[server ip]*

srv dhcp relay subnet *[index]*

Syntax Description

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

Example

```
> srv dhcp relay servip 192.168.1.46
> srv dhcp relay subnet 2
```

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

Telnet Command: srv dhcp startip

srv dhcp startip *[?]*

srv dhcp startip *[IP address]*

Syntax Description

Parameter	Description
?	It means to display current used start IP address.
IP address	It means the IP address that you can specify for the DHCP server as the starting point.

Example

```
> srv dhcp startip 192.168.1.53
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: srv dhcp status

This command can display general information for the DHCP server, such as IP address, MAC address, leased time, host ID and so on.

Example

```
> srv dhcp status
LAN1      : 192.168.1.1/255.255.255.0, DHCP server: On
Default gateway: 192.168.1.1
Index   IP Address      MAC Address            Leased Time      HOST ID
1      192.168.1.12    00-05-5D-E4-D8-EE       118:18:19        A1000351
2      192.168.1.255   00-00-00-00-00-00       BAD IP
3      192.168.1.0     00-00-00-00-00-00       BAD IP
4      192.168.1.1     00-00-00-00-00-00       BAD IP
```

Telnet Command: srv dhcp leasetime

This command can set the lease time for the DHCP server.

srv dhcp leasetime *[?]*

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

Syntax Description

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

Example

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

Telnet Command: srv dhcp nodetype

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

srv dhcp nodetype *<count>*

Syntax Description

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

Example

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

Telnet Command: srv dhcp primWINS

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

srv dhcp primWINS *[WINS IP address]*

srv dhcp primWINS clear

Syntax Description

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

Example

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

Telnet Command: srv dhcp secWINS

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

srv dhcp secWINS *[WINS IP address]*

srv dhcp secWINS clear

Syntax Description

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

Example

```
> srv dhcp secWINS 192.168.1.180
> srv dhcp secWINS ?
%% srv dhcp secWINS <WINS IP address>
%% srv dhcp secWINS clear
% Now: 192.168.1.180
```

Telnet Command: srv dhcp expRecycleIP

This command can set the time to check if the IP address can be assigned again by DHCP server or not.

srv dhcp expRecycleIP *<sec time>*

Syntax Description

Parameter	Description
sec time	It means to set the time (5~300 seconds) for checking if the IP can be assigned again or not.

Example

```
> srv dhcp expRecycleIP 250
% DHCP expired_RecycleIP = 250
```

Telnet Command: srv dhcp tftp

This command can set the TFTP server as the DHCP server.

srv dhcp tftp *<TFTP server name>*

Syntax Description

Parameter	Description
TFTP server name	It means to type the name of TFTP server.

Example

```
> srv dhcp tftp TF123
> srv dhcp tftp ?
%% srv dhcp tftp <TFTP server name>
% Now: TF123
```

Telnet Command: srv dhcp tftpdel

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

srv dhcp tftpdel

Example

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

Dray Tek

Telnet Command: srv dhcp option

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

srv dhcp option *-h*

srv dhcp option *-l*

srv dhcp option *-d [idx]*

srv dhcp option *-e [1 or 0] -i [lan number] -c [option number] -v [option value]*

srv dhcp option -*e [1 or 0] -i [lan number] -c [option number] -a [option value]*

srv dhcp option *-e [1 or 0] -i [lan number] -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
-i	It means to set LAN number. 1: lan1 a: all LAN r: routed subnet.
-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 -i 2/r -c 44 -a 192.168.1.10,192.168.1.20
> srv dhcp option -l
% state   idx interface       opt type    data


% enable  1  LAN2/r          44  Address
192.168.1.10  ,192.168.1.20  ,

```

Telnet Command: srv nat addrmapping

This command allows users to map specific private IP to specific WAN IP alias.

srv nat addrmapping *n [-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
n	It means the number of the address mapping rule profile. n = 1 to 10
[<command> <parameter>|...]	The available commands with parameters are listed below. *[...]* means that you can type in several commands in one line.
-e <enable>	It means to enable or disable the address mapping rule profile. 0: disable 1:enable
-l <ip>	It means private IP address (LAN IP).
-w <idx>	It means to specify the public IP. 1: WAN1 Default, 2: WAN1 Alias 1, ...
-p <protocol>	Specify the transport layer protocol. Avaialbe values are TCP, UDP and ALL.
m <masklen>	It means the lenght of the mask address. Avaialbe values are 16, 24-32.
-v	It means to view current settings.

Example

```
> srv nat addrmapping 1 -e 1 -l 192.168.1.90 -p TCP -m 16
> srv nat addrmapping -v
-------------current NAT address map settings----------

#rule-set 1
-----------------------
enable: 1
protocol: TCP
public IP: #1: 208.228.145.2
private IP: 192.168.1.90
mask: /16

#rule-set 2
-----------------------
enable: 0
protocol: all
public IP: #1: 192.168.1.90
private IP: 0.0.0.0
mask: /32
```

Telnet Command: srv nat dmz

This command allows users to set DMZ host. Before using this command, please set WAN IP Alias first.

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

Syntax Description

Parameter	Description
n	It means to map selected WAN IP to certain host. 1: wan1 2: wan2
m	It means the index number (1 ~ 8) of the DMZ host. Default setting is "1" (WAN 1). It is only available for Static IP mode. If you use other mode, you can set 1 ~ 8 in this field. If WAN IP alias has been configured, then the number of DMZ host can be added more.
[<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.

Srv nat ipsecpass *[options]*

Syntax Description

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

	source port (500) preservation.
status	It means to display current status for checking.

Example

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

Telnet Command: srv nat openport

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

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

Syntax Description

Parameter	Description
n	It means the index number for the profiles. The range is from 1 to 20.
m	It means to specify the sub-item number for this profile. The range is from 1 to 10.
[<command> <parameter>|...]	The available commands with parameters are listed below. *[...]* means that you can type in several commands in one line.
-a <enable>	It means to enable or disable the open port rule profile. 0: disable 1:enable
-c <comment>	It means to type the description (less than 23 characters) for the defined network service.
-i <local ip>	It means to set the IP address for local computer. Local ip: Type an IP address in this field.
-w <idx>	It means to specify the public IP. 1: WAN1 Default, 2: WAN1 Alias 1, …and so on.
-p <protocol>	Specify the transport layer protocol. Available values are TCP, UDP and ALL.
-s<start port>	It means to specify the starting port number of the service offered by the local host. The range is from 0 to 65535.
-e<end port>	It means to specify the ending port number of the service offered by the local host. The range is from 0 to 65535.
-v	It means to display current settings.
-r <remove>	It means to delete the specified open port setting. remove: Type the index number of the profile.
-f <flush>	It means to return to factory settings for all the open ports

Dray Tek

profiles.

Example

```
> srv nat openport 1 1 -a 1 -c games -i 192.168.1.100 -w 1 -p TCP -s
23 -e 83
> srv nat openport -v
%% Status: Enable
%% Comment: games
%% Private IP address: 192.168.1.100
Index   Protocal       Start Port     End Port
****************************************************************
  1.    TCP            23             83

%% Status: Disable
%% Comment:
%% Private IP address: 0.0.0.0
Index   Protocal       Start Port     End Port
****************************************************************

%% Status: Disable
%% Comment:
%% Private IP address: 0.0.0.0
Index   Protocal       Start Port     End Port
****************************************************************
>
```

Telnet Command: srv nat portmap

This command allows users to set port redirection table for NAT server.

srv nat portmap *add [idx][serv name][proto][pub port][pri ip][pri port][wan1/wan2]*

srv nat portmap *del [idx]*

srv nat portmap *disable [idx]*

srv nat portmap *enable [idx] [proto]*

srv nat portmap *flush*

srv nat portmap *table*

Syntax Description

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

del [idx]	It means to remove the selected port redirection setting.
disable [idx]	It means to inactivate the selected port redirection setting.
enable [idx]	It means to activate the selected port redirection setting.
flush	It means to clear all the port mapping settings.
table	It means to display Port Redirection Configuration Table.

Example

```
> srv nat portmap add 1 game tcp 80 192.168.1.11 100 wan1
> srv nat portmap table

NAT Port Redirection Configuration Table:

Index  Service Name    Protocol  Public Port  Private IP      Private
Port ifno
 1     game              6          80    192.168.1.11         100     -1
 2                       0           0                          0      -2
 3                       0           0                          0      -2
 4                       0           0                          0      -2
 5                       0           0                          0      -2
 6                       0           0                          0      -2
 7                       0           0                          0      -2
 8                       0           0                          0      -2
 9                       0           0                          0      -2
10                       0           0                          0      -2
11                       0           0                          0      -2
12                       0           0                          0      -2
13                       0           0                          0      -2
14                       0           0                          0      -2
15                       0           0                          0      -2
16                       0           0                          0      -2
17                       0           0                          0      -2
18                       0           0                          0      -2

19                       0           0                          0      -2

20                       0           0                          0      -2


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

Telnet Command: srv nat trigger

This command allows users to set port redirection table for NAT server.

srv nat trigger n *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
n	It means the index number for the profiles. The range is from 1 to 20.
*[-<command> <parameter>	...]*	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one

	line.
-c	It means to type a brief description for the setting profile.
-e	It means to enable/disable the specified profile. 1: Enable 0: Disable
-p	It means to set the the protocol for the profile. 1: TCP 2: UDP 3: All
-t	It means to set triggering port.
-P	It means to set the protocol for incomming packets. 1:TCP 2:UDP 3:All
-i	It means to set the protocol for incomming port. The range is from 0 to 65535.
-d	It means to delete the specified profile.
-v	It means to display port trigger setting.

Example

```
> srv nat trigger 1 -c test -e 1 -p 1 -t 500 -P 1 -i 1000
> srv nat trigger -v
%%     Port Trigger Rule status:
 Index  Status  Comment TProto  TPort   IProto  IPort
-----------------------------------------------------
   1    Enable  test    TCP     500     TCP     1000
   2    Disable
   3    Disable
   4    Disable
   5    Disable
   6    Disable
   7    Disable
   8    Disable
   9    Disable
  10    Disable
  11    Disable
  12    Disable
  13    Disable
  14    Disable
  15    Disable
  16    Disable
  17    Disable
  18    Disable
  19    Disable
  20    Disable
```

Telnet Command: srv nat 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.

switch -i *[switch idx_no] [option]*

switch not_respond 0

switch not_respond 1

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.
switch not_respond 0	It is used to disable "No Respond to External Device packets".
switch not_respond 1	It is used to enable "No Respond to External Device packets".

Example

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

Telnet Command: switch status

This command is used to display current status for external devices.

Example

```
>switch status
External Device auto discovery status : Disable

No Respond to External Device : Enable
```

Telnet Command: sys admin

This command is used for RD engineer to access into test mode of Vigor router.

Telnet Command: sys bonjour

This command is used to disable/enable and configure the Bonjour service.

sys bonjour *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
-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.

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 ?
```

Dray Tek

Telnet Command: sys ftpd

This command displays current status of FTP server.

sys ftpd *on*

sys ftpd *off*

Syntax Description

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

Example

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

Telnet Command: sys domainname

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

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

sys domainname *[wan1/wan2] 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 39.
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. 39 characters)>
% sys domainname <wan1/wan2> clear
% Now: wan1 == clever, wan2 ==intelligent
>
```

Telnet Command: sys iface

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

Example

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

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

Telnet Command: sys name

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

sys name *[wan1] [ASCII string]*

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

Syntax Description

Parameter	Description
wan1	It means to specify WAN interface for assigning a name for it.
ASCII string	It means the name for router. The maximum character that you can set is 20.

Example

```
> sys name wan1 drayrouter
> sys name ?
% sys name <wan1/wan2> <ASCII string (max. 39 characters)>
% sys name <wan1/wan2> clear
% Now: wan1 == drayrouter, wan2 ==
```

Note: Such name can be used to recognize router's identification in SysLog dialog.

Telnet Command: sys passwd

This command allows users to set password for the administrator.

sys passwd *[ASCII string]*

Syntax Description

Parameter	Description
ASCII string	It means the password for administrator. The maximum character that you can set is 23.

Example

```
> sys passwd admin123
>
```

Telnet Command: sys reboot

This command allows users to restart the router immediately.

Example

```
> sys reboot
>
```

Telnet Command: sys autoreboot

This command allows users to restart the router automatically within a certain time.

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

Syntax Description

Parameter	Description
on/off	On – It means to enable the function of auto-reboot. Off – It means to disable the function of auto-reboot.
hours	It means to set the time schedule for router reboot. For example, if you type "2" in this field, the router will reboot with an **interval** of two hours.

Example

```
> sys autoreboot on
 autoreboot is ON
> sys autoreboot 2
 autoreboot is ON
 autoreboot time is 2 hour(s)
```

Telnet Command: sys commit

This command allows users to save current settings to FLASH. Usually, current settings will be saved in SRAM. Yet, this command will save the file to FLASH.

Example

```
> sys commit
>
```

Telnet Command: sys tftpd

This command can turn on TFTP server for upgrading the firmware.

Example

```
> sys tftpd
% TFTP server enabled !!!
```

Telnet Command: sys cc

This command can display current 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: Vigor2120n+   Version: 3.7.5.4_RC1 [web]English
Profile version: 3.0.0   Status: 1 (0x6df0ae83)
Router IP: 192.168.1.1   Netmask: 255.255.255.0
Firmware Build Date/Time: Jan  7 2015 20:11:29
Router Name:
Revision: 46359 2120_375
```

Telnet Command: sys qrybuf

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

Example

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

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

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

Telnet Command: sys pollbuf

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

sys pollbuf *[on]*

sys pollbuf *[off]*

Syntax Description

Parameter	Description
on	It means to turn on pulling buffer.

| off | It means to turn off pulling buffer. |

Example

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

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

Telnet Command: sys tr069

This command can set CPE settings for applying in VigorACS.

sys tr069 get *[parm] [option]*

sys tr069 set *[parm] [value]*

sys tr069 getnoti *[parm]*

sys tr069 setnoti *[parm] [value]*

sys tr069 log

sys tr069 debug *[on/off]*

sys tr069 save

sys tr069 inform *[event code]*

sys tr069 port *[port num]*

sys tr069 cert_auth *[on/off]*

Syntax Description

Parameter	Description
get [parm] [option]	It means to get parameters for tr-069. option=<nextlevel>: only gets nextlevel for GetParameterNames.
set [parm] [value]	It means to set parameters for tr-069.
getnoti [parm]	It means to get parameter notification value.
setnoti [parm] [value]	It means to set parameter notification value.
log	It means to display the TR-069 log.
debug [on/off]	on: turn on the function of sending debug message to syslog. off: turn off the function of sending debug message to syslog.
save	It means to save the parameters to the flash memory of the router.
Inform [event code]	It means to inform parameters for tr069 with different event codes. [event code] includes: 0-"0 BOOTSTRAP", 1-"1 BOOT", 2-"2 PERIODIC",

Dray Tek

	3-"3 SCHEDULED",
	4-"4 VALUE CHANGE",
	5-"5 KICKED",
	6-"6 CONNECTION REQUEST",
	7-"7 TRANSFER COMPLETE",
	8-"8 DIAGNOSTICS COMPLETE",
	9-"M Reboot"
port [port num]	It means to change tr069 listen port number.
cert_auth [on/off]	on: turn on certificate-based authentication.
	off: turn off certificate-based authentication.

Example

```
> sys tr069 get Int. nextlevel
Total number of parameter is 24
Total content length of parameter is 915
InternetGatewayDevice.LANDeviceNumberOfEntries
InternetGatewayDevice.WANDeviceNumberOfEntries
InternetGatewayDevice.DeviceInfo.
InternetGatewayDevice.ManagementServer.
InternetGatewayDevice.Time.
InternetGatewayDevice.Layer3Forwarding.
InternetGatewayDevice.LANDevice.
InternetGatewayDevice.WANDevice.
InternetGatewayDevice.Services.
InternetGatewayDevice.X_00507F_InternetAcc.
InternetGatewayDevice.X_00507F_LAN.
InternetGatewayDevice.X_00507F_NAT.
InternetGatewayDevice.X_00507F_Firewall.
InternetGatewayDevice.X_00507F_Bandwidth.
InternetGatewayDevice.X_00507F_Applications.
InternetGatewayDevice.X_00507F_VPN.
InternetGatewayDevice.X_00507F_VoIP.
InternetGatewayDevice.X_00507F_WirelessLAN.
InternetGatewayDevice.X_00507F_System.
InternetGatewayDevice.X_00507F_Status.


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

Telnet Command: sys sip_alg

This command can turn on/off SIP ALG (Application Layer Gateway) for traversal.

sys sip_alg *[1]*

sys sip_alg *[0]*

Syntax Description

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

Example

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

Telnet Command: sys license

This command can process the system license.

sys license *licmsg*

sys license *licauth*

sys license *regser*

sys license *licera*

sys license *licifno*

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

sys license *dev_chg*

sys license *dev_key*

Syntax Description

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

Dray *Tek*

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

Example

```
> sys license licifno

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

Ex: licifno wan1

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

Telnet Command: sys fr_log

This command is used to display the content of web syslog (including time and message).

sys fr_log

Example

```
> sys fr_log

"2015-01-30 10:50:29", "[Telnet]Login success from IP
192.168.3.50 "
----------------------------------------------------------------
"2015-01-30 10:50:05", "Admin Mode save [System Maintenance >>>
Management]"
----------------------------------------------------------------
"2015-01-30 10:49:25", "Local User: 64.233.187.154:80 ->
192.168.1.11:17935 (TCP
) close connection"
----------------------------------------------------------------
-
"2015-01-30 10:49:25", "Local User: 141.8.224.25:80 ->
192.168.1.11:17934 (TCP)
close connection"
----------------------------------------------------------------
"2015-01-30 10:49:24", "Local User (MAC=00-00-00-45-00-00):
192.168.1.11:17935 -
> 64.233.187.154:80 (TCP)Web"
----------------------------------------------------------------
"2015-01-30 10:49:24", "Local User (MAC=00-00-00-3E-00-00):
192.168.1.11:17934 -
> 141.8.224.25:80 (TCP)Web"
----------------------------------------------------------------
"2015-01-30 10:49:15", "[H2L][UP][PPTP][@Radius:sh.test1]"
----------------------------------------------------------------
```

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<<
```

Dray Tek

```
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
>>>>> SERVICE TABLE3 <<<<<
  serviceType urn:schemas-upnp-org:service:WANIPConnection:1
  serviceId   urn:upnp-org:serviceId:WANIPConn1
  SCPDURL     /upnp/WIPConn1.xml
  controlURL  /upnp?control=WANIPConn1
  eventURL    /upnp?event=WANIPConn1
  UDN         uuid:1f41d0d6-4a64-42da-9593-5e266b10aed2
```

Telnet Command: upnp subscribe

This command can show all UPnP services subscribed.

Example

```
> upnp on
UPNP start.
> upnp subscribe
Vigor> upnp subscribe
>>>> (1) serviceType urn:schemas-microsoft-com:service:OSInfo:1

  ----- Subscribtion1 -------

    sid = 7a2bbdd0-0047-4fc8-b870-4597b34da7fb

    eventKey =1, ToSendEventKey = 1

    expireTime =6926

    active =1

    DeliveryURLs
=<http://192.168.1.113:2869/upnp/eventing/twtnpnsiun>

>>>> (2) serviceType
urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1

  ----- Subscribtion1 -------

    sid = d9cd47a5-d9c9-4d3d-8043-d03a82f27983

    eventKey =1, ToSendEventKey = 1
.
.
.
```

Telnet Command: upnp tmpvs

This command can display current status of temp Virtual Server of your router.

Example

```
Vigor> upnp tmpvs
*****************  Temp virtual server status  ***************

((0))
real_addr  >>192.168.1.10<<, pseudo_addr >>172.16.3.229<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>TCP<<
time >>0<<

((1))
real_addr  >>0.0.0.0<<, pseudo_addr >>0.0.0.0<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>0<<
time >>0<<
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
```

Telnet Command: upnp wan

This command is used to specify WAN interface to apply UPnP.

upnp wan *[n]*

Syntax Description

Parameter	Description
n	It means to specify WAN interface to apply UPnP.
	n=0, it means to auto-select WAN interface.
	n=1, WAN1
	n=2, WAN2 ……….

Example

```
> upnp wan 1
use wan1 now.
```

Telnet Command: usb list

This command is used 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
Alcatel    Alcatel L100V      LTE          Y
Alcatel    Alcatel W100       LTE          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 C502      3.5G          Y
Huawei     Huawei E169u       3.5G          Y
Huawei     Huawei E220        3.5G          Y
Huawei     Huawei E303D       3.5G          Y
Huawei     Huawei E3131       3.5G          Y
Huawei     Huawei E3372        LTE          Y
Huawei     Huawei E392         LTE          Y
Huawei     Huawei E398         LTE          Y
Huawei     Huawei K3772       3.5G          M
Huawei     Huawei K4605       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

ZTE        ZTE MF626         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!
```

Dray Tek

Telnet Command: vigbrg status

This command can show whether the Vigor Bridge Function is enabled or disabled.

Example

```
> vigbrg status
%Vigor Bridge Function is enable!

%Wan1 management is disable!
```

Telnet Command: vigbrg cfgip

This command allows users to transfer a bridge modem into ADSL router by accessing into and adjusting specified IP address. Users can access into Web UI of the router to manage the router through the IP address configured here.

vigbrg cfgip *[IP Address]*

Syntax Description

Parameter	Description
IP Address	It means to type an IP address for users to manage the router.

Example

```
> vigbrg cfgip 192.168.1.15
> vigbrg cfgip ?
% Vigor Bridge Config IP,
% Now: 192.168.1.15
```

Telnet Command: vigbrg wanstatus

This command can display the existed WAN connection status for the modem (change from ADSL router into bridge modem), including index number, MAC address, Stamp Time, PVC, VLAN port for Vigor Bridge Function.

Example

```
> vigbrg wanstatus
Vigor Bridge: Running
WAN mac table:
Index  MAC Address          Stamp Time      PVC        VLan
    Port
```

Telnet Command: vigbrg wlanstatus

This command can display the existed WLAN connection status for the modem (change from router into bridge modem), including index number, MAC address, Stamp Time, PVC, VLAN port for Vigor Bridge Function.

Example

```
> vigbrg wlanstatus
Vigor Bridge: Running
WAN mac table:
Index  MAC Address          Stamp Time      PVC      VLan      Port
```

Telnet Command: vpn group

This command allows you to set VLAN group. You can set four VLAN groups. Please run `vlan restart` command after you change any settings.

vlan group *id [set/set_ex] [p1/p2/p3/p4/s1/s2/s3/s4][5gs1/5gs2/5gs3/5gs4]*

Syntax Description

Parameter	Description
id	It means the group 0 to 7 for VLAN.
set	It indicates each port can join more than one VLAN group.
set_ex	It indicates each port can join one VLAN group at one time.
p1/p2/p3/p4	It indicates LAN port 1 to LAN port 4. To group LAN1, LAN2, LAN3 and/or LAN4 under one VLAN group, please type the port number(s) you want.
s1/s2/s3/s4	It is only available for WALN models.
5gs1/5gs2/5gs3/5gs4	It is only available for WLAN n-plus model.

Example

```
> > vlan group 3 set p1 s3 s4 5gs3 5gs4
 VLAN   p1   p2   p3   p4   s1   s2   s3   s4  5gs1  5gs2  5gs3  5gs4

 ------------------------------------------------------------------
   3    V                            V    V               V     V
```

Telnet Command: vlan off

This command allows you to disable VLAN function.

vlan off

Example

```
> vlan off
 VLAN is Disable!
 Force subnet LAN2/3/4 to be disabled!!
```

Telnet Command: vlan on

This command allows you to enable VLAN function.

vlan on

Example

```
> vlan on
 VLAN is Enable!
```

Telnet Command: vlan pri

This command is used to define the priority for each VLAN profile setting.

vlan pri *n pri_no*

Syntax Description

Parameter	Description
n	It means VLAN ID number. n=VLAN ID number (from 0 to 7).
pri_no	It means the priority of VLAN profile. pri_no=0 ~7 (from none to highest priority).

Example

```
> vlan pri 1 2
 VLAN1: Priority=2
```

Telnet Command: vlan restart

This command can make VLAN settings restarted with newest configuration.

vlan restart

Example

```
> vlan restart ?
 VLAN restarts!!!
```

Telnet Command: vlan status

This command display current status for VLAN.

vlan status

Example

```
> > vlan status
VLAN  is Disable :
-----------------------------------------------------------------------
VLAN Enable VID  Pri   p1 p2 p3 p4 s1 s2 s3 s4 5gs1 5gs2 5gs3 5gs4  subnet
-----------------------------------------------------
 0    OFF   0   0                                            1:LAN1
 1    OFF   0   2                                            1:LAN1
 2    OFF   0   0                                            1:LAN1
 3    OFF   0   0   V                 V  V            V    V  1:LAN1
 4    OFF   0   0                                            1:LAN1
 5    OFF   0   0                                            1:LAN1
 6    OFF   0   0                                            1:LAN1
 7    OFF   0   0                                            1:LAN1
 7    OFF   0   0                                            1:LAN1
-----------------------------------------------------------------------
-
 Note: they are only untag for s1/s2/s3/s4/5gs1/5gs2/5gs3/5gs4, but they can
join tag vlan with lan ports.
>
```

Telnet Command: vlan subnet

This command is used to configure the LAN interface used by the VLAN group.

vlan subnet group_id *[1/2]*

Syntax Description

Parameter	Description
[1/2]	It means interfaces, LAN1 ~ LAN2.

Example

```
> vlan subnet group_id 2
% Vlan Group-0 using LAN2      !

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: vlan submode

This command changes the VLAN encapsulation mechanisms in the LAN driver.

vlan submode *[on|off|status]*

Syntax Description

Parameter	Description
on	It means to enable the promiscuous mode.
off	It means to enable the normal mode.
status	It means to display if submode is normal mode or promiscuous mode.

Example

```
> vlan submode status
% vlan subnet mode : normal mode
> vlan submode on
% vlan subnet mode modified to promiscuous mode.
> vlan submode status
% vlan subnet mode : promiscuous mode
```

DrayTek

Telnet Command: vlan tagged

This command is used to enable or disable the incoming of untagged packets.

vlan tagged *[n] [on/off]*

vlan tagged *[unlimited] [on/off]*

Syntax Description

Parameter	Description
n	It means VLAN channel. The ranage is from 0 to 7.
on/off	It means to enable/disable the tagged VLAN.
[unlimited] [on/off]	unlimited on: It allows the incoming of untagged packets even all VLAN are tagged. unlimited off: It does not allows the incoming of untagged packets.

Example

```
> vlan tagged unlimited on
 unlimited mode is ON
```

Telnet Command: vlan vid

This command is used to configure VID number for each VLAN channel.

vlan vid *n vid_no*

Syntax Description

Parameter	Description
n	It means VLAN channel. The ranage is from 0 to 7.
vid_no	It means the value of VLAN ID. Type the value as the VLAN ID number. The range is form 0 to 4095.

Example

```
> vlan vid 1 4095
 VLAN1, vid=4095
```

Telnet Command: vlan sysvid

This command is used to modify and show the scope (reserved 64) of the VLAN IDs used internally by the system.

vlan sysvid *[show | n]*

Syntax Description

Parameter	Description
show	It means to show the scope of VLAN ID used internally.
n	It means the value to be set as VLAN ID. The range is from 0 to 4032.

Example

```
> vlan sysvid 100
 You have set system VLAN ID to range: 100 ~ 163,
 We recommend that you reboot the system now.

> vlan sysvid 200
 You have set system VLAN ID to range: 200 ~ 263,
 We recommend that you reboot the system now.
> vlan sysvid show
 The system VLAN ID is in range: 200 ~ 263
```

Telnet Command: vpn l2lset

This command allows users to set advanced parameters for LAN to LAN function.

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]* **phase***2[lifetime]*

vpn l2lset *[list index]* **x509localid** *[0/1]*

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.

DrayTek

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.
x509localid	It means to enable or disable local ID configuration for X509. 0 – disable 1- enable

Example

```
> > vpn l2lset 1 x509localid 1
% X509 local ID set
```

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.

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>	It means to set PIN code with secret.

| *<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.

vpn subnet *[index] [1/2]*

Syntax Description

Parameter	Description
<index>	It means the index number of the VPN profile.
<1/2>	1 – it means LAN1 2 – it means LAN2.

Example

```
> vpn subnet 1 2
>
```

Telnet Command: vpn setup

This command allows users to setup VPN for different types.

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.

Dray Tek

| | 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.

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 wlf, wlo, 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".

DrayTek

	"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.

DrayTek

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.

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.

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.

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 2ndsubnet

This command allows users to enable second subnet IP as VPN server IP.

vpn 2ndsubnet *on*

vpn 2ndsubnet *off*

Syntax Description

Parameter	Description
on/off	It means to enable or disable second subnet.

Example

```
> vpn 2ndsubnet on
%Enable second subnet IP as VPN server IP!
```

Telnet Command: vpn NetBios

This command allows users to enable or disable NetBios for Remote Access User Accounts or LAN-to-LAN Profile.

vpn NetBios set *<H2l/L2l> <index> <Block/Pass>*

Syntax Description

Parameter	Description
<H2l/L2l>	H2l means Remote Access User Accounts.

	L2l 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.

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 5 – SSL Tunnel
<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 SSL Tunnel : 1 ~ 1360

Example

```
>vpn mss set 1 1400
```

```
% VPN TCP maximum segment size (MSS) :
  PPTP  = 1400
  L2TP  = 1360
  IPSec = 1360
  L2TP over IPSec  = 1360
>vpn mss show
 VPN TCP maximum segment size (MSS) :
 PPTP  = 1400
 L2TP  = 1360
 IPSec = 1360
 L2TP over IPSec  = 1360
```

Telnet Command: vpn ike

This command is used to display IKE memory status and leakage list.

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**.**

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.

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.

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!!
```

DrayTek

Telnet Command: wan ppp_mru

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

wan ppp_mru *<WAN interface number> <MRU 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: 1500

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

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

Telnet Command: wan mtu

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

wan mtu *[value]*

Syntax Description

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

Example

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

Telnet Command: wan DF_check

This command allows you to enable or disable the function of DF (Don't fragment)

wan DF_check *[on]*

wan DF_check *[off]*

Syntax Description

Parameter	Description
on/off	It means to enable or disable DF.

Example

```
> wan DF_check on
%DF bit check enable!
```

Telnet Command: wan disable

This command allows you to disable WAN connection.

Example

```
> wan disable WAN
%WAN disabled.
```

Telnet Command: wan enable

This command allows you to disable wan connection.

Example

```
> wan enable WAN
%WAN1 enabled.
```

Telnet Command: wan forward

This command allows you to enable or disable the function of WAN forwarding. The packets are allowed to be transmitted between different WANs.

wan forward *[on]*

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!
```

Dray *Tek*

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 allows you to configure settings for USB modem.

wan modem *init [string]*

wan modem *init2[string]*

wan modem *dial [string]*

wan modem *pin [string]*

wan modem *paponly [on/off]*

wan modem *backup_wait [value]*

wan modem *pipe [string]*

wan modem *wakeup [on/off/value]*

wan modem status

Syntax Description

Parameter	Description
init [string]	It means to set initial modem AT command. string: type text. (default: AT&FE0V1X1&D2&C1S0=0)

init2[string]	It means to set initial2 modem AT command. string: type text.
dial [string]	It means to set dial modem AT command. string: type the command (default: ATDT*99#).
pin [string]	It means to set PIN code (0: disable) on SIM card. If "0" is typed, it means disable the function. string: type the PIN code (4 digits) in this field.
paponly [on/off]	Force PPP authentication PAP only (on/off).
backup_wait [value]	Set the wait time (1-255 sec) for rebooting the router when work in backup mode.
pipe [string]	Force 3G Modem pipe to be Int/Din/Dout (ex: 0x81 0x82 0x02). Int: It means USB interrupt pipe. Din: It means USB data input pipe. Dout: It means USB data output pipe.
wakeup on	It means to wake up the modem by telnet.
wakeup off	It means to wake up the modem by Vigor router.
wakeup [value]	It means the commands used to wakup modem. The format shall be heximal digits. *vid*: Set device VID belong to this interface (for multiple device) *pid*: Set device PID belong to this interface (for multiple device)
status	It means to display current information of WAN status.

Example

```
> wan modem pipe 0x81 0x82 0x01
  Force 3G USB Int/Din/Dout Pipe 0x81 0x82 0x1
> wan modem wakeup on
  turn on wakeup by telnet mode, usb will reset now
  wakeup string should be 31 bytes
> wan modem wakeup off
  turn off wakeup by telnet mode, usb will reset now
  wakeup string should be 31 bytes
```

Telnet Command: wan wimax

This command allows you to enable or disable WAN 3G/4G DHCP mode for Vigor router.

wan wimax *[on/off]*

Syntax Description

Parameter	Description
On	It means to enable WAN 3G/4G DHCP mode.

Dray Tek

off	It means to disable WAN 3G/4G DHCP mode.

Example

```
> wan wimax ?
 Current status is wimax OFF
> wan wimax on
>
```

Telnet Command: wan detect

This command allows you to Ping a specified IP to detect the WAN connection (static IP or PPPoE mode).

wan detect *[wan1][on/off/always_on]*

wan detect *[wan1]***target** *[ip addr]*

wan detect *[wan1]***ttl** *[1-255]*

wan detect status

Syntax Description

Parameter	Description
on	It means to enable ping detection. The IP address of the target shall be set.
off	It means to enable ARP detection (default).
always_on	disable link detect, always connected(only support static IP)
target	It means to set the ping target.
ip addr	It means the IP address used for detection. Type an IP address in this field.
ttl	It means to set the ping TTL value (work as trace route)
	If you do not set any value for ttl here or just type 0 here, the system will use default setting (255) as the ttl value.
status	It means to show the current status.

Example

```
> wan detect status
 WAN1: always on
 WAN2: off
 WAN3: off
 WAN4: off
 WAN5: off
> wan detect wan1 target 192.168.1.78
 Set OK

> wan detect wan1 on
 Set OK
```

```
> wan detect status
 WAN1: on, Target=192.168.1.78, TTL=255
 WAN2: off
 WAN3: off
 WAN4: off
 WAN5: off
>
```

Telnet Command: wan lb

This command allows you to Enable/Disable for each WAN to join auto load balance member.

wan lb *[wan1/wan2/…] on*

wan lb *[wan1/wan2/…] off*

Syntax Description

Parameter	Description
wan1/wan2	It means to specify which WAN will be applied with load balance.
on	It means to make 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
```

Telnet Command: wan mvlan

This command allows you to configure multi-VLAN for WAN and LAN. It supports pure bridge mode (modem mode) between Ethernet WAN and LAN port 2~4.

wan mvlan *[pvc_no/status/save/enable/disable] [on/off/clear/tag tag_no] [service type/vlan priority] [px ...]*

Syntax Description

Parameter	Description
pvc_no	It means index number of PVC. There are 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.

Dray Tek

on/off	It means to turn on/off bridge mode for the specific channel.
clear	It means to turn off/clear the port.
tag tag_no	It means to tag a number for the VLAN. -1: No need to add tag number. 1-4095: Available setting numbers used as tagged number.
service type	It means to specify the service type for VLAN. 0: Normal. 1: IGMP.
vlan priority	It means to specify the priority for the VALN setting. Range is from 0 to 7.
px	It means LAN port. Available setting number is from 2 to 4. Port number 1 is locked for NAT usage.

Example

PVC 7 will map to LAN port 2/3/4 in bridge mode; service type is Normal. No tag added.

```
> wan mvlan 7 on p2 p3 p4
PVC  Bridge  p1 p2 p3 p4   Service Type   Tag     Priority
 ---------------------------------------------------------
   7  ON      0  0  1  1      Normal      0(OFF)     0
>
```

Telnet Command: wan multifno

This command allows you to specify a channel (in Multi-PVC/VLAN) to make bridge connection to a specified WAN interface.

wan multifno *[channel #] [WAN interface #]*

wan multifno *status*

Syntax Description

Parameter	Description
channel #	There are several channels including VLAN and PVC. Available settings are: 3=Channel 3 4=Channel 4 5=Channel 5 6=Channel 6 7=Channel 7 8=Channel 8
WAN interface #	Type a number to indicate the WAN interface. *1=WAN1* *2=WAN2*
status	It means to display current bridge status.

Example

```
> wan multifno 5 1
% Configured channel 5 uplink to WAN1
> wan multifno status
% Channel 3 uplink ifno: 3
% Channel 4 uplink ifno: 3
% Channel 5 uplink ifno: 3
% Channel 6 uplink ifno: 3
% Channel 7 uplink ifno: 3
>
```

Telnet Command: wan vlan

This command allows you to tag packets on WAN VLAN with specified number.

wan vlan wan *[#]* **tag** *[value]*

wan vlan wan *[#]* *[enable|disable]*

wan vlan stat

Syntax Description

Parameter	Description
#	It means the number of WAN interface. 1: means WAN1 2: means WAN2.
value	It means the number to be tagged on packets. The range of the value is between 32 ~ 4095.
enable|disable	It means to enable or disable the WAN interface for VLAN.
stat	It means to display the table of WAN VLAN status.

Example

```
> wan vlan stat
%Interface    Pri    Tag    Enabled
%======================================
%WAN1         0      0
%WAN2         0      0
> wan vlan wan 1 tag 3
% Set tag to 3 for WAN1
> wan vlan wan 1 tag 50
%Set tag to 50 for WAN1
> wan vlan wan 2 tag 60
%Set tag to 60 for WAN2
> wan vlan wan 1 enable
%Enabled VLAN header encap for WAN1
> wan vlan wan 2 enable
%Enabled VLAN header encap for WAN2
> wan vlan stat
```

Dray Tek

```
%Interface     Pri     Tag     Enabled
%======================================
%WAN1          0       50        v
%WAN2          0       60        v
> wan vlan wan 2 disable
% Disabled VLAN header encap for WAN2
```

Telnet Command: wan fiber

This command allows you to configure the transmission rate for fiber connection.

wan fiber *status*

wan fiber *auto/100/1000*

Syntax Description

Parameter	Description
status	It means to show fiber WAN link status.
auto/100/1000	It means the transmission rate for fiber connection.
	It means to configure the transmission rate to 100Mbps, 1000Mbps or auto detection.
	100: menas 100Mbps
	1000: means 1000Mbps

Example

```
> wan fiber status
% Fiber is not detected
```

Telnet Command: wptl

This command is used to set the profile for wireless access control.

This command is used to set profile for web portal. Web portal is a special page that is shown when users browse to websites for the first time.

wptl -p *<profile> [-l <lan>] [-s <ssid>] [-m <message> | -u <url> | -f <url>] [-e | -d]*

wptl -p *<profile> -c*

wptl -i

Syntax Description

Parameter	Description
profile	It means to specify one of the SSID profiles for configuration.
	The range is from 1 to 4.
-l <lan>	It means to specify which LAN interface to be applied with such profile.
-s <ssid>	It means to specify which WLAN interface (identified by SSID number) will be applied with such profile.
	1: SSID1
	2: SSID2

	3: SSID3
	4: SSID4
-m \<message\>	It means the wireless client will be redirected to a page with message when the client accesses into Internet.
	message: type the text to be displayed.
-u \<url\>	It means the wireless client will be redirecte to a page with URL specifeied here when the client access into the Internet.
	url: type the url of the web page.
-f \<url\>	It means the wireless client will be redirecte to a page with URL specifeied here when the client access into the Internet.
	The client must click on the button to proceed.
	url: type the url of the web page.
-e	It means to enable such profile.
-d	It means to disnable such profile.
-i	It means to show the content of such command.
-c	It means to reset the specified profile.

Example

```
> wptl -e -p 1 -l 1,2 -s 1 -u http://www.draytek.com
Profile 1 enable ... [OK]
Applied LAN interfaces ... [OK]
Applied WLAN interfaces ... [OK]
Redirect to URL mode ... [OK]
> wptl -i
Profile 1:        ON
 Redirect to URL: "http://www.draytek.com"
 Applied interface:  LAN1, LAN2, SSID1

Profile 2:       OFF
 Redirect to URL: ""
 Applied interface:

Profile 3:       OFF
 Redirect to URL: ""
 Applied interface:

Profile 4:       OFF
 Redirect to URL: ""
 Applied interface:
```

DrayTek

Telnet Command: wl acl

This command allows the user to configure wireless access control settings.

wl acl enable *[ssid1 ssid2 ssid3 ssid4]*

wl acl disable *[ssid1 ssid2 ssid3 ssid4]*

wl acl add *[MAC] [ssid1 ssid2 ssid3 ssid4] [isolate]*

wl acl del *[MAC]*

wl acl mode *[ssid1 ssid2 ssid3 ssid4] [white/black]*

wl acl show

wl acl showmode

wl acl clean

Syntax Description

Parameter	Description
enable [ssid1 ssid2 ssid3 ssid4]	It means to enable the settings for SSID1, SSID2, SSID3 and SSID4.
disable [ssid1 ssid2 ssid3 ssid4]	It means to disable the settings for SSID1, SSID2, SSID3 and SSID4.
add [MAC] [ssid1 ssid2 ssid3 ssid4] [isolate]	It means to associate a MAC address to certain SSID interfaces' access control settings. The isolate setting will limit the wireless client's network capabilities to accessing the wireless LAN only. [MAC] format: xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx or xx.xx.xx.xx.xx.xx
del [MAC]	It means to delete a MAC address entry defined in the access control list.
mode [ssid1 ssid2 ssid3 ssid4] [white/black]	It means to set white/black list for each SSID.
wl acl show	It means to show access control status.
wl acl showmode	It means to show the mode for each SSID.
wl acl clean	It means to clean all access control setting.

Example

```
> > wl acl showmode
 ssid1: none
 ssid2: none
 ssid3: none
 ssid4: none
> wl acl add 00-50-70-ff-12-70
 Set Done !!
> wl acl add 00-50-70-ff-12-70 ssid1 ssid2 isolate
 Set Done !!
> wl acl show
```

```
         ----------Enable Mac Address Filter---------
 ssid1: dis   ssid2: dis   ssid3: dis   ssid4: dis
 ----------MAC Address Filter----------
 Index    Attribute      MAC Address        Associated SSIDs
   0                   00:50:70:ff:12:70   ssid1 ssid2 ssid3 ssid4
   1        s          00:50:70:ff:12:70   ssid1 ssid2

 s: Isolate the station from LAN
>
```

Telnet Command: wl config

This command allows users to configure general settings and security settings for wireless connection.

wl config mode *[value]*

wl config mode show

wl config channel *[number]*

wl config preamble *[enable]*

wl config txburst *[enable]*

wl config ssid *[ssid_num enable ssid_name [hidden_ssid]]*

wl config security *[SSID_NUMBER] [mode]*

wl config ratectl *[ssid_num enable upload download]*

wl config isolate *[ssid_num lan member]*

wl config dtim *[value]*

wl config dtim show

wl config beaconperiod

wl config radio enable

Syntax Description

Parameter	Description
mode[value]	It means to select connection mode for wireless connection.
	Available settings are: "11bgn", "11gn", "11n", "11bg", "11g", or "11b".
mode show	It means to display what the current wireless mode is.
channel [number]	It means the channel of frequency of the wireless LAN.
	The available settings are 0,1,2,3,4,5,6,7,8,9,10,11,12 and 13.
	number=0, means Auto
	number=1, means Channel 1
	….
	number=13, means Channel 13.
preamble [enable]	It means to define the length of the sync field in an 802.11 packet.
	Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync

DrayTek

	field. However, some original 11b wireless network devices only support long preamble.
	0: disable to use long preamble.
	1: enable to use long preamble.
txburst [enable]	It means to enhance the performance in data transmission about 40%* more (by enabling **Tx Burst**). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time.
	0: disable the function.
	1: enable the funciton.
ssid[ssid_num enable ssid_name [hidden_ssid]]	It means to set the name of the SSID, hide the SSID if required.
	ssid_num: Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4.
	ssid_name: Give a name for the specified SSID.
	hidden_ssid: Type 0 to hide the SSID or 1 to display the SSID
Security [SSID_NUMBER] [mode][key][index]	It means to configure security settings for the wirelesss connection.
	SSID_NUMBER: Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4.
	mode: Available settings are:
	disable: No security.
	wpa1x: WPA/802.1x Only
	wpa21x: WPA2/802.1x Only
	wpamix1x: Mixed (WPA+WPA2/802.1x only)
	wep1x: WEP/802.1x Only
	wpapsk: WPA/PSK
	wpa2psk: WPA2/PSK
	wpamixpsk: Mixed (WPA+WPA2)/PSK
	wep: WEP
	key, index: Moreover, you have to add keys for *wpapsk, wpa2psk, wpamixpsk* and *wep*, and specify index number of schedule profiles to be followed by the wireless connection.
	WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8~63 ASCII text string or 64 Hexadecimal digit format.
ratectl [ssid_num enable upload download]	It means to set the rate control for the specified SSID.
	ssid_num: Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4.
	enable: It means to enable the function of the rate control for the specified SSID. 0: disable and 1:enable.
	upload: It means to configure the rate control for data upload. The unit is kbps.
	download: It means to configure the rate control for data download. The unit is kbps.

isolate [ssid_num lan member]	It means to isolate the wireless connection for LAN and/or Member. *lan* – It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other. *member* – It can make the wireless clients (stations) with the same SSID not accessing for each other.
dtim [value]	It means to input DTIM value. Adjustable value is "1~255".
dtim show	It means to display current DTIM value.
beaconperiod	It means to set beacon period. Adjustable value is "20~1023". Unit is milli-second.
beaconperiod show	It means to display current beaconperiod value.
radio [enable]	It means to enable wireless Wi-Fi function. 1: enable 0: disable
raido show	It means to display current status of Wi-Fi function.

Example

```
> wl config mode 11bgn
 Current mode is 11bgn
% <Note> Please restart wireless after you set the channel
> wl config channel 13
 Current channel is 13
% <Note> Please restart wireless after you set the channel.
> wl config preamble 1
 Long preamble is enabled
% <Note> Please restart wireless after you set the parameters.
> wl config ssid 1 enable dray
 SSID  Enable  Hide_SSID  Name
 1     1       0          dray
% <Note> Please restart wireless after you set the parameters.
> wl config security 1 wpa1x
%% Configured Wlan Security Setting:
% SSID1
%% Mode: wpa1x
%% Wireless card must be reset for configurations to take effect
%% (Telnet Command: wl restart)
```

Telnet Command: wl set

This command allows users to configure basic wireless settings.

wl set *[SSID] [CHAN[En]]*

wl set txburst *[enable]*

Syntax Description

Parameter	Description
SSID	It means to type the SSID for the router. The maximum character that you can use is 32.
CHAN[En]	It means to specify required channel for the router. *CHAN:* The range for the number is between 1 ~ 13. *En*: type *on* to enable the function; type *off* to disable the function.
txburst [enable]	It means to enhance the performance in data transmission about 40%* more (by enabling **Tx Burst**). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. 0: disable the function. 1: enable the function.

Example

```
> wl set MKT 2 on
% New Wlan Setting is:
% SSID=MKT
% Chan=2
% Wl is Enable
```

Telnet Command: wl act

This command allows users to activate wireless settings.

wl act *[En]*

Syntax Description

Parameter	Description
En	It means to enable or disable the function of VPN isolation. 0: diable 1: enable

Example

```
> wl act on
% Set Wlan to Enable.
```

Telnet Command: wl stamgt

This command is used to configure connection time and reconnection time for each SSID that wireless client used for accessing into Internet.

wl stamgt *[enable/disable] [ssid_num]*

wl stamgt *[show] [ssid_num]*

wl stamgt set *[ssid_num] [c] [r]*

wl stamgt reset *[ssid_num]*

Syntax Description

Parameter	Description
enable/disable	It means to enable/disable the station management control.
ssid_num	It means channel selection. Available channel for 2.4G: 0/1/2/3 Available channel for 5G: 4/5/6/7.
show	It means to display status or configuration of the selected channel.
c	It means connection time. The unit is minute.
r	It means reconnection time. The unit is minute.

Example

```
> wl stamgt enable 1
% Station Management Status: enabled
> wl stamgt set 1 60 60
> wl stamgt show 1
NO. SSID          BSSID                 Connect time  Reconnect time
1.  Draytek       00:11:22:aa:bb:cc  0d:0:58:26       0d:0:0
```

Telnet Command: wl iso_vpn

This command allows users to activate the function of VPN isolation.

wl iso_vpn *[ssid] [En]*

Syntax Description

Parameter	Description
ssid	It means the number of SSID. 1: SSID1 2: SSID2 3: SSID3 4: SSID4
En	It means to enable or disable the function of VPN isolation. 0: disable 1: enable

Example

```
> wl iso_vpn 1 on
% ssid: 1 isolate vpn on :1
```

Telnet Command: wl wmm

This command allows users to set WMM for wireless connection. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs).

wl wmm ap *QueIdx Aifsn Cwmin Cwmax Txop ACM*

wl wmm bss *QueIdx Aifsn Cwmin Cwmax Txop ACM*

wl wmm ack *Que0_Ack Que1_Ack Que2_Ack Que3_Ack*

wl wmm enable *SSID0 SSID1 SSID2 SSID3*

wl wmm apsd *value*

wl wmm show

Syntax Description

Parameter	Description
ap	It means to set WMM for access point.
bss	It means to set WMM for wireless clients.
ack	It means to map to the Ack policy settings of AP WMM.
enable	It means to enable the WMM for each SSID. 0: disable 1: enable
Apsd [value]	It means to enable / disable the ASPD(automatic power-save delivery) function. 0: disable 1: enable

show	It displays current status of WMM.
QueIdx	It means the number of the queue which the WMM settings will be applied to. There are four queues, best effort, background, voice, and video.
Aifsn	It controls how long the client waits for each data transmission.
Cwmin/ Cwmax	**CWMin** means contention Window-Min and **CWMax** means contention Window-Max. Specify the value ranging from 1 to 15.
Txop	It means transmission opportunity. Specify the value ranging from 0 to 65535.
ACM	It can restrict stations from using specific category class if it is enabled. 0: disable 1: enable

Example

```
> wl wmm ap 0 3 4 6 0 0
 QueIdx=0: APAifsn=3,APCwmin=4,APCwmax=6, APTxop=0,APACM=0
> wl wmm enable 1 0 1 0
 WMM_SSID0 =1, WMM_SSID1 =0,WMM_SSID2 =1,WMM_SSID3 =0
> wl wmm show
 Enable WMM: SSID0 =1, SSID1 =0,SSID2 =1,SSID3 =0
 APSD=0
 QueIdx=0: APAifsn=3,APCwmin=4,APCwmax=6, APTxop=0,APACM=0
 QueIdx=1: APAifsn=7,APCwmin=4,APCwmax=10, APTxop=0,APACM=0
 QueIdx=2: APAifsn=1,APCwmin=3,APCwmax=4, APTxop=94,APACM=0
 QueIdx=3: APAifsn=1,APCwmin=2,APCwmax=3, APTxop=47,APACM=0
 QueIdx=0: BSSAifsn=3,BSSCwmin=4,BSSCwmax=10, BSSTxop=0,BSSACM=0
 QueIdx=1: BSSAifsn=7,BSSCwmin=4,BSSCwmax=10, BSSTxop=0,BSSACM=0
 QueIdx=2: BSSAifsn=2,BSSCwmin=3,BSSCwmax=4, BSSTxop=94,BSSACM=0
 QueIdx=3: BSSAifsn=2,BSSCwmin=2,BSSCwmax=3, BSSTxop=47,BSSACM=0
 AckPolicy[0]=0: AckPolicy[1]=0,AckPolicy[2]=0,AckPolicy[3]=0
```

Telnet Command: wl ht

This command allows you to configure wireless settings.

wl ht bw *value*

wl ht gi *value*

wl ht badecline *value*

wl ht autoba *value*

wl ht rdg *value*

wl ht msdu *value*

wl ht txpower *value*

wl ht antenna *value*

DrayTek

wl ht greenfield *value*

Syntax Description

Parameter	Description
wl ht bw value	The value you can type is 0 (for BW_20) and 1 (for BW_40).
wl ht gi value	The value you can type is 0 (for GI_800) and 1 (for GI_4001)
wl ht badecline value	The value you can type is 0 (for disabling) and 1 (for enabling).
wl ht autoba value	The value you can type is 0 (for disabling) and 1 (for enabling).
wl ht rdg value	The value you can type is 0 (for disabling) and 1 (for enabling).
wl ht msdu value	The value you can type is 0 (for disabling) and 1 (for enabling).
wl ht txpower value	The value you can type ranges from 1 – 6 (level).
wl ht antenna value	The value you can type ranges from 0-3. 0: 2T3R 1: 2T2R 2: 1T2R 3: 1T1R
wl ht greenfield value	The value you can type is 0 (for mixed mode) and 1 (for green field).

Example

```
> wl ht bw value 1
 BW=0
 <Note> Please restart wireless after you set new parameters.
> wl restart
 Wireless restart...............
```

Telnet Command: wl restart

This command allows you to restart wireless setting.

Example

```
> wl restart
 Wireless restart...............
```

Telnet Command: wl btnctl

This command allows you to enable or disable wireless button control.

wl btnctl *[value]*

Syntax Description

Parameter	Description

| value | 0: disable |
| | 1: enable |

Example

```
> wl btnctl 1
Enable wireless botton control
Current wireless botton control is on
>
```

Telnet Command: wl iwpriv

It is reserved for RD debug. Do not use it.

Telnet Command: wl efuse

This command is used to configure parameters related to wireless RF hardware. At present, it is not allowed for end user to operate.

Telnet Command: wl ce_cert

It is reserved for RD debug. Do not use it.

Telnet Command: wl dual acl

This command allows the user to configure wireless (5GHz) access control settings.

wl dual acl enable *[ssid1 ssid2 ssid3 ssid4]*

wl dual acl disable*[ssid1 ssid2 ssid3 ssid4]*

wl dual acl add *[MAC][ssid1 ssid2 ssid3 ssid4][isolate]*

wl dual acl del *[MAC]*

wl dual acl mode *[ssid1 ssid2 ssid3 ssid4] [white/black]*

wl dual acl show

wl dual acl showmode

wl dual acl clean

Syntax Description

Parameter	Description
enable [ssid1 ssid2 ssid3 ssid4]	It means to enable the settings for SSID1, SSID2, SSID3 and SSID4.
disable [ssid1 ssid2 ssid3 ssid4]	It means to disable the settings for SSID1, SSID2, SSID3 and SSID4.
add [MAC] [ssid1 ssid2 ssid3 ssid4] [isolate]	It means to associate a MAC address to certain SSID interfaces' access control settings. The isolate setting will limit the wireless client's network capabilities to accessing the wireless LAN only.
	[MAC] format: xx-xx-xx-xx-xx-xx
	or xx:xx:xx:xx:xx:xx
	or xx.xx.xx.xx.xx.xx
isolate	It means to isolate the wireless connection of the wireless

	client (identified with the MAC address) from LAN.
del[MAC]	It means to delete a MAC address entry defined in the access control list.
	[MAC] format: xx-xx-xx-xx-xx-xx
	or xx:xx:xx:xx:xx:xx
	or xx.xx.xx.xx.xx.xx
mode [ssid1 ssid2 ssid3 ssid4] [white/black]	It means to set white/black list for each SSID.
show	It means to display current status of access control.
showmode	It means to show the mode for each SSID.
clean	It means to clear all of the access control settings.

Example

```
> wl dual acl showmode
 SSID1: None
 SSID2: None
 SSID3: None
 SSID4: None
> wl dual acl add 00-50-70-ff-12-80
> wl acl add 00-50-70-ff-12-80 ssid1 ssid2 isolate
 Set Done !!
> wl acl show
 ----------Enable Mac Address Filter---------
 ssid1: dis   ssid2: dis   ssid3: dis   ssid4: dis
 ----------MAC Address Filter----------
 Index   Attribute      MAC Address       Associated SSIDs
   0       s           00:50:70:ff:12:80   ssid1 ssid2

 s: Isolate the station from LAN
>
```

Telnet Command: wl dual apscan

This command is used to scan Access Point installed near the location of Vigor router.

wl dual apscan *start*

wl dual apscan *show*

Syntax Description

Parameter	Description
start	It menas to execute the AP scanning.
show	It means to disaply the content of the AP list.

Example

```
> wl dual apscan start
> wl dual apscan show
```

```
5G Access Point List :
BSSID           Channel  SSID
00:1d:aa:b6:1b:ba    60    Marketing-wi-fi_5G
00:1d:aa:ba:07:2a    36    DrayTek_5G
>
```

Telnet Command: wl dual config

This command allows users to configure general settings and security settings for wireless connection (5GHz).

wl dual config enable *[value]*

wl dual config enable show

wl dual config mode *[value]*

wl dual config mode show

wl dual config channel *[number]*

wl dual config channel show

wl dual config preamble *[enable]*

wl dual config preamble show

wl dual config ssid *[ssid_num enable ssid_name]*

wl dual config ssid hide *[ssid_num enable]*

wl dual config ssid show

wl dual config ratectl *[ssid_num enable upload download]*

wl dual config ratectl show

wl dual config isolate lan *[ssid_num enable]*

wl dual config isolate member *[ssid_num enable]*

wl dual config isolate vpn *[ssid_num enable]*

wl dual config isolate show

Syntax Description

Parameter	Description
enable[value]	It means to enable/disable the 5GHz wireless function. 1: enable 0: disable
show	It means to display if 5G wireless function is enabled or not.
mode[value]	It means to select connection mode for wireless connection. Available settings are: "11a", "11n_5g", "11n" and "11an".
mode show	It means to display what the current wireless mode is.
channel [number]	It means the channel of frequency of the wireless LAN. The available settings are: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136 and 140. number=0, means Auto number=36, means Channel 36

Dray Tek

	….
	Number=52, means Channel 52.
channel show	It means to display what the current channel is.
preamble [enable]	It means to define the length of the sync field in an 802.11 packet.
	Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble.
	0: disable to use long preamble.
	1: enable to use long preamble.
preamble show	It means to display if preamble is enabled or not.
ssid[ssid_num enable ssid_name]	It means to set the name of the SSID, hide the SSID if required.
	ssid_num: Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4.
	ssid_name: Give a name for the specified SSID.
ssid hide [ssid_num enable]	It means to hide the name of the SSID if required.
	ssid_num: Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4.
	enable: Type 0 to hide the SSID or 1 to display the SSID.
ssid show	It means to display a table of SSID configuration.
ratectl [ssid_num enable upload download]	It means to set the rate control for the specified SSID.
	ssid_num: Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4.
	enable: It means to enable the function of the rate control for the specified SSID. 0: disable and 1:enable.
	upload: It means to configure the rate control for data upload. The unit is kbps.
	download: It means to configure the rate control for data download. The unit is kbps.
	(example: `wl dual config ratectl 1 1 25 25`)
ratectl show	It means to display the data transmission rate (upload and download) for SSID1, SSID2, SSID3 and SSID4.
isolate lan [ssid_num enable]	It means to isolate the wireless connection from LAN.
	It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other.
	ssid_num: Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4.
	enable: It means to enable such function.
	0: disable and 1:enable
isolate member [ssid_num enable]	It means to isolate the wireless connection from Member.
	It can make the wireless clients (stations) with the same SSID not accessing for each other.
	ssid_num: Choose 1, 2, 3 or 4 to specify SSID1, SSID2,

	SSID3 or SSID4.
	enable: It means to enable such function.
	0: disable and 1:enable.
isolate vpn [ssid_num enable]	It means to isolate the wireless connection from VPN.
	ssid_num: Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4.
	enable: It means to enable such function.
	0: disable and 1:enable.
isolate show	It means to display the status of wireless isolation.

Example

```
> wl dual config mode 11a
 Current mode is 11a
% <Note> Please restart 5G wireless after you set the channel
> wl dual config channel 60
 Current channel is 60
% <Note> Please restart 5G wireless after you set the channel.
> wl dual config preamble 1
Long preamble is enabled
% <Note> Please restart 5G wireless after you set the parameters.
> wl dual config ssid 1 enable dray
SSID  Enable  Hide_SSID  Name
 1    1       0          dray
% <Note> Please restart 5G wireless after you set the parameters.
> > wl dual config ssid show
 SSID  Enable  Hide_SSID  Name
 1    1       0          dray
 2    0       0          DrayTek_5G_Guest
 3    0       0
 4    0       0
```

Telnet Command: wl dual cmd

It is reserved for RD debug. Do not use it.

Telnet Command: wl dual ce_cert

It is reserved for RD debug. Do not use it.

Telnet Command: wl dual restart

This command allows you to restart wireless setting (5GHz).

Example

```
> > wl dual restart
 5G wireless restart...............
```

Telnet Command: wl dual security

This command allows users to configure security settings for the wirelesss connection (5GHz).

wl dual security*[SSID_NUMBER] [mode][key][index]*

wl dual security show

Syntax Description

Parameter	Description
Security [SSID_NUMBER] [mode][key][index]	*SSID_NUMBER*: Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4.
	mode: Available settings are:
	disable: No security.
	wpa1x: WPA/802.1x Only
	wpa21x: WPA2/802.1x Only
	wpamix1x: Mixed (WPA+WPA2/802.1x only)
	wep1x: WEP/802.1x Only
	wpapsk: WPA/PSK
	wpa2psk: WPA2/PSK
	wpamixpsk: Mixed (WPA+WPA2)/PSK
	wep: WEP
	key, index: Moreover, you have to add keys for *wpapsk, wpa2psk, wpamixpsk* and *wep*, and specify index number of schedule profiles to be followed by the wireless connection.
	WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8~63 ASCII text string or 64 Hexadecimal digit format.
show	It means to display current mode selection for each SSID.

Example

```
> wl dual security 1 wpa2psk 123456789e
% <Note> Please restart 5G wireless after you set the parameters.

> wl dual security show
%% 5G Wireless LAN Security Settings:
% SSID1
%%  Mode: WPA2/PSK
% SSID2
%%  Mode: Disable
% SSID3
%%  Mode: Disable
% SSID4
%%  Mode: Disable
>
```

Telnet Command: wl dual stalist

This command is used to display the wireless station which accessing Internet via Vigor2120.

wl dual stalist

Example

```
> wl dual stalist
  5G Wireless Station List :
  SSID  MAC Address         Status
  1     00:50:7f:f0:c5:3c    C

  Status Codes :
    C: Connected, No Encryption.
    E: Connected, WEP.
    P: Connected, WPA.
    A: Connected, WPA2.
    N: Connecting.
```

Telnet Command: wl dual wds

This command allows users to configure WDS for wireless connection (5GHz).

wl dual wds mode *[value]*

wl dual wds security *[value]*

wl dual wds ap *[value]*

wl dual wds hello *[value]*

wl dual wds status

wl dual wds show

wl dual wds mac add *[index addr]*

wl dual wds mac clear/disable/enable *[index/all]*

wl dual wds flush

Syntax Description

Parameter	Description
mode *[value]*	It means to specify connection mode for WDS.
	[value]: Available settings are :
	d: Disable
	b: Bridge
	r: Repeapter
security *[value]*	It means to configure security mode with encrypted keys for WDS.
	mode: Available settings are:
	disable: No security.
	wep: WEP
	wpapsk [key]: WPA/PSK

	wpa2psk [key]: WPA2/PSK
	key: Moreover, you have to add keys for *wpapsk, wpa2psk,* and *wep*, and specify index number of schedule profiles to be followed by the wireless connection.
	WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8~63 ASCII text string or 64 Hexadecimal digit format.

	e.g., `wl dual wds security disable`
	`wl dual wds security wep 12345`
	`wl dual wds security wpa2psk 12345678`

ap *[value]*	It means to enable or disable the AP function. Value: 1 – enable the function. 0 – disable the function.
hello *[value]*	It means to send hello message to remote end (peer). Value: 1 – enable the function. 0 – disable the function.
status	It means to display WDS link status for 5GHz connection.
show	It means to display current WDS settings.
mac add *[index addr]*	**add** *[index addr] – A*dd the peer MAC entry in Repeater/Bridge WDS MAC table.
mac clear/disable/enable *[index/all]*	**clear/disable/enable** *[index/all]*- Clear, disable, enable the specifed or all MAC entries in Repeater/Bridge WDS MAC table. e.g, `wl dual wds mac enable 1`
flush	It means to reset all WDS setting.

Example

```
> wl dual wds status
Please enable WDS hello function first.

> wl dual wds hello 1
% <Note> Please restart router after you set the parameters.
> wl dual wds mode b
> wl dual wds security wep
>
>
> wl dual wds show
5G Wireless WDS Setting

Mode : Bridge
Security : WEP
AP Function : Enable
Send Hello Function : Enable

Bridge :
```

```
Index  Enable  MAC Address
  1     0      00:00:00:00:00:00
  2     0      00:00:00:00:00:00
  3     0      00:00:00:00:00:00
  4     0      00:00:00:00:00:00


Repeater :
Index  Enable  MAC Address
  5     0      00:00:00:00:00:00
  6     0      00:00:00:00:00:00
  7     0      00:00:00:00:00:00
  8     0      00:00:00:00:00:00
> wl dual wds wep 12345
% <Note> Please restart router after you set the parameters.
```

Telnet Command: wl dual wps

This command allows users to configure WPS for wireless connection (5GHz).

wl dual wps enable *[value]*

wl dual wps pbc

wl dual wps pin *[code]*

wl dual wps show

Syntax Description

Parameter	Description
enable [value]	It means to enable WPS. 1 – enable 0 – disable
pbc	It means to start WPS by pressing the WLAN ON/OFF WPS button on Vigor router.
pin [code]	It means to start WPS by using client PIN code. [code]: Client PIN code (digit number).
show	It means to display current WPS settings.

Example

```
> wl dual wps enable 1
 WPS is enabled.
> wl dual wps pin 88563337
 WPS has triggered by PIN code.
 The AP will wait for WPS request from your client for 2 minutes...
>
```

Dray Tek

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.

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: on

> wol fromWan_Setting 1 192.168.1.45 255.255.255.0
% wol fromWan_Setting 1 192.168.1.45 255.255.255.0
```

Telnet Command: appqos

The command is used to configure QoS for APP.

appqos view

appqos enable*[0/1]*

appqos traceable *[-v | -e AP_INDEX CLASS | -d AP_INDEX]*

appqos untraceable

appqos show_config *[-t |–u]*

Syntax Description

Parameter	Description
view	It means to display current status of APP QoS.
enable[0/1]	It means to enable or disable the function of APP QoS.
traceable/ untraceable	The APPs are divided into traceable and untraceable based on their properties.
-v	It means to view the content of all traceable APs. Use "appqos traceable –v" to display all of the traceable APS with speficed index number. Use "appqos untraceable –v" to display all of the untraceable APS with speficed index number.
-e	It menas to enable QoS for application(s) and assign QoS class.
AP_INDEX	Each index number represents one application. Index number: 50, 51, 52, 53, 54, 58, 60, 62, 63, 64, 65, 66, 68 are used for 13 traceabel APPs. Index number: 0~49, 55~59, 61, 67, 69, and 70~123 are used for 125 untraceable AP.
CLASS	Specifies the QoS class of the application, from 1 to 4 1:Class 1, 2:Class 2, 3:Class 3, 4:Other Class
-d	It means to disable QoS for application(s).
show_config [-t /–u]	It means to display all of the traceable/untraceable APs and the configuration.

Example

```
> appqos enable 1

APP QoS set to Enable.
> appqos traceable -e 68 2

TELNET: ENABLED, QoS Class 2.
```